Table of Contents

Introduction 7

Chapter 1: Components Used by Cognos 8 Controller 9
  Server Components 9
    Interfaces 9
    Gateway Components 9
    Application Tier Components 10
    Content Manager Components 10
    Modeling Components 11
  Third-party Components 11

Chapter 2: Distribution Options for Cognos 8 Controller 13
  Distributing Cognos 8 Controller Components 13
    All Components on One Computer 13
    Components Distributed on Multiple Computers 14

Chapter 3: Workflows for Cognos 8 Controller 21

Chapter 4: Upgrading Cognos 8 Controller 25
  Install or Upgrade Third-party Products 25
  Back Up Your Application Data 26
  Uninstall the Older Version of Cognos 8 Controller 26
  Install the New Version of Cognos 8 Controller 26
  Apply the New Configuration 27
  Upgrade Your Application Databases 27
    Schedule a Performance Optimization Procedure for an Oracle Controller Database 27
  Upgrade the Data Entry Forms 28
  Upgrade the User-defined Reports 28
  Upgrade the Excel Link Report Formulas 29
  Upgrade the Consolidation Model 29
  Upgrading to a New Computer 30

Chapter 5: Installing Cognos 8 Controller 31
  Confirm System Requirements 31
    Review Supported Environments 33
  Set Up Database Connectivity for the Reporting Database 33
  Set Up Database Connectivity for the Content Store Database 34
  Set Up Database Connectivity for the Controller Data Mart 34
  Install Microsoft .NET Framework 35
    Install Microsoft .NET Framework SDK 35
  Install and Configure ASP.NET 35
  Install Cognos 8 Controller Server Components 35
    Default Settings for Cognos 8 Controller 37
  Install the Cognos 8 Controller Client and Add-In for Excel 38
  Install Framework Manager 38
  Uninstall Cognos 8 Controller 39

Chapter 6: Setting Up the Environment 41
  Create a Cognos Controller Database 41
  Create the Content Store 42
  Set Up the Database Client for the Content Store 45
  Create a Controller Data Mart Database 46
Update the Java Environment 47
Configure the Web Server 47
Configure Microsoft .NET Framework 48
Configure the Web Browser 50
Configure the Router to Test Dispatcher Availability 51

Chapter 7: Configuring Cognos 8 Controller 53
Configuring Single-computer Installations 53
  Set Database Connection Properties for the Content Store 54
  Test the Reporting Components Installation and Configuration 55
  Set Database Connection Properties for the Controller Data Source 56
  Set Database Connection Properties for the Controller Data Mart 57
  Import the Cognos 8 Controller Standard Reports Package 58
  Define a Data Source for the Controller Data Mart 58
  Extract the Publish to Data Mart Model and Publish It to Cognos Connection 59
  Set Import Directories for Flat Files 59
  Enable Access to the COM+ Server 59
  Configure the COM+ Server 60
  Test the Cognos 8 Controller Installation and Configuration 60
Configuring Distributed Installations 61
  Configuring the Content Manager Computer 63
  Configure the Report Server Computers 65
  Configure the Gateway Computers 65
  Configure Framework Manager Computers 66
  Test the Content Manager, Report Server, Gateway, and Framework Manager Installation and Configuration 67
  Configuring the Controller Web Services Server Computers 68
  Configure the Controller Client Distribution Server Computer 72
  Import the Cognos 8 Controller Standard Reports Package 73
  Define a Data Source for the Controller Data Mart 73
  Extract the Publish to Data Mart Model and Publish It to Cognos Connection 74
  Schedule a Performance Optimization Procedure for an Oracle Controller Database 74
  Test the Cognos 8 Controller Installation and Configuration 74
Changing Cognos 8 Controller Default Configuration Settings 76
  Change a URI 76
  Changing the Gateway 78
  Configure Cryptographic Settings 80
  Configuring the SSL Protocol 81
  Configure Reporting Components to Use Cognos Application Firewall 84
  Configure Temporary File Properties 85
  Configuring Log Messages 86
  Changing the Gateway 88
  Configure the Gateway to Use a Namespace 88
  Enable and Disable Services 89
  Specify Resources for the Cognos 8 Service 89
  Global Settings 90
  Add or Remove Controller Database Connections 91
  Change the COM+ Server Configuration 92
  Enable Batch Services 93
  Enable Enhanced Reporting Optimization 93
  Change the Default Installation of the Cognos 8 Controller Add-in for Excel 95
  Configuring Consolidation Load Balancing 95
  Configuring Multiple Server Operation with the Reporting Database 97

Chapter 8: Configuring Authenticated Access 101
Configure the Cognos 8 Controller Authentication Method 101
  Add Cognos Controller Users to the Cognos Controller Roles 103
  Map Cognos Controller Users to Cognos 8 Users 104
Introduction

This document is intended for use with Cognos 8 Controller. This guide contains instructions for installing, configuring, and testing Cognos 8 Controller.

Cognos 8 Controller is a Web-based financial consolidation tool that provides standard reports to support both statutory and management reporting.

Audience

To use this guide, you should be familiar with
- 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: If an error message appears when you click a document name, search the Documentation library of the Cognos Global Customer Services Web site (http://support.cognos.com). If you require logon credentials, consult your administrator or send an email to support.america@cognos.com.

<table>
<thead>
<tr>
<th>Document</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cognos 8 Controller Architecture and Deployment Guide</td>
<td>Planning the Cognos 8 Controller architecture, developing installation strategies, and optimizing performance</td>
</tr>
<tr>
<td>Cognos Configuration User Guide</td>
<td>Using Cognos Configuration to configure the Cognos 8 Controller components</td>
</tr>
<tr>
<td>Cognos Controller Configuration User Guide</td>
<td>Using Controller Configuration to configure Cognos 8 Controller components</td>
</tr>
<tr>
<td>Cognos 8 Administration and Security Guide</td>
<td>Managing servers and security; and customizing reporting components</td>
</tr>
<tr>
<td>Cognos 8 Supplementary Languages Installation and Configuration Guide</td>
<td>Installing Supplementary Languages, and configuring Cognos 8 to work with the selected languages.</td>
</tr>
</tbody>
</table>

Finding Information

To find the most current product documentation, including all localized documentation, access the Cognos Global Customer 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 Cognos products. You can also download documentation in PDF format from the Cognos Global Customer Services Web site, or click the following link to open a printable version of this document (PDF).

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

**Using Quick Tours**

Quick tours are short online tutorials that illustrate key features in Cognos product components. To view a quick tour, start 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 Global Customer Services Web site ([http://support.cognos.com](http://support.cognos.com)). This site provides product information, services, user forums, and a knowledge base of documentation and multimedia materials. To create a case, contact a support person, or provide feedback, click the Contact Us link. For information about education and training, click the Training link.

**Printing Copyright Material**

You can print selected pages, a section, or the whole book. Cognos grants you 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 Cognos software.
Chapter 1: Components Used by Cognos 8 Controller

Cognos 8 Controller is a Web-based solution designed to address financial consolidation needs and to support statutory and management reporting requirements.

Cognos 8 Controller integrates easily into your existing infrastructure by using resources that are in your environment. Some of these existing resources are required, such as a Java Virtual Machine or a third-party database for the content store. Other resources are optional, such as using a third-party security provider for authentication.

By default, the Cognos 8 Controller reporting components use the Tomcat application server.

Server Components

Server components provide the user interfaces for reporting and product configuration, as well as the server functionality for routing and processing user requests. Server components can be organized into four functional groups: interfaces, gateway components, application tier components and Content Manager components.

Interfaces

The following user interfaces are available for using and configuring Cognos 8 Controller.

**Cognos Controller**
Cognos Controller provides the user interface for financial consolidation. Cognos Controller is accessible through Cognos Connection, as well as through a URL.

**Cognos Connection**
Cognos Connection is a Web portal provided with 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 Cognos 8 applications through Cognos Connection. Other business intelligence applications, and URLs to other applications, can be integrated with Cognos Connection.

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

**Cognos Controller Configuration**
Cognos Controller Configuration is a Windows interface that you use to configure Cognos Controller data sources, set security, and administer system-wide Cognos Controller settings.

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

Gateway Components

The Cognos 8 Controller gateway components provide Web communication and access for client computers. The following gateway components are provided.
Chapter 1: Components Used by Cognos 8 Controller

**Gateway**
Web communication in Cognos 8 Controller 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.

**Controller Client Distribution Server**
Controller Client Distribution Server provides access to Cognos Controller for client computers. When a user starts Cognos Controller within a Web browser, Controller client components are downloaded from Controller Client Distribution Server (if necessary) and then Cognos Controller runs.

**Gateway Integration Enabler**
The Gateway Integration Enabler updates the gateway to make it aware of both the Cognos Controller and reporting components.

**Application Tier Components**
Application tier components provide the user interface for reporting and the server functionality for routing and processing requests. Cognos 8 Controller includes the following application tier components.

**Controller Web Services Server**
Controller Web Services Server processes all Cognos Controller requests, except for downloading Cognos 8 Controller components to the user's computer. Controller Web Services Server handles requests for activities within Cognos Controller, such as working with accounts, consolidations, companies, and dimensions. Controller Web Services Server also manages data source connections and security information, as well as preparing data in the Cognos Controller database for reports.

**Report Server**
Report Server renders Cognos Controller reports, in PDF and HTML formats using information provided in the Controller standard reports package. Report Server does not render reports for Cognos 8 Report Studio or other Cognos Studios and must not be installed with other Cognos 8 Business Intelligence products.

**Cognos Connection Integration Enabler**
The Cognos Connection Integration Enabler activates the links in Cognos Connection that users click to access Cognos Controller. These links are available from the Cognos Connection Welcome page and the home page.

**Content Manager Components**
The Cognos 8 Controller Content Manager components support the data functionality for the content store and Controller database.

**Content Manager**
Content Manager is the 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 models, retrieve or store report specifications, manage scheduling information, and manage the Cognos namespace.

Content Manager stores information in a content store database.

**Controller Standard Reports Package**
Report Server uses information in the Controller standard reports package, a Framework Manager package provided with Cognos 8 Controller, to determine the structure of data in the Controller database. The package contains preformatted templates that are used to obtain the data necessary for rendering the standard reports that are available with Cognos 8 Controller. You do not need to install Cognos 8 Framework Manager to use the standard reports package.
**Controller Framework Manager Model**

The Framework Manager model provided with Controller can be used to author custom reports. This Publish to Data Mart Framework Manager model is provided as a template designed for reporting against a Controller data mart database. You can also customize the model in Cognos 8 Framework Manager before creating the reports in Cognos 8 Report Studio.

To use this model, you must install Cognos 8 Framework Manager from the CD provided with Cognos 8 Controller or use Framework Manager from your Cognos 8 Business Intelligence installation.

**Modeling Components**

Modeling components are used to model data within data sources to structure and present data in a way that is meaningful to users.

**Framework Manager**

Framework Manager is the Cognos 8 modeling tool for creating and managing business-related metadata for use in 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.

**Third-party Components**

In addition to the tools provided with Cognos 8 Controller, the following components use third-party resources.

**Content Store**

The content store is a relational database that contains data that Cognos 8 Controller needs to operate, such as report packages and connection information about the external namespace and the Cognos namespace.

Log files are not stored in the content store.

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

**Controller Database**

Data sources, such as relational databases or other physical data stores, are used as the Controller database, which contains the data that the clients work with in Cognos 8 Controller.

Application Tier Components use data source connections to access the Controller database.

**Controller Data Mart Database**

A Controller data mart database is required if you use the Publish to Data Mart Framework Manager model provided with Cognos 8 Controller. By using the Publish to Data Mart functionality in Controller, you can publish data and structures from a Controller database to the data mart database. After it is populated, the Controller data mart database can be used for custom reporting using the Controller Publish to Data Mart Framework Manager model.
Chapter 1: Components Used by Cognos 8 Controller
Chapter 2: Distribution Options for Cognos 8 Controller

Before implementing Cognos 8 Controller, decide how you will install it in your environment. You can install all Cognos 8 Controller components on one computer, or distribute them across a network. The best distribution option depends on your reporting requirements, resources, and preferences. Configuration requirements differ depending on whether you install all components on a single or multiple computers.

Cognos 8 Controller is compatible with other Cognos 8 products. If your environment includes other Cognos products, you must consider how Cognos Controller will fit into that environment.

Distributing Cognos 8 Controller Components

When you install Cognos 8 Controller components, you specify where to place the gateways, Content Manager, and Application Tier Components.

Important: When Controller Client Distribution Server is installed on a different computer from the gateway or Report Server, additional configuration is required.

You can install the server components using any of these options:

• Install all components on one computer.
  This option is typically used for a demonstration or in a proof of concept environment.

• Distribute components in a role-based configuration and begin load balancing.
  You can start this distribution scenario by installing the gateway on a computer that has a Web server installed. You can install the reporting components, such as Content Manager and Report Server, on another computer, referred to as the reporting services server. Lastly, you can install the components that handle client requests and do the data calculations and consolidations of Cognos 8 Controller on another computer. This computer, referred to as the Controller Web Server, has Controller Web Services Server and Controller Client Distribution Server installed.

• Distribute components to improve load balancing of the consolidation functions.
  In this option, you add more computers to the previous scenario for increased distribution of the processing load. For example, you add an additional Controller Web Server computer for improved load balancing of the data consolidation functions.

• Install Cognos 8 Controller components to integrate with other Cognos 8 products.
  Cognos 8 Business Intelligence can share the Content Store and other components for analysis and reporting, such as Framework Manager and Report Studio, with other Cognos 8 products. If you plan to install Cognos 8 Controller components on the same computer as other Cognos 8 products, we recommend that you install them in the same installation location.

After installing Cognos 8 Controller components, you must configure them so they can communicate with each other.

All Components on One Computer

You can install all the Cognos 8 Controller components on one Windows computer. Choose this scenario for small, Controller-only installations. This type of installation is suitable for testing or proof of concept requirements.

Because the gateway must be located with the Web server, the single Windows computer must also be running a Web server.
Chapter 2: Distribution Options for Cognos 8 Controller

In the following diagram, all server components for Cognos 8 Controller are installed on one computer. The content store, Cognos Controller databases, and Controller data mart database are located on separate computers. The client components are also assumed to be on a separate computer.

**Configuration Requirements**

If you install all components for Cognos 8 Controller on the same computer, you must then
- configure your Web server
- specify connection information to the content store
- import the Cognos Controller standard reports package
- specify connection information to the Cognos Controller databases
- configure the COM+Server

If you have separate client computers, download the Microsoft .NET Runtime Security Policy, after you export it from the Controller Client Distribution Server.

If you want to use the Publish to Data Mart Framework Manager model, you must also install Cognos 8 Framework Manager and do some additional configuration to use the Publish to Data Mart Framework Manager model.

**Components Distributed on Multiple Computers**

You can distribute components on multiple computers to improve performance, availability, capacity, and security. You can use two or more computers and start the distribution by first distributing the gateway, then the Content Manager components, then the Application Tier components, and finally adding multiple Controller Web Services servers until you achieve optimal performance.
**Distributing Components in a Role-based Configuration**

You can distribute the gateway, the reporting components, and the Cognos 8 Controller data calculation and consolidation components on separate computers.

In the following diagram, the gateway is on a separate Web server computer. If the gateway is located outside the firewall, as in this configuration, you must also install the Controller Client Distribution Server on the gateway computer so it can communicate with the external clients. A separate computer serves as the reporting services server with Content Manager, Report Server, and related Cognos 8 components installed. Another computer serves as the Controller Web server with the Controller Web Services Server installed to do the data consolidations and the Controller Client Distribution Server installed to communicate with the internal clients.

The report modeler computer has Cognos 8 Framework Manager installed for using or customizing the Publish to Data Mart Framework Manager model provided with Controller.

**Configuration Requirements**

When you distribute the Cognos 8 Controller components, configure them so that they can access the required components on other computers. On each computer, you must configure properties and set up virtual directories.
Chapter 2: Distribution Options for Cognos 8 Controller

On the Controller Web server, use Cognos Controller Configuration to configure the URIs for Report Server and the dispatcher, and to specify connection information for the Cognos Controller database. Use Internet Information Services (IIS) to create the following virtual directories:

- /cognos8
- /cognos8/controllerbin
- /cognos8/controller
- /cognos8/controllerServer
- /cognos8/controllerHelp

On the reporting services server, use Cognos Configuration to specify connection information for the content store, and to configure the URI for Controller Client Distribution Server.

On the gateway computer, use Cognos Configuration to configure the URIs for the gateway and the dispatcher. Use Cognos Controller Configuration to configure the CASUrl, WSSUrl, and HelpUrl. Use IIS to create the following virtual directories:

- /cognos8
- /cognos8/cgi-bin
- /cognos8/controllerbin
- /cognos8/controller
- /cognos8/controllerHelp

On the client computers, download the Microsoft .NET Runtime Security Policy, after you export it from the Controller Client Distribution Server.

**Distributing Components for Load Balancing of the Consolidation Functions**

You can build on the previous distribution example and further balance the load for the calculation and consolidation functions of Cognos 8 Controller. In this example, you install Controller Web Services Server on two computers and then move the COM+ components that are used for consolidation to the second computer. The first computer serves as a request server and accepts user requests, but it does not perform consolidation tasks. You also install the Controller Client Distribution Server on this computer to communicate with the internal clients. The second computer serves as the consolidation server and does all the data calculations.

In the following diagram, the components are distributed across several computers, and two computers are set up for consolidation load balancing.
Configuration Requirements

When you distribute components on several computers, configure the components so that they can access the required components on the other computers. On each computer, you must configure properties and set up virtual directories.

On the reporting services server, use Cognos Configuration to specify connection information for the content store, and to configure the URIs for Controller Client Distribution Server, the dispatcher, and the gateway.

On the Controller Web Services Server computer that is used as the request server, use Cognos Controller Configuration to configure the URIs for Report Server and the dispatcher, and to specify connection information for the Cognos Controller database and the Controller data mart database. Use the Component Services tool in Administrative Tools to configure load balancing between the Controller request server and the Controller consolidation server. Because this computer also has the Controller Client Distribution Server installed, use Microsoft .NET Framework Configuration to create a Runtime Security Policy. Use IIS to create the following virtual directories:

- `/cognos8`
- `/cognos8/controllerbin`
- `/cognos8/controller`
- `/cognos8/controllerServer`
- `/cognos8/controllerHelp`
On the gateway server, use Cognos Configuration to configure the URIs for the gateway and the dispatcher. Use Cognos Controller Configuration to configure the CASUrl, WSSUrl, and HelpUrl. Use IIS to create the following virtual directories:

- /cognos8
- /cognos8/cgi-bin
- /cognos8/controllerbin
- /cognos8/controller
- /cognos8/controllerHelp

On the client computers, download the Microsoft .NET Runtime Security Policy, after you export it from the Controller Client Distribution Server.

**Integrating Cognos8 Controller with Other Cognos 8 Products**

You can install Cognos 8 Controller in an environment that includes other Cognos 8 products and benefit from sharing the same security settings and sharing many tools, such as Report Studio.

Cognos 8 Controller and Cognos 8 Business Intelligence products can share components of the same version, such as the Content Store and gateway.

*Note:* If you install any Cognos 8 Controller component on a shared Cognos 8 gateway, the gateway must be on a Windows computer. Cognos 8 Controller can interoperate with a non-Windows gateway on a separate computer, but you cannot install Controller components, for example, the Controller Distribution Server, on a non-Windows computer.

Cognos 8 Business Intelligence users can access published Controller data and structures for analysis and reporting using Framework Manager and Report Studio. The Publish to Data Mart feature in Cognos 8 Controller publishes Controller data to the Controller data mart for access by a Framework Manager model.

Cognos 8 Controller users can import published data from Cognos BI applications by using the Import from Framework Manager function in Cognos 8 Controller.

With the Cognos 8 Controller OLAP extension, you can create an OLAP cube of Controller data that can be used by Cognos 8 Business Intelligence users.

Cognos 8 Controller users can prepare actual values for export to Cognos 8 Planning – Contributor so that the data can be used in the planning process. The Send to Application function in Cognos 8 Controller creates a Microsoft Excel spreadsheet for import to external applications.

Cognos 8 Controller users can also import plans from Contributor so that the data can be consolidated. The necessary stored procedures and staging tables to do this import are in the Controller database and are delivered with Cognos 8 Controller. The Import from Flat Files feature in Cognos 8 Controller imports data from spreadsheets and text files.

**Accessing Product Documentation in an Integrated Environment**

The documentation for Cognos 8 components is installed with the gateway component. If you integrate different 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 Cognos 8 gateway component for each product into the same location on the same computer. This ensures that all of the product documentation is available to all users. If you want to use separate gateways for each product, you can install the Cognos 8 gateway component for each product on separate computers, but the product documentation on each gateway will be specific for the Cognos 8 product you installed.

For example, you have Cognos 8 Business Intelligence and Cognos 8 Controller installed using separate gateways but sharing the same content store. When users access Cognos Connection, both Report Studio and Controller are available, assuming they have permission for both components. If users access Report Studio through the Cognos 8 Business Intelligence gateway, they are able to use the component and access the documentation for that component. However, if users access Report Studio through the Cognos 8 Controller gateway, they are able to use the component but do not have access to the Report Studio documentation.
If you want users to access each Cognos 8 product through separate gateways, yet still be able to access documentation for all components, you can install each product's gateway component into the same location as your other Cognos 8 gateway components.
Chapter 3: Workflows for Cognos 8 Controller

After you decide on the appropriate distribution options (p. 13) for your environment, you must follow a specific workflow to install and configure Cognos 8 Controller. For example, follow one workflow to install and configure Cognos 8 Controller on a single computer. Follow another workflow to install and configure Cognos 8 Controller in a distributed installation.

The workflows require that you perform tasks in sequence. Many of the tasks you perform for distributed installations are the same as those you perform for single-computer installations. However, additional tasks are required for distributed installations so that the components can communicate with each other.

For a distributed installation, you follow the workflow from beginning to end on one computer, installing and configuring the appropriate components, and then begin the workflow again for the next computer.

These workflows show the required tasks for installing and configuring on a single computer and in a distributed installation. We recommend that you print the workflow you plan to use. You can then use the printed copy as a checklist to ensure that you have completed all tasks.
Chapter 3: Workflows for Cognos 8 Controller

Single-Computer Installation

Install
- Install Microsoft .NET Framework and SDK
- Install and configure ASP.NET
- Install Cognos 8 Controller
- Check default settings

Set up environment
- Create Cognos Controller database
- Create content store database
- Set up database client for content store
- Create Controller data mart database
- Update Java environment

Configure
- Set database connection properties for content store
- Test reporting components installation and configuration
- Set database connection properties for Controller database
- Set database connection properties for Controller data mart
- Import the Controller standard reports package
- Define data source for Controller data mart
- Extract Controller data mart model and publish package
- Configure COM+ Server
- Test Cognos 8 Controller installation and configuration
- Finish configuration

Distributed Installation

You must start the services on the computer where Content Manager is installed before starting services on any other computer. We also recommend that you install, configure, start, and test the remaining gateway and reporting components before you add the Controller Web Services Server and the Controller Client Distribution Server.
Chapter 3: Workflows for Cognos 8 Controller

Content Manager, Gateway, and Reporting Components

Install
- Install database API for reporting database on Report Server computer
- Install database client software for content store on Content Manager computer
- Install Content Manager, the gateway, and reporting components on two or more computers
- Install Framework Manager
- Check default settings

Set up environment
- Create content store database
- Set up database clients for content store
- Update Java environment
- Configure Web server
- Configure Web browsers

Configure
- Configure the Content Manager computer, including the authentication namespace, and start the services.
- Configure Report Server computers, including the authentication namespace
- Configure gateway computers
- Configure Framework Manager computer
- Test reporting components and Framework Manager installation and configuration
Chapter 3: Workflows for Cognos 8 Controller

Controller Components
Install
- Install database API for reporting database on Web Services Server computers
- Install Microsoft .NET Framework and SDK
- Install and configure ASP.NET
- Install Cognos 8 Controller components on two or more computers
- Check default settings

Set up environment
- Create Cognos Controller database
- Create Controller data mart database
- Configure Microsoft .NET Framework
- Configure Web server

Configure
- Configure Web Services Server computers, including the authentication method
- Configure Client Distribution Server computers, including the authentication method
- Import Cognos Controller standard reports package
- Define data source for Controller data mart
- Extract Controller data mart model and publish package
- Test Cognos 8 Controller installation and configuration
- Finish Configuration
You can upgrade from any previous version of Cognos 8 Controller to Version 8.2.

If you installed Cognos 8 Controller with other Cognos 8 products such as Cognos 8 Business Intelligence or Cognos 8 Planning, upgrading is supported when all products are at the same version. You must upgrade Cognos 8 Business Intelligence before upgrading Cognos 8 Controller. For information about upgrading Cognos 8 Business Intelligence, see the Cognos 8 Business Intelligence Installation and Configuration Guide.

You can upgrade by replacing components in the same directory or by installing the new version of Cognos 8 Controller in a separate directory on the same computer or on a separate computer.

When you upgrade to the same directory as an older version or when you upgrade to a new directory on the same computer, you back up your data, uninstall the older version, install the new version and configure it to use the same databases as the older version, and then upgrade the databases.

When you upgrade to a new computer, you back up your data, install the new version, configure it to use copies of the databases from the older version, and then upgrade the databases. After the new version is operating, you can uninstall the old version. For more information, see "Upgrading to a New Computer" (p. 30).

Use the following checklist to guide you through the tasks to upgrade in the same directory or in a different directory on the same computer:

- Install or upgrade third-party products
- Back up your application data
- Uninstall the older version of Cognos 8 Controller
- Install the new version of Cognos 8 Controller
- Apply the configuration
- Upgrade your application databases
- Upgrade your data entry forms
- Upgrade the user-defined reports
- Upgrade the Excel link report formulas
- Upgrade the consolidation model, if required

After upgrading, there may be additional installation and configuration required to use new features. For example, if you want to use the Publish to Data Mart Framework Manager model, you must also install (p. 38) and configure (p. 66) Cognos 8 Framework Manager, set up a database (p. 46) and define a data source (p. 58) for the Controller data mart, and then extract and publish the Framework Manager model to Cognos Connection (p. 59).

Install or Upgrade Third-party Products

When you upgrade Cognos 8 Controller, you may need to upgrade to new versions of third-party products or install additional third-party products to support new features in Cognos 8 Controller.

To view a list of third-party products that are used by Cognos 8 Controller, see "Confirm System Requirements" (p. 31).

To review an up-to-date list of environments supported by 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).
Step

- If you do not have the supported version of a required third-party product, install or upgrade the product.

Instructions are provided in this guide for some of the required third-party products:

- installing Microsoft .NET Framework (p. 35)
- installing Microsoft .NET Framework SDK (p. 35)
- installing and configuring ASP.NET (p. 35)
- setting up a database client (p. 45)
- configuring a Web server (p. 47)
- configuring a Web browser (p. 50)

For instructions to install or upgrade other third-party products, see the instructions provided with each product.

Back Up Your Application Data

Before you upgrade Cognos 8 Controller, we recommend that you back up your application data and make copies of your application uniform data language (UDL) files in a secure location.

If your normal production procedures include backing up data, you may want to schedule your upgrade after you perform a regular backup.

For information about backing up your database system, see the documentation for your database application.

Uninstall the Older Version of Cognos 8 Controller

You must uninstall the older version of Cognos 8 Controller before you can install a new version. Different versions of Cognos 8 Controller cannot exist on the same computer due to resource conflicts.

You can keep the older version of Cognos 8 Controller if you install the new version on a separate computer. For more information, see "Upgrading to a New Computer" (p. 30).

Steps

1. From the Start menu, click Programs, Cognos 8, Uninstall Cognos 8, Uninstall Cognos 8.
2. Follow the instructions to uninstall the components.
   The cognos_uninst_log.htm file, in the Temp directory, records the activities that the Uninstall wizard performs.

Install the New Version of Cognos 8 Controller

The process for installing the new version of Cognos 8 Controller is the same as for a new installation.

We recommend that you install the new components in the same location from which you uninstalled the older version. Ensure that you have uninstalled the older version first. If you want to keep the older version running until you switch over to the new version, you can install the new version on a separate computer. For more information, see "Upgrading to a New Computer" (p. 30).

Steps

1. Insert the Cognos 8 Controller CD and then open the installation menu.
   The Welcome page of the installation wizard should appear.
   If no Welcome page appears, in the win32 directory on the CD, double-click the issetup.exe file.
2. In the Welcome page of the installation wizard, click Next.
3. Accept the licensing agreement and then click Next.
4. Select the installation directory and then click Next.
   If you receive a warning that you are installing to the same location as a previous installation, click No and then ensure that you select the correct directory and that you uninstalled the older version of Cognos 8 Controller. This warning protects other Cognos 8 products from being overwritten.
5. Follow the directions in the installation wizard to copy the same components to your computer that were installed for the older version.
6. In the Finish page of the installation wizard, choose whether to start Cognos Configuration or view the Readme and then click Finish.

You must now apply the new configuration.

**Apply the New Configuration**

Before you can use the new version of Cognos 8 Controller, you must save the configuration so that the content store is upgraded. Even if you do not change any configuration settings, you must still save the configuration.

**Steps**
1. If it is not already running, start Cognos Configuration.
2. If you want to change any settings, do the following:
   - In the Explorer window, click the node for the component that you want to configure.
   - In the Properties window, change the settings as required.
3. From the File menu, click Save.

**Upgrade Your Application Databases**

When you upgrade from an older version of Cognos 8 Controller, you must upgrade your Controller application databases.

You perform the database upgrade by using the database conversion utility to import new data structures into the existing database that is specified in the Controller UDL file.

Tip: For Oracle databases, after completing the database upgrade, we recommend that you schedule a performance optimization procedure, prc_analyze_schema, to run on a weekly basis.

**Steps to Upgrade the Controller Database**
1. From the Start menu, start Cognos Controller Configuration.
2. In the Explorer window, expand Database Connections.
3. Select the database that you want to upgrade.
4. From the Actions menu, click Run.
5. In the Database Conversion Utility window, click Run Steps.
   The database conversion utility upgrades the existing database with the new data structures.
6. Click Close.

**Schedule a Performance Optimization Procedure for an Oracle Controller Database**

Cognos 8 Controller provides an SQL procedure that analysis the schema in the Controller database and gathers the appropriate statistics, which Oracle requires for optimal performance. This procedure can be run by the Controller user, but we recommend that you create a job to run it automatically on a weekly basis.
Chapter 4: Upgrading Cognos 8 Controller

Steps
1. Create a file and add the following command lines:

   SQL> DECLARE JOB BINARY_INTEGER;
   BEGIN
   DBMS_SCHEDULER.create_job (  
   job_name => 'Analyze_Controller_Schema_week',
   job_type => 'PLSQL_BLOCK',
   job_action => 'BEGIN PRC_ANALYZE_SCHEMA; END;',
   start_date => SYSTIMESTAMP,
   repeat_interval => 'freq=weekly; byday=sat; byhour=9; byminute=0; bysecond=0;',
   end_date => NULL,
   enabled => TRUE,
   comments => 'Analyze schema job to be run Saturdays 9:00 AM');
   END;

2. Run the file on a weekly basis.

Upgrade the Data Entry Forms

If you upgrade to Cognos 8 Controller from an earlier version of the product, or you migrate data from Consolidator, you must upgrade your existing data entry forms to the new product design.

The data entry form conversion utility converts the forms as they were designed, with row and column definitions, layout, and formatting, so that the forms retain the original functionality and appearance. However, if the standard colors were redefined in Consolidator, the colors revert to the original standard colors used in Cognos 8 Controller.

If a matrix form contains more than two languages, only the current locale and group languages will be available in the converted form.

Because forms that were invalid before the upgrade remain invalid after the upgrade, you should correct invalid forms prior to the upgrade.

To run the data entry form conversion utility in Microsoft Excel, you

- must use Microsoft Excel 2000
- must have installed the Cognos 8 Controller Add-in for Excel

Steps
1. On the computers where Controller Client Distribution Server is installed, open Windows Explorer.
2. Go to the $c8_location\webcontent\ccr directory.
3. Copy the Controllerconv.msi file to a location that is accessible to Cognos 8 Controller client computers.
4. On a Cognos 8 Controller client computer, run the utility.
5. Start Cognos 8 Controller.
6. From the Maintain menu, click Special Utilities, Convert, Forms to New Design.
7. Click Run.
8. Repeat steps 4 to 7 for each database.

Upgrade the User-defined Reports

If you upgrade to Cognos 8 Controller from an earlier version of the product, or you migrate data from Consolidator, you must upgrade your existing user-defined reports to the new design before you run the reports.

For more information about upgrading user-defined reports, contact your Cognos consultant.
Steps
1. Start Cognos 8 Controller.
2. If you are not already in single user mode, from the Maintain menu, click User, Single Mode.
3. From the Maintain menu, click Special Utilities, Convert, Reports to New Design.

Upgrade the Excel Link Report Formulas

If you upgrade to Cognos 8 Controller from an earlier version of the product, or you migrate data from Consolidator, you must upgrade your existing Excel Link reports to the current version of Cognos 8 Controller.

For more information about upgrading Excel Link report formulas, contact your Cognos consultant.

Steps
1. In Microsoft Excel, log on to Cognos 8 Controller.
2. Open an existing workbook.
3. Ensure that
   - the first worksheet in the workbook is active
   - the workbook and worksheets are not protected
4. From the Controller menu, click Reports, Convert Workbook.
5. When asked to confirm, click Yes.
   When the conversion process is complete, the following message appears:
   Workbook has been successfully converted.

Upgrade the Consolidation Model

By default, Cognos 8 Controller uses the Cognos Controller 8.1 consolidation model to consolidate your financial data. If you used this model in your previous version of Cognos Controller and want to keep using it, no changes are required.

If you used the Cognos Controller 2.3 consolidation model in your previous version of Cognos Controller, we recommend that you change to the Cognos Controller 8.1 consolidation model. Although the older model provides a contribution view of the lowest level against the highest level, it has limitations when handling complex ownership structures. The newer model provides a more detailed method of handling complex ownership structures for all customers and facilitates migration to Cognos 8 Controller from the Consolidator consolidation application. In addition, the new model is required to support all new features in Cognos 8 Controller.

For more information about the Cognos 8 Controller consolidation models, see the Cognos 8 Controller New Features Guide, or contact your Cognos consultant.

Step to Change to the Cognos Controller 8.1 Consolidation Model
- If you were using the Cognos Controller 2.3 consolidation model with your previous version of Cognos Controller and want to use the new consolidation model, you must perform an upgrade procedure.
  For more information, see your Cognos consultant.

Steps to Continue Using the Cognos Controller 2.3 Consolidation Model
1. Using a Cognos Controller administrative user account, start Cognos 8 Controller.
2. From the Maintain menu, click General Configuration.
3. On the Server Preference tab, change the value for the CONS-BY-LEVEL variable to False.
Upgrading to a New Computer

You can install a new version of Cognos 8 Controller on a separate computer and configure it to use your existing data. Using this as a staging environment, you can test your reports with the new product. You can continue to run the older version of Cognos 8 Controller in your production environment. When the new version is operating and fully tested, you can switch your production environment to the new version and then uninstall the old version.

To configure the new version of Cognos 8 Controller to use your existing data, you must create copies of the databases and then configure the new version to use the copies. Then you must upgrade your databases.

Use the following checklist to guide you through the tasks to upgrade on a separate computer:

- Using your database tools, create copies of your existing databases:
  - content store database
  - Controller data source

- Install the new version of Cognos 8 Controller (p. 31) on the new computer.
  
  If you do not accept the default installation location, be sure to use only ASCII characters in the name of any new installation directory you create.

- Configure a new set of Web server aliases (p. 47) for Cognos 8 Controller.

- Configure Cognos 8 Controller (p. 53), using the following requirements:
  - Configure the Content Manager computer to use the copy of your content store database (p. 56).
  - Configure the Controller Web Services Server computers to use the copy of your Controller data source (p. 69).

- Upgrade your application databases (p. 27).

- Upgrade your data entry forms (p. 28).

- Upgrade the user-defined reports (p. 28).

- Upgrade the Excel link report formulas (p. 29).

- Upgrade the consolidation model (p. 29), if required.

- Test the new version with existing reports.

After upgrading, there may be additional installation and configuration required to use new features. For example, if you want to use the Publish to Data Mart Framework Manager model, you must also install (p. 38) and configure (p. 66) Cognos 8 Framework Manager, set up a database (p. 46) and define a data source (p. 58) for the Controller data mart, and then extract and publish the Framework Manager model to Cognos Connection (p. 59).
Chapter 5: Installing Cognos 8 Controller

There are several tasks that you should perform before you install Cognos 8 Controller. After these tasks are complete, you can install the Cognos 8 Controller server components. After you install Cognos 8 Controller, you must set up your environment.

Use the following checklist to guide you through the installation tasks:

- Ensure that your computer meets the software and hardware requirements
- Review the Cognos 8 Controller supported environments
- Set up the database connectivity for the reporting database
- Set up the database connectivity for the content store database
- Set up the database connectivity for the data mart database
- Install Microsoft .NET Framework
- Install Microsoft .NET Framework SDK
- Install and configure ASP.NET
- Install Cognos 8 Controller Server Components
- Install the Cognos 8 Controller Client and Add-in for Excel, if required
- Install Framework Manager, if required

If you no longer require Cognos 8 Controller, you can uninstall all Cognos 8 Controller components.

Confirm System Requirements

Ensure that your computer meets the minimum hardware and software requirements to run Cognos 8 Controller. The hardware requirements depend on your Cognos environment. You may require additional resources, such as disk space.

Step

- Use the following table to check the requirement specifications.

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Windows 2003 Enterprise Edition</td>
</tr>
<tr>
<td></td>
<td>The following Windows components must be installed:</td>
</tr>
<tr>
<td></td>
<td>• Windows Support Tools</td>
</tr>
<tr>
<td></td>
<td>• Windows Scripting Host</td>
</tr>
<tr>
<td>RAM</td>
<td>Minimum: 1 GB</td>
</tr>
<tr>
<td>Disk space</td>
<td>Minimum: 1.5 GB</td>
</tr>
<tr>
<td>Web server</td>
<td>Microsoft Internet Information Services (IIS)</td>
</tr>
<tr>
<td></td>
<td>• IIS must have ASP.NET enabled.</td>
</tr>
<tr>
<td>JRE</td>
<td>Java Runtime Environment (JRE)</td>
</tr>
<tr>
<td></td>
<td>JRE is installed automatically with Cognos 8 Controller.</td>
</tr>
</tbody>
</table>
Chapter 5: Installing Cognos 8 Controller

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Specification</th>
</tr>
</thead>
</table>
| Database            | One of the following databases available to store Cognos data:  
|                     |   • Oracle  
|                     |   • DB2  
|                     |   • Microsoft SQL Server  
|                     |   • TCP/IP connectivity to Microsoft SQL Server  
|                     |   • Sybase  
|                     | One of the following databases available to store Cognos 8 Controller data:  
|                     |   • Oracle  
|                     |   • Microsoft SQL Server  
|                     | One of the following databases available to use as the Controller data mart, if required:  
|                     |   • Oracle  
|                     |   • Microsoft SQL Server  
|                     | For a minimal installation of Oracle Client, the following components are required:  
|                     |   • Oracle Network Utilities  
|                     |   • Oracle Database Utilities  
|                     |   • SQL* Plus  
|                     |   • Oracle JDBC/OCI Interface  
|                     |   • Oracle Windows Interface  
| Web browser         | Microsoft Internet Explorer  
|                     | The following settings must be enabled:  
|                     |   • cookies  
|                     |   • JavaScript  
|                     |   • Active scripting  
|                     |   • Allow META REFRESH  

32 Cognos 8 Controller
Review Supported Environments

To ensure your product works properly, apply all required operating system patches and use only the versions of third-party software that are supported for a Cognos product.

Step
- View an up-to-date list of software environments supported by Cognos products, such as operating systems, patches, browsers, Web servers, directory servers, database servers, and application servers, on the Cognos Global Customer Services Web site (http://support.cognos.com).

Set Up Database Connectivity for the Reporting Database

For Cognos 8 Controller, both Controller Web Services Server and Report Server access the Controller database, which is also known as the reporting database. The Web server must be able to connect to the reporting database.

Step
- Install the database API software for your reporting sources on each Controller Web Services Server and Report Server computer.
  
  For more information, see the documentation for your database API software.
Chapter 5: Installing Cognos 8 Controller

Set Up Database Connectivity for the Content Store Database

If you are using a database other than Cognos Content Database as the content store, database client software must be installed and configured on each computer where you install Content Manager.

**Step**

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

<table>
<thead>
<tr>
<th>Database</th>
<th>JDBC Driver</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle</td>
<td>JDBC thin driver, ojdbc14.jar</td>
</tr>
<tr>
<td></td>
<td>If the directory contains the classes12.jar file, you must delete it before installing the ojdbc14.jar file.</td>
</tr>
<tr>
<td>DB2</td>
<td>JDBC driver that requires DB2 client installation</td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>Included with Cognos components. No other software is required.</td>
</tr>
<tr>
<td></td>
<td>Cognos 8 requires TCP/IP connectivity with Microsoft SQL Server.</td>
</tr>
<tr>
<td>Sybase</td>
<td>JDBC driver, jconn2.jar</td>
</tr>
<tr>
<td>Cognos Content Database</td>
<td>Included with Cognos components. No other software is required.</td>
</tr>
</tbody>
</table>

Set Up Database Connectivity for the Controller Data Mart

If you use a different type of database for the Controller data mart than you use for the content store, then you must set up connectivity to the Controller data mart. A Controller data mart database is required only if you intend to use the Publish to Data Mart Framework Manager model that is provided with Cognos 8 Controller.

**Step**

- Install the appropriate JDBC driver for your Controller data mart, as follows:

<table>
<thead>
<tr>
<th>Database</th>
<th>JDBC Driver</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle</td>
<td>JDBC thin driver, ojdbc14.jar</td>
</tr>
<tr>
<td>DB2</td>
<td>JDBC driver that requires DB2 client installation</td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>Included with Cognos components. No other software is required.</td>
</tr>
<tr>
<td></td>
<td>Cognos 8 requires TCP/IP connectivity with Microsoft SQL Server.</td>
</tr>
<tr>
<td>Sybase</td>
<td>JDBC driver, jconn2.jar</td>
</tr>
<tr>
<td>Cognos Content Database</td>
<td>Included with Cognos components. No other software is required.</td>
</tr>
</tbody>
</table>
Install Microsoft .NET Framework

Microsoft .NET Framework supports smart client technology that allows applications to be started using a URL and downloaded from a server.

Microsoft .NET Framework must be installed on the Controller Client Distribution Server computers, the Controller Web Services Server computers, and on all Cognos 8 Controller client computers.

Tip: To view up-to-date product information, such as supported versions for third-party software, visit the Cognos Global Customer Services Web site (http://support.cognos.com).

Step
• If you do not already have Microsoft .NET Framework installed, go to the Microsoft .NET Framework Web page and follow the download instructions.

Install Microsoft .NET Framework SDK

The Microsoft .NET Framework SDK is required if you want to use the graphical user interface administrative tool, .NET Framework Configuration, to configure the .NET Framework security policy (p. 48). It provides convenient alternative to using the command line interface that is available by default with Microsoft .NET Framework.

We recommend that you install the SDK on the Controller Client Distribution Server computers because this is the most convenient place to configure the security policy, which is then distributed to all the Cognos 8 Controller client computers.

Tip: To view up-to-date product information, such as supported versions for third-party software, visit the Cognos Global Customer Services Web site (http://support.cognos.com).

Step
• If you do not already have Microsoft .NET Framework SDK installed, go to the Microsoft .NET Framework Web page and follow the download instructions.

Install and Configure ASP.NET

ASP.NET is a Microsoft Internet Information Services (IIS) extension that is bundled with the Microsoft .NET Framework. You must install and configure ASP.NET on all computers where Controller Web Services Server and Controller Client Distribution Server are installed.

Steps
1. In a Command Prompt window, go to c:/Windows/Microsoft.NET/Framework/v2.0.50727
2. Run aspnet_regiis.exe /i
3. In Administrative Tools, start Internet Information Services (IIS).
4. In the left pane, expand Internet Information Services, (local computer), Web Service Extensions.
5. In the right pane, click ASP.NET v2.0, and then click the Allow button.
6. Click All Unknown CGI Extensions, and then click the Allow button.

Install Cognos 8 Controller Server Components

Use the installation wizard to select the components that you want to install and the location on your computer where you want to install them. If you plan to install two or more Cognos 8 Controller components on the same computer, we strongly recommend that you install them in the same installation location to avoid conflicts among ports and other default settings. Only the components that you choose to install are copied from the CD to your computer.

You can install the gateway and Application Tier components on multiple computers.
Chapter 5: Installing Cognos 8 Controller

**Important:** Although the gateway and Controller Client Distribution Server can be installed on separate computers in a distributed installation, we recommend that these two components be installed on the same computer. When Controller Client Distribution Server is installed on a different computer from the gateway or Report Server, additional configuration is required.

The installation wizard for Cognos 8 Controller is provided on the installation CDs.

Ensure that you have administrator privileges for the Windows computer that you are installing on. 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.

### Where to Install Cognos 8 Controller Relative to Other Cognos 8 Products

You can install Cognos 8 Controller in the same location where other Cognos 8 products of the same version are installed. This is the typical scenario in a single-computer installation. For a distributed installation, you can also choose to install components to the directory where the same component from another Cognos 8 product is located. You can, however, also achieve integration by installing Cognos 8 Controller in a separate location and then sharing some common resources, such as the content store. Installing Cognos 8 Controller in a separate location from other Cognos 8 products allows you more flexibility for upgrading each product independently.

If Cognos 8 Controller is in a separate directory from other Cognos 8 products and you intend to use it independent of the other Cognos 8 products, you must configure a different content store and a different set of ports and URLs for the Cognos 8 Controller installation.

### Steps

1. Insert the Cognos 8 Controller CD and then open the installation menu.
   
   The **Welcome** page of the installation wizard should appear.
   
   If no **Welcome** page appears, in the win32 directory on the CD, double-click the issetup.exe file.

2. In the **Welcome** page of the installation wizard, click **Next**.

3. If you are installing Cognos 8 Controller in the same location as another Cognos 8 installation, the following warning appears:
   
   **You are installing to the same location as a previous installation. Do you want to continue?**
   
   - If this is a single-computer installation, click **Yes**.
     
     If this is a distributed installation, you can also click **Yes** if this is the way you want to integrate Cognos 8 Controller with an existing Cognos 8 installation.
   
   - If you want the flexibility of managing the Cognos 8 Controller upgrades independently of the Cognos 8 upgrades, click **No**, and choose a different installation directory.

   **Note:** If you do not accept the default installation location, be sure to use only ASCII characters in the name of any new installation directory you create.

4. Follow the directions in the installation wizard to copy the required files to your computer:
   
   - To install all components on one computer, on the **Component Selection** page, select all the components listed.
     
     **Tip:** To distribute components on multiple computers, we recommend that you first install the Content Manager, the reporting components, and the gateway:
   
   - To install Content Manager, on the **Component Selection** page, select **Content Manager Components**. Clear all the other components.
   
   - To install the Application Tier Components for reporting, on the **Component Selection** page, under **Application Tier Components**, select **Report Server** and Cognos Connection Integration Enabler. Clear all the other components.
   
   - To install the gateway, on the **Component Selection** page, under **Gateway Components**, select **Gateway** and **Gateway Integration Enabler**. Clear all the other components.

   **Tip:** We recommend that you configure and test the components that you already installed before continuing with the installation of the remaining Cognos 8 Controller components.
• To install the Client Distribution Server, on the Component Selection page, under Gateway Components, select Controller Client Distribution Server. Clear all the other components.

• To install the Web Services Server, on the Component Selection page, under Application Tier Components, select Controller Web Services Server. Clear all the other components.

5. In the Finish page of the installation wizard, do one of the following:
   • If you want to change any default settings immediately, click Start Cognos Configuration.
   • If you want to see late-breaking information about Cognos components, click View the Readme.

6. Click Finish.
   Use the Windows Start menu to start Cognos Configuration from the shortcut folder.

**Default Settings for Cognos 8 Controller**

The following table lists the default ports and URI settings for the gateway, Content Manager, and Report Server. After installation, you can use Cognos Configuration to change the settings (p. 76). You can also change them by editing the cogstartup.xml file in the c8_location/configuration directory.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content Manager URI</td>
<td><a href="http://localhost:9300/p2pd/servlet">http://localhost:9300/p2pd/servlet</a></td>
<td>The URI to Content Manager</td>
</tr>
<tr>
<td>Gateway URI</td>
<td><a href="http://localhost:80/cognos8/cgi-bin/cognos.cgi">http://localhost:80/cognos8/cgi-bin/cognos.cgi</a></td>
<td>The URI to the gateway</td>
</tr>
<tr>
<td>Dispatcher URI (Internal)</td>
<td><a href="http://localhost:9300/p2pd/servlet/dispatch">http://localhost:9300/p2pd/servlet/dispatch</a></td>
<td>The URI to the dispatcher</td>
</tr>
<tr>
<td>Dispatcher URI (External)</td>
<td><a href="http://localhost:9300/p2pd/servlet/dispatch">http://localhost:9300/p2pd/servlet/dispatch</a></td>
<td>The URI to the dispatcher</td>
</tr>
<tr>
<td>Dispatcher URIs for gateway</td>
<td><a href="http://localhost:9300/p2pd/servlet/dispatch/ext">http://localhost:9300/p2pd/servlet/dispatch/ext</a></td>
<td>The URI to the primary dispatcher used by the gateway</td>
</tr>
<tr>
<td>Controller URI for gateway</td>
<td><a href="http://localhost:80/cognos8/controllerserver">http://localhost:80/cognos8/controllerserver</a></td>
<td>The URI to Controller Web Services Server used by the gateway</td>
</tr>
<tr>
<td>Log server port</td>
<td>9362</td>
<td>The port used by the local log server</td>
</tr>
</tbody>
</table>

The following table lists default URI settings for Controller Web Services Server and Controller Client Distribution Server. After installation, you can use Cognos Controller Configuration to change the settings (p. 76).

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Authentication,</td>
<td><a href="http://localhost:9300/p2pd/servlet/dispatch">http://localhost:9300/p2pd/servlet/dispatch</a></td>
<td>The URI to the dispatcher used by Controller Web Services Server</td>
</tr>
<tr>
<td>Dispatcher URI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Report Server URI</td>
<td><a href="http://localhost/cognos8/cgi-bin/cognos.cgi">http://localhost/cognos8/cgi-bin/cognos.cgi</a></td>
<td>The URI to the Report Server used by Controller Web Services Server</td>
</tr>
</tbody>
</table>
Chapter 5: Installing Cognos 8 Controller

The following table lists the default settings used by Cognos 8 Controller for Tomcat. The non-SSL connector is automatically updated in the server.xml file when you use Cognos Configuration to change the dispatcher port (p. 76). You can directly update the shutdown port using Cognos Configuration.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
| CASURL                        | http://localhost/cognos8/contr
ollerbin                     | The Controller Client Distribution Server URI used by client downloads       |
| WSSURL                        | http://localhost/cognos8/contr
ollerserver                   | The Controller Web Services Server URI used by client downloads              |
| Controller online help URL    | http://localhost/cognos8/contr
ollerhelp                     | The URI to the Cognos 8 Controller online help used by client downloads       |

The following table lists the default settings used by Cognos 8 Controller for Tomcat. The non-SSL connector is automatically updated in the server.xml file when you use Cognos Configuration to change the dispatcher port (p. 76). You can directly update the shutdown port using Cognos Configuration.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-SSL Coyote HTTP/1.1</td>
<td>9300</td>
<td>The port Tomcat uses to pass requests from the Web server to Cognos 8</td>
</tr>
<tr>
<td>Connector</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shutdown port</td>
<td>9399</td>
<td>The port Tomcat uses to listen for a shutdown command</td>
</tr>
</tbody>
</table>

Install the Cognos 8 Controller Client and Add-In for Excel

Cognos 8 Controller provides an add-in for Microsoft Excel that is automatically downloaded, along with the Controller client, the first time users access Cognos 8 Controller. Users must have administrative privileges for their computers so that the Add-in for Excel can be downloaded. The Controller client will download in any case.

If your users do not have administrative privileges, you can install the Add-in for Excel remotely for them. For users who have slow network connections, you may prefer to copy the complete client installation package to CD and then distribute the CD for users to install.

Steps
1. On the computer where Controller Client Distribution Server is installed, go to the c8_location\webcontent\ccr directory.
2. To distribute the Add-in for Excel remotely to the Cognos 8 Controller client computers, run the ClientAdmin.msi file on Cognos 8 Controller client computers by using Active Directory or Patchlink.
3. To copy the complete client installation package to a CD or USB drive for installation by users:
   - Copy the CCRLocalClient.msi file from the ccr directory to your transportable media.
   - Users with administrative privileges can copy the client installation package from the media to their Cognos 8 Controller client computer and run the CCRLocalClient.msi file.

Install Framework Manager

To deploy the Publish to Data Mart Framework Manager model that is provided with Cognos 8 Controller, you must have an installation of Framework Manager.
You can install Framework Manager from the Cognos BI Modeling 8.2 CD provided with Cognos 8 Controller or use a Framework Manager installation from other Cognos 8 products.

**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 and the Application Tier Components are 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 Cognos 8. Error messages, sort order, date, time, monetary, numeric, and calendar conventions automatically adapt to the native language and locale.
   
   If the Application Tier Components are installed on a UNIX computer, the NLS_LANG variable must be set up for the user who owns and starts the Cognos 8 service.

2. If you are installing in a directory with other Cognos 8 components, stop the Cognos 8 service.

3. Insert the CD for your Cognos modeling product.
   
   The Welcome page of the installation wizard should appear.
   
   If no Welcome page appears, in the win32 directory on the CD, double-click the issetup.exe file.

4. Select the language to use for the installation.

5. 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 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 Cognos components immediately, click **Start Cognos Configuration**.
   
   - If you want to see late-breaking information about Cognos components, click **View the Readme**.

7. Click Finish.
   
   Use the Windows Start menu to start Cognos Configuration from the shortcut folder.

---

**Uninstall Cognos 8 Controller**

If you no longer require Cognos 8 Controller, uninstall all Cognos 8 Controller 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 Cognos 8 Controller. Otherwise, some files may not be removed.

**Steps**

1. From the Start menu, click **Programs, Cognos 8, Uninstall Cognos 8, Uninstall Cognos 8**.
   
   The Uninstall wizard appears.
   
   **Tip:** 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.
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.
Chapter 6: Setting Up the Environment

After you install Cognos 8 Controller, you must set up resources in your environment so that the components can operate. For example, you must ensure that a Java Runtime Environment (JRE) is available. You must ensure that a Web browser and a Web server are set up to provide access to Cognos components. If you use a router, you must configure it to support Cognos features.

If you want to use the Publish to Data Mart Framework Manager model, you must create an additional database for the Controller data mart.

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

- Create a Cognos Controller database.
- Create the content store.
- Set up the database client for the content store (Oracle, DB2 and Sybase).
- Create the Controller data mart database, if required.
- Update the Java environment, if required.
- Configure the Web server.
- Configure Microsoft .NET Framework.
- Configure the Web browser.
- Configure the router to test whether a dispatcher is available, if required.

After you complete these tasks, you must configure the Cognos components (p. 53) to work in your environment.

Create a Cognos Controller Database

If you are installing Cognos 8 Controller for the first time, you must create an empty Controller database. This is because Cognos 8 Controller requires a configured Controller database to run.

If you installed previous versions of Cognos 8 Controller and have established Controller databases, you do not need to create an empty database for Cognos 8 Controller to run. You can configure the Controller database connections using an existing Controller database.

**Important:** Before you configure existing Controller databases for use with Cognos 8 Controller, contact your Cognos consultant. Your Cognos consultant will discuss the Cognos 8 Controller consolidation models and possible database upgrade procedures.

Cognos Controller databases must be created using Oracle or Microsoft SQL Server.

**Tip:** To view up-to-date product information, such as supported versions for third-party software, visit the Cognos Global Customer Services Web site (http://support.cognos.com).

**Steps for Microsoft SQL Server**

1. If you performed a Typical installation of Microsoft SQL Server, after you install you must change the authentication mode to SQL Server and Windows.
   For more information, see the related knowledge base article on the Microsoft Web site.
2. Create the database.
   Ensure that the database collation sequence is case insensitive.
3. Determine which user account Controller Web Services Server will use to access the database.
4. Grant create table privileges for the database to the user account.
   Ensure that the user account is a member of the db_owner role.
Steps for Oracle

1. Determine whether the database is Unicode.
   Tip: One method is to type the following select statement:
   
   ```sql
   select * from NLS_DATABASE_PARAMETERS
   ```

2. If the result set returns an NLS_CHARACTERSET that is not Unicode, create a new database that uses a Windows 1252 character set such as WE8MSWIN1252.

3. Determine which user account Controller Web Services Server will use to access the database.

4. Grant the following privileges to the user account that accesses the database:
   - create session
   - alter session
   - create table
   - create database link
   - create sequence
   - create trigger
   - create view
   - create procedure
   - create materialized view
   - create synonym
   - create job
   - select_catalog_role
   - unlimited tablespace

5. Connect as `sys` and grant execute privileges to the user account for the DBMS_LOCK procedure.

6. Create a single tablespace and set it as the default tablespace for exclusive use by the user account that accesses the Controller database.

   Tip: You can increase the performance of your Oracle database by changing the default setting of the `optimizer_index_cost_adj` parameter in the `init.ora` file. We recommend that you change the default setting of 100 to a much smaller number, for example: `set optimizer_index_cost_adj = 5`

Create the Content Store

The content store is a database that Content Manager uses to store global configuration data and global Cognos 8 Controller settings (such as the language formats shown in Cognos Connection). Log files are not stored in the content store.

You must create this database using Oracle, Microsoft SQL Server, DB2, or Sybase Adaptive Server Enterprise (ASE).

   Tip: To view up-to-date product information, such as supported versions for third-party software, visit the Cognos Global Customer Services Web site (http://support.cognos.com).

An Oracle or Microsoft SQL Server database can use UTF-8 or UTF-16 encoding. A DB2 or Sybase database must use UTF-8 encoding. All database types must use the TCP/IP protocol, which is required by Cognos 8 to access data.

Content Manager 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.

   Tips:
   - Your database administrator must regularly back up the content store database because it contains the Cognos data.
   - To ensure the security and integrity of databases, it is also important to protect them from unauthorized or inappropriate access.
Steps for Microsoft SQL Server
1. Ensure that your installation of Microsoft SQL Server is configured with the following properties:
   • 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 Cognos 8 to access data.

2. Create the database.

3. If the content store database uses Windows authentication instead of SQL Server authentication, then you must ensure that SQL Server database (Windows Authentication) is selected as the database type for the content store in Cognos Configuration. For information, see (p. 63).

4. Determine which user account will be used to access the database.
   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 Cognos 8 instance is fully isolated from the others.

5. Grant create and drop table privileges for the database to the user account.
   Ensure that the user account’s database access roles include the db_ddladmin, db_datareader, and db_datawriter roles.
   Ensure that the user is the owner of their default schema.

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:
   ```sql
   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 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 appropriate environment variables for DB2.
Chapter 6: Setting Up the Environment

2. Determine if the database is Unicode by typing the following at the command prompt:
   `db2 get database configuration for database_name`
   The codepage is Unicode if it has a value of 1208.
3. If the codepage is not Unicode, create a new database that has a codepage value of 1208.
4. Ensure that you set the following configuration parameters.

<table>
<thead>
<tr>
<th>Environment variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DB2DIR</td>
<td>The top level directory that contains the database client software or the entire database installation.</td>
</tr>
<tr>
<td>DB2INSTANCE</td>
<td>The default database server connection.</td>
</tr>
<tr>
<td>DB2CODEPAGE</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 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 Content Store

If you use Oracle, DB2, or Sybase as the database server for the content store, additional steps are required after you install Cognos 8 Controller before you can configure it. You must set up the following on the Content Manager computer:

<table>
<thead>
<tr>
<th>Database</th>
<th>Additional steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle</td>
<td>Set up the JDBC driver.</td>
</tr>
<tr>
<td>DB2</td>
<td>Set up the database client software and the JDBC 2.0 driver.</td>
</tr>
<tr>
<td>Sybase</td>
<td>Set up the JDBC driver.</td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>The JSQLConnect.jar file is installed to the appropriate location by default and no additional steps are required.</td>
</tr>
</tbody>
</table>

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 to the c8_location/webapps/p2pd/WEB-INF/lib directory.
   This file includes the driver required by the content store.
   In a distributed installation, you must copy this file to the computers where Content Manager is installed.

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 automatically becomes the alias.

3. Stop the DB2 services and the HTML Search Server.

4. To copy the JDBC2 driver, copy the `DB2_installation/sqllib/java/db2java.zip` file to the `c8_location/webapps/p2pd/WEB-INF/lib` directory.

5. Rename the `db2java.zip` file to `db2java.jar`.

6. Restart the DB2 services and the HTML Search Server.

7. Repeat this entire procedure on the computers where Content Manager is installed.

You can tune the database to take advantage of DB2 features. For more information, see the Cognos 8 Controller 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.

   In a distributed installation, you must copy this file to the computers where Content Manager is installed.

If the installation is complete, some configuration tasks are required to ensure that Cognos 8 Controller (p. 53) works in your environment.

**Create a Controller Data Mart Database**

If you want to use the Publish to Data Mart Framework Manager model provided with Cognos 8 Controller, you must create an additional database to use for the Controller data mart.

The Controller data mart database must be created using Oracle or Microsoft SQL Server.

**Tip:** To view up-to-date product information, such as supported versions for third-party software, visit the Cognos Global Customer Services Web site (http://support.cognos.com).

**Steps for Microsoft SQL Server**

1. If you performed a Typical installation of Microsoft SQL Server, after you install you must change the authentication mode to **SQL Server and Windows**.

   For more information, see the related knowledge base article on the Microsoft Web site.

2. Create the database.

   Ensure that the database collation sequence is case insensitive.

3. Determine which user account Controller Web Services Server will use to access the database.

4. Grant the following privileges to the database to the user account.

   Ensure that the user account is a member of the db_owner role.

**Steps for Oracle**

1. Determine whether the database is Unicode.

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

   ```sql
   select * from NLS_DATABASE_PARAMETERS
   ```

2. If the result set returns an NLS_CHARACTERSET that is not Unicode, create a new database that uses a Windows 1252 character set such as WE8MSWIN1252.

3. Determine which user account Controller Web Services Server will use to access the database.

4. Grant the following privileges to the user account that accesses the database:

   - create session
   - alter session
   - create table
   - create database link
5. Create a tablespace and set it as the default tablespace for exclusive use by the user account that accesses the Controller data mart database.

Tip: You can increase the performance of your Oracle database by changing the default setting of the optimizer_index_cost_adj parameter in the init.ora file. We recommend that you change the default setting of 100 to a much smaller number, for example: set optimizer_index_cost_adj = 5

Update the Java Environment

Cognos 8 Controller cryptographic services use specific .jar (Java Archive) files in your Java Runtime Environment (JRE) to determine the allowed strength of the JRE. Cognos 8 Controller provides the necessary jurisdictional policy .jar files in case your JRE does not have the minimum requirements to require cryptographic strength.

If you do not have a JAVA_HOME variable already set or if JAVA_HOME points to a Java version that is not valid for Cognos 8 Controller, the JRE files provided with the installation will be used, and you do not have to update any files in your environment.

If you want to use your own JRE and have JAVA_HOME set to that location, you may have to update the Java environment for the cryptographic services.

The need to update your Java environment depends on the relative strength of jurisdictional policy .jar files in your environment. For example, if you already have stronger files in your environment than are provided with Cognos 8 Controller, you do not have to update the environment. Doing so, in this case, may cause other applications to not work correctly.

If you update your Java environment, it is recommended that you make a backup copy of the files you overwrite. If other applications fail, you may have to replace the original jurisdictional policy .jar files.

You can set JAVA_HOME as a system variable or a user variable. If you set it as a system variable, it may be necessary to restart your computer for it to take effect. If you set it as a user variable, set it so that the environment in which Tomcat is running can access it.

Java 1.3.1 is the minimum supported JRE for Cognos 8. Ensure that you installed the correct JRE for the hardware that you are using. The encryption .jar files provided with the installation are for Java 1.4.2. These files will not work with Java 1.3.1.

Step

Ensure that the JAVA_HOME environment variable is set to the JRE location.

For example, to set JAVA_HOME to the JRE files provided with the installation, the path is c8_location/bin/jre/version.

Configure the Web Server

Before you can use Web pages generated by Cognos 8 Controller, you must configure your Web server. You must set up virtual directories, also known as Web aliases, for the directories that contain the HTML and Web files for Cognos 8 Controller.
### Steps

1. Create the following virtual directories:

<table>
<thead>
<tr>
<th>Alias</th>
<th>Location</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>cognos8</td>
<td>c8_location/webcontent</td>
<td>Read</td>
</tr>
<tr>
<td>cognos8/cgi-bin</td>
<td>c8_location/cgi-bin</td>
<td>Execute</td>
</tr>
<tr>
<td>cognos8/controllerbin</td>
<td>c8_location/webcontent/ccr</td>
<td>Read</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Run scripts</td>
</tr>
<tr>
<td>cognos8/controller</td>
<td>c8_location/webcontent/ccr</td>
<td>Read</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Run scripts</td>
</tr>
<tr>
<td>cognos8/controllerserver</td>
<td>c8_location/ControllerProxyServer</td>
<td>Read</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Run scripts</td>
</tr>
<tr>
<td>cognos8/controllerhelp</td>
<td>c8_location/webcontent</td>
<td>Read</td>
</tr>
</tbody>
</table>

You can use a name other than cognos8 in the aliases. However, you must use cgi-bin as the second part of the alias and you must change the virtual directory in the Gateway URI property to match the new Cognos alias. For more information about changing the gateway URI, see "Change a URI" (p. 76).

If you use cognos8 in the Web aliases and embed them within other applications, such as Microsoft Excel reports, should you upgrade to a future version of Cognos 8 Controller, you must update the embedded aliases.

2. Right-click the controller Web alias, and then click Properties.
3. On the Virtual Directory tab, click A redirection to a URL.
4. In the Redirect to: box, type /cognos8/controllerbin/ccr.exe
5. Click Apply, and then click OK.

If you use Web aliases other than cognos8, or your Web server is on another computer, or you are using Microsoft Internet Application Interface (ISAPI), change the Gateway URI (p. 76) when you configure Cognos 8 Controller components.

### Configure Microsoft .NET Framework

When you configure Microsoft .NET Framework, you set up a Runtime Security Policy to create a trust between the Controller Client Distribution Server computer and the Cognos 8 Controller client computers. The Microsoft .NET Framework security policy is configured using a hierarchy of code groups at the machine policy level.

**Important:** Ensure that you installed the Microsoft .NET Framework SDK on the Controller Client Distribution Server computer so that you can use the configuration tool in the following steps.

After the Microsoft .NET Framework is configured on the Controller Client Distribution Server computer, you must deploy the Runtime Security Policy package to all Cognos 8 Controller client computers.

**Important:** If you install the gateway in a DMZ configuration, you must create two versions of the full trust. One version is used when users access Controller Client Distribution Server in the DMZ configuration, and the other version is used when users access Controller Client Distribution Server on the LAN. Users who access Controller Client Distribution Server in both configurations must install both versions of the full trust.

**Steps to Configure the Controller_URL Code Group**

1. In Administrative Tools, start Microsoft .NET Framework 2.0 Configuration.
2. In the left pane, expand **Runtime Security Policy, Machine, Code Groups, All_Code**.
3. Right-click **All_Code**, and click **New**.
4. Under **Identify the new Code Group**, click **Create a new code group**.
5. In the **Name** box, type a new code group name. For example, type **Controller_URL**.
6. Click **Next**.
7. Under **Choose a condition type**, in the drop-down list, click **URL**.
8. In the **URL:** box, type `http://<servername>/` (*where `<servername>` is the name of the computer where Controller Client Distribution Server is installed.**
   *Important:* Do not include an asterisk (*) in this URL.
9. Click **Next**.
10. Under **Assign a Permission Set to the Code Group**, click **Use existing permission set:** and in the drop-down list, click **Nothing**.
11. Click **Next**, and then click **Finish**.

**Steps to Configure the ControllerDomain Code Group**
1. In the left pane, right-click the **Controller_URL** code group, and click **New**.
2. Under **Identify the new Code Group**, click **Create a new code group**.
3. In the **Name** box, type **ControllerDomain**, and then click **Next**.
4. Under **Choose a condition type**, in the drop-down list, click **URL**.
5. In the **URL:** box, type the URL for the Controller Client Distribution Server computer. For example, type `http://<servername>/`
   *Important:* Do not include an asterisk (*) in this URL.
6. Click **Next**.
7. Under **Assign a Permission Set to the Code Group**, click **Use existing permission set:** and in the drop-down list, click **Full Trust**.
8. Click **Next**, and then click **Finish**.

**Steps to Configure the Controllerbin Code Group**
1. In the left pane, right-click the **Controller_URL** code group, and click **New**.
2. Under **Identify the new Code Group**, click **Create a new code group**.
3. In the **Name** box, type **Controllerbin**, and then click **Next**.
4. Under **Choose a condition type**, in the drop-down list, click **Publisher**.
5. Click **Import from Signed File...**
6. Go to the `c8_location/webcontent/ccr` directory, select **CCR.exe**, and then click **Open**.
7. Click **Next**.
8. Under **Assign a Permission Set to the Code Group**, click **Use existing permission set:** and in the drop-down list, click **Full Trust**.
9. Click **Next**, and then click **Finish**.

**Steps to Configure the Xceed Code Group**
1. In the left pane, right-click the **Controller_URL** code group, and click **New**.
2. Under **Identify the new Code Group**, click **Create a new code group**.
3. In the **Name** box, type **Xceed**, and then click **Next**.
4. Under **Choose a condition type**, in the drop-down list, click **Publisher**.
5. Click **Import from Signed File...**
6. Go to the `c8_location/webcontent/ccr` directory, select **Xceed.zip.dll**, and then click **Open**.
7. Click **Next**.
8. Under **Assign a Permission Set to the Code Group**, click **Use existing permission set:** and in the drop-down list, click **Full Trust**.
Chapter 6: Setting Up the Environment

9. Click Next, and then click Finish.

**Steps to Configure the C1.Print, C1.Common, C1.FlexGridClassic, C1.FlexGrid, and C1PrintPreview Code Groups**
1. In the left pane, right-click the Controller_URL code group, and click New.
2. Under **Identify the new Code Group**, click **Create a new code group**.
3. In the Name box, type C1.Print, and then click Next.
4. Under **Choose a condition type**, in the drop-down list, click **Strong Name**.
5. Click Import.
6. Go to the $c8_location/webcontent/ccr$ directory, select C1.C1PrintDocument.dll, and then click Open.
7. Select the Name and Version check boxes, and then click Next.
8. Under **Assign a Permission Set to the Code Group**, click Use existing permission set:, and in the drop-down list, click Full Trust.
9. Click Next, and then click Finish.
10. Repeat steps 1 to 9 for the following code groups:

<table>
<thead>
<tr>
<th>Code group name</th>
<th>Assembly file</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1.FlexGridClassic</td>
<td>C1.Win.C1FlexGridClassic.dll</td>
</tr>
<tr>
<td>C1.FlexGrid</td>
<td>C1.Win.C1FlexGrid.dll</td>
</tr>
<tr>
<td>C1.PrintPreview</td>
<td>C1.Win.C1PrintPreview.dll</td>
</tr>
</tbody>
</table>

**Steps to Configure the Deployment Package**
1. In the left pane, right-click Runtime Security Policy, and then click Create Deployment Package.
2. Under **Select the security policy level to deploy**, click Machine.
3. Beside the Choose a folder and file name for the new Windows Installer Package box, click Browse.
4. Go to the $c8_location/webcontent/ccr$ directory.
5. In the File name: box, type ControllerFullTrust.msi and then click Save.
6. Click Next, and then click Finish.

After you configure the deployment package, you must deploy the package to Cognos 8 Controller client computers. You can

- distribute the package to Cognos 8 Controller end users to download using email or a URL
  **Tip:** To install the deployment package, Cognos 8 Controller end users must have administrator privileges on the local computer.
- push the package to Cognos 8 Controller client computers using Active Directory or Patchlink

**Configure the Web Browser**

Cognos 8 Controller uses the default browser configurations provided by Microsoft. You must ensure that settings are enabled for cookies and Java scripts. Additional required settings are specific to the browser.

**Step**

- Ensure that the following settings are enabled in the Web browser.
Cognos 8 Controller uses the following cookies to store user information.

<table>
<thead>
<tr>
<th>Cookie</th>
<th>Type</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS_TICKET</td>
<td>Session temporary</td>
<td>Created if Cognos 8 is configured to use a Cognos Series 7 namespace</td>
</tr>
<tr>
<td>Cam_passport</td>
<td>Session temporary</td>
<td>Stores a reference to a user session stored on the Content Manager server</td>
</tr>
<tr>
<td>cc_session</td>
<td>Session temporary</td>
<td>Holds session information that is specific to Cognos Connection</td>
</tr>
<tr>
<td>cea-ssa</td>
<td>Session temporary</td>
<td>Stores the setting that specifies whether the user session information is shared with other Cognos 8 products</td>
</tr>
<tr>
<td>qs</td>
<td>Persistent</td>
<td>Stores the settings that the user makes for user interface elements such as menus and toolbars</td>
</tr>
</tbody>
</table>

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 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 a 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
Chapter 7: Configuring Cognos 8 Controller

After you install one or more Cognos 8 Controller components on your computer, you must configure them to work in your Cognos environment.

Initially, default property settings chosen by Cognos are used to configure the Cognos 8 Controller 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 Cognos environment. Use these optional configuration tasks to customize your configuration so that Cognos 8 Controller easily integrates into your existing environment. You can also configure Cognos 8 Controller to use other resources, such as using an authentication provider and then enabling single signon for the database connection and the users.

Cognos 8 Controller uses two configuration tools, Cognos Configuration, and Cognos Controller Configuration. Both of these configuration tools are used in a single server and distributed computer environment.

Cognos Configuration
Use Cognos Configuration to configure your Cognos Environment URIs and to specify the database connection properties to the content store.

You should start Cognos Configuration in the last page of the installation wizard only if additional setup is not required. For example, if you use a database server other than Microsoft SQL for the content store, we recommend that you copy the JDBC drivers to the appropriate location before you start the configuration tool.

When you change the value of a property, you must save the configuration and then restart the Cognos 8 service to apply the new settings to your computer.

Cognos Controller Configuration
Use Cognos Controller Configuration to configure your Controller data source and Controller data mart connections, the COM+ Server, and server authentication.

When you change the value of a property, you must save the configuration.

Configuring Single-computer Installations

If you install all Cognos 8 Controller server components on one computer, some configuration tasks are required so that the components work in your Cognos environment.

Before you configure Cognos 8 Controller, ensure that

- all Cognos server components are installed on one computer
- Microsoft Internet Information Services (IIS) is installed, configured, and running on the computer
- you created the database for the content store
- Microsoft .NET Framework is installed (p. 35) and configured on the computer (p. 48)

Important: Microsoft .NET Framework must also be installed and configured on all client computers that will be running Cognos 8 Controller.

- Microsoft SOAP Toolkit is installed on the computer
- Microsoft Data Access Components (MDAC) is installed on the computer
- ASP.NET is installed and configured (p. 35) on the computer
- an Oracle or Microsoft SQL Server database exists (p. 41) for use as a Controller database
Tip: The database user must have create table privileges.

- Microsoft Internet Explorer is installed and configured on the computer, and on client computers that will be running Cognos 8 Controller
- an Oracle or Microsoft SQL Server database exists for use as the Controller data mart database (p. 46) and Framework Manager is installed (p. 38) if you want to use the Publish to Data Mart Framework Manager model

Use the following checklist to guide you through the required configuration tasks:

- Set the database connection properties for the content store.
- Test the reporting components installation and configuration.
- Set database connection properties for the Cognos Controller data source.
- Set database connection properties for the Controller data mart, if required.
- Import the Cognos 8 Controller standard reports package.
- Define a data source for the Controller data mart, if required.
- Extract and publish the Publish to Data Mart model, if required.
- Set import directories for flat files, if required.
- Enable the COM+ Server.
- Configure the COM+ Server.
- Test the Cognos 8 Controller installation and configuration.

After you complete these configuration tasks, you can change the default behavior of Cognos 8 Controller (p. 76) to better suit your Cognos environment.

### Set Database Connection Properties for the Content Store

For all installations, 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 use one of the supported database servers to create the content store. The content store must be created using Oracle, Microsoft SQL Server, DB2, or Sybase Adaptive Server Enterprise (ASE). Cognos 8 Controller requires the TCP/IP protocol to access data and the content store. Ensure that the database server has the protocol set to TCP/IP. For more information, see "Create the Content Store" (p. 42).

If you are using Oracle, you do not have to install an Oracle client on the same computer as Content Manager. Content Manager, however, does require an Oracle JDBC driver called ojdbc14.jar. The driver is available from an Oracle client or server installation, and it can also be downloaded from the Oracle technology Web site (http://www.oracle.com/technology). The ojdbc14.jar driver file must be copied to the c8_location\p2pd\WEB-INF\lib directory where you installed the Content Manager.

Note: Some database servers are available with advanced features. When you select an advanced database, Cognos 8 Controller uses features of the database server to manage the connection. If you select the advanced Oracle database, for example, Cognos 8 Controller 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. On the computer where you installed Content Manager, start 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:JSQLConnect://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.
   Content Manager can now create the required tables in the content store when you start the Cognos 8 service for the first time. If the connection properties are not specified correctly, the tables are not created and you cannot connect to Cognos Connection.

### Test the Reporting Components Installation and Configuration

You should test your reporting components configuration before you proceed to the configuration tasks that are performed in Cognos Connection, the Cognos Web portal.

You can test your reporting components configuration settings by running the test feature before you start the Cognos 8 service. Then you can test the installation by starting the Cognos 8 service and then opening Cognos Connection.

If you installed Framework Manager for use with the Publish to Data Mart Framework Manager model, you can also test the connection to Framework Manager.

**Steps**

1. Start Cognos Configuration.
2. Ensure that you save your configuration, otherwise you cannot start the Cognos 8 service.
3. From the **Actions** menu, click **Test**.
Chapter 7: Configuring Cognos 8 Controller

Cognos Configuration checks the CSK availability, tests the namespace configuration, and tests the connections to the content store and logging database.

Tip: If Test is not available for selection, in the Explorer window, click Local Configuration.

4. If the test fails, reconfigure the affected properties and then test again.
Do not start the service until all tests pass.

5. From the Actions menu, click Start.
It may take a few minutes for the 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.

6. Open a Web browser.

7. Open Cognos Connection by typing one the following, where cognos8 is the virtual directory you created when you configured the Web server.
   - For the CGI gateway: http://host_name:port/cognos8
   - For an ISAPI gateway: http://host_name:port/cognos8/isapi
It may take a few minutes for the Web page to open. If you see the Welcome page of Cognos Connection, your installation is working.

Steps for Framework Manager
1. Start the Cognos 8 service.
2. To start Framework Manager, from the Start menu, click Programs, Cognos 8, Framework Manager.
   If you see the Welcome page of Framework Manager, your installation is working.

Set Database Connection Properties for the Controller Data Source

Before you can run Cognos 8 Controller, you must configure a Controller database connection. Cognos Controller databases must be created using either Oracle or Microsoft SQL Server.
To run reports against Cognos Controller data sources, the data sources must be configured for Report Server and appear in Cognos Connection.

If you are installing Cognos 8 Controller for the first time, or if you do not want to connect to an existing Controller database, you can create a database connection to an empty Controller database.

If you want to create a connection to an existing Controller database, we recommend that you create a backup of your database before you create the Controller data source connection. This is because the Controller Database Conversion Utility, which runs against the database during the data source connection process, updates the database tables for use with Cognos 8 Controller.

Steps
1. From the Start menu, start Cognos Controller Configuration.
2. In the Explorer window, click Database Connections, and then from the File menu, click New.
3. In the Properties window, click the Database type box, and then use the drop-down arrow to select the database type.
   You can choose Oracle or SQL Server.
4. In the Name box, type a name for the database connection.
5. In the Provider box, type the name of the database provider.
   To obtain the database provider information, see the Oracle or SQL Server documentation.
6. In the User ID and Password boxes, type the user name and password for the Controller database.
7. In the Initial catalog box, type the Controller database name.
8. In the Data source box, type the database server computer name.
Do not use localhost.

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

10. In the **Explorer** window, under **Database Connections**, click the database.

11. From the **Actions** menu, click **Run**.
    The Database Conversion Utility opens.

12. If this is an empty Controller database, in the **Database Conversion Utility** dialog box, click **Create Db**.
    The Database Conversion Utility initializes the database.

13. In the **Database Conversion Utility** dialog box, click **Run Steps**.
    The Database Conversion Utility updates the database for use with Cognos 8 Controller.

14. Click Close.

15. From the **Actions** menu, click **Check**.
    If the database connection validation fails, review the database connection properties and fix any errors.

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

17. In the **Explorer** window, under **Web Services Server**, click **Report Server**.

    The new database is now configured as a data source for Report Server, and is listed as a data source in Cognos Connection.

---

### Set Database Connection Properties for the Controller Data Mart

To prepare for using the Publish to Data Mart Framework Manager model, provided with Cognos 8 Controller, you must create a database connection to the empty Controller data mart database, which you previously created.

Before you configure the Publish to data mart connection, you must have set the connection properties for the Controller database. The Controller database contains the data to be published to the data mart.

#### Steps

1. From the **Start** menu, start Cognos Controller Configuration.

2. In the **Explorer** window, click **Database Connections for publish to data mart**.

3. In the **Properties** window, select the Controller database that will be used to publish to the data mart.

4. In the **Provider** box, type the name of the database provider that is appropriate for the database type that is hosting the data mart.
   To obtain the database provider information, see the Oracle or SQL Server documentation.

5. In the **User ID** and **Password** boxes, type the user name and password for the data mart database.

6. In the **Initial catalog** box, type the data mart database name.

7. In the **Data source** box, type the name of the server computer that hosts the data mart database.
   Do not use localhost.

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

9. From the **Actions** menu, click **Check**.
    If the database connection validation fails, review the database connection properties and fix any errors.

10. In the **Explorer** window, under **Database Connections**, click the Controller database that will be used to publish to the data mart.

11. From the **Actions** menu, click **Run**.
    The Database Conversion Utility opens.

12. Click the **DmConv** tab.
13. In the **Data** box, browse to the location of the UDL file for the Controller data mart database at `c8_location` `\DMData` and click **Open**.

14. Click **Run Steps**.

   The Database Conversion Utility creates the data mart tables.

15. Click **Close**.

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

17. In the **Explorer** window, under **Web Services Server**, click **Report Server**.


   If the repair button is unavailable, the data mart database is already known to Content Manager. The new data mart database is now configured as a data source for Report Server, and is listed as a data source in Cognos Connection.

---

**Import the Cognos 8 Controller Standard Reports Package**

Before you can run Cognos 8 Controller and view reports in Cognos Viewer, you must import the Cognos 8 Controller standard reports package into Content Manager.

**Steps**

1. Start Cognos Connection.
2. On the portal toolbar, click **Tools**, and then click **Content Administration**.
3. On the toolbar, click the **New Import** button. The **New Import** wizard appears.
4. In the **Deployment archive** box, click the **Controller** package, and then click **Next**.
5. Type an optional description and screen tip for the deployment specification, select the folder where you want to save it, and then click **Next**.
6. Select the content that you want to include in the import.
7. Select the options you want, along with your conflict resolution choice for options that you select.
8. In the **Specify the general options** page, select whether to include access permissions and references to external namespaces, and who should own the entries after they are imported in the target environment.
9. Click **Next**.

   The summary information appears.

10. Review the summary information and click **Next**.
11. In the **Select an action** page, select **Save and run once**, and then click **Finish**.

   After you run the import, the Cognos 8 Controller reports package appears in your Cognos Connection content.

---

**Define a Data Source for the Controller Data Mart**

If you are preparing to use the Publish to Data Mart Framework Manager model provided with Cognos 8 Controller, you must define a new data source so that Framework Manager can communicate with the Controller data mart database. You can define data sources in Cognos Connection or in Framework Manager. The data source appears in both places, regardless of where it was defined. Existing data source connections can be edited only in the portal.

**Steps**

1. Start Cognos Connection.
2. On the portal toolbar, click **Tools**, and then click **Directory**.
3. Click the **Data Sources** tab.
4. Click the **New Data Source** button.
5. In the **Name** box, type `CCR82_DM`, the name of the Controller data mart database.
6. In the **Description** box, type text to describe the database, and then click **Next**.
7. In the **Type** box, select the appropriate database type for the data mart database.
The connection string page for the selected database appears.

8. Enter any parameters that make up the connection string, and specify any other settings, such as a signon or a timeout.
   Tip: To test whether parameters are correct, click Test. If prompted, type a user ID and password or select a signon, and then click OK.

9. Click Finish.
   The data source appears as an entry in the Directory tool in the portal, and can be selected when using the import wizard in Cognos 8 Framework Manager.

**Extract the Publish to Data Mart Model and Publish It to Cognos Connection**

You must unzip the Publish to Data Mart Framework Manager model and publish it to Cognos Connection so that a report author can use the model in Report Studio for creating custom reports.

You must have Cognos 8 Framework Manager installed and configured before you can open the Publish to Data Mart model.

**Steps**

1. Copy the CCR82_DM.zip file from the c8_location/deployment directory to a location that is accessible by Framework Manager.
2. Unzip the CCR82_DM.zip file to extract the CCR82_DM.cpf model.
3. In Cognos 8 Framework Manager, from the File menu, click Open and go to the location of CCR82_DM.cpf project file and then click Open.
4. In the Project Viewer, expand the CCR82_DM folder, under Packages, click CCR82_DM, and from the Actions menu, click Package and then select Publish Packages.
5. Click Publish.
   A message informs you that the model is published under Public Folders CCR82_DM in Cognos Connection.
6. Click Finish and then click Close.
7. Close Framework Manager.

**Set Import Directories for Flat Files**

If a Controller user intends to import external data contained in flat files, you must specify the directories that contain the files so that they are available for selection when importing the data. This step is necessary only if the files are not located on the client computer so that the Controller user can select the Server option for Import file provider.

**Steps**

1. From the Start menu, start Cognos Controller Configuration.
2. In the Explorer window, click Import Directories.
3. In the Properties window, click the browse button and go to the folder that contains the text files to be imported into Cognos 8 Controller, and click OK.
4. Repeat the previous step to add more than one folder.
5. From the File menu, click Save.

**Enable Access to the COM+ Server**

When you install Cognos 8 Controller, a Controller COM+ application is created. After you install Cognos 8 Controller, you must confirm that network access to the COM+ Server is enabled.

By default, installations of Windows 2003 Server and Windows 2003 Server SP1 restrict the functionality of network and communication components. You must enable the COM+ Server before Cognos 8 Controller can operate.
Chapter 7: Configuring Cognos 8 Controller

Steps
1. In the Windows Control Panel, click Add or Remove Programs, and then click Add/Remove Windows Components.
2. Click Application Server, and then click Details.
3. Click Enable network COM+ Access, and then click OK.
4. Click Next, and then click Finish.

Configure the COM+ Server

After you configure network access to the COM+ Server, you must configure the Controller COM+ Server to run under a dedicated user.

Steps
1. From the Start menu, start Cognos Controller Configuration.
2. In the Explorer window, click COM+ Server.
3. In the COM+ Server window, click Specify Account to configure the COM+ Server with a user account that has administrator privileges on the computer.
4. In the User box, type the user name for the account.
5. In the Password box, type the password for the account.
6. In the Confirm Password box, retype the password for the account.
7. Click in the space under COM+ Role, and then from the File menu, click New.
8. Under COM+ Role, type ControllerUsers.
9. Under COM+ User, type IUSR_XXX, where XXX is the ID configured in IIS for anonymous access.
   This ID must be the same ID under which you configured the Web aliases.
   To locate the IIS anonymous access ID, in IIS, right-click the cognos8 Web alias, and then click Properties. On the Directory Security tab, click the Edit button. Copy the Anonymous AccessID in the User name box.
10. From the File menu, click New.
11. Under COM+ Role, type ControllerUsers.
12. Under COM+ User, type IWAM_XXX, where XXX is the ID configured in IIS for anonymous access.
13. From the Actions menu, click Check to validate each user.
14. From the File menu, click Save.

Test the Cognos 8 Controller Installation and Configuration

After you configure the Controller database connection and COM+ Server, test your configuration settings to confirm that you can start Cognos 8 Controller and connect to a Controller database.

You can test your Cognos 8 Controller installation and configuration on a client computer by starting Cognos 8 Controller from Cognos Connection or from a URL, and by running the Cognos 8 Controller Add-in for Excel. You can test from Cognos Connection only if you are using Cognos 8 Controller native authentication.

If you installed Framework Manager for use with the Publish to Data Mart Framework Manager model, you can also test the connection to Framework Manager.

Before you can run Cognos 8 Controller from a client computer, you must set up the local environment. To set up the local environment for Cognos 8 Controller, you must install and configure the Microsoft .NET Framework.

Tip: To view the Cognos 8 Controller user interface in optimal conditions, we recommend that you set the Display Properties for your monitor to a screen resolution of 1024 X 768 and a DPI setting of 96.

Steps to Run Cognos 8 Controller from Cognos Connection
1. Start Microsoft Internet Explorer.
2. Start Cognos Connection by typing one the following, where cognos8 is the virtual directory you created when you configured the Web server:
   • For the CGI gateway: type http://host_name:port/cognos8
   • For an ISAPI gateway: type http://host_name:port/cognos8/isapi
   It may take a few minutes for the Web page to open.
3. In the Cognos Connection Welcome page, click the Cognos Controller link. The Select Database window opens.
4. Select a database in the list, and click the check mark button.
5. Enter your logon credentials:
   • In the Cognos Controller - Login window, type the User ID, Password, Actuality, and Period, and then click the check mark button.
   Tip: For new databases, the default User ID is ADM and the default Password is kbs. If Cognos 8 Controller opens in your Web browser, your Cognos 8 Controller installation is working.

Steps to Run Cognos 8 Controller from a URL
1. On a client computer, start Microsoft Internet Explorer.
2. Type the following URL, where servername is the computer where Cognos 8 Controller Client Distribution Server is installed:
   http://servername/cognos8/controller
   The Select Database window opens.
3. Select a database in the list, and click the check mark button.
4. Enter your logon credentials:
   • In the Cognos Controller - Login window, type the User ID, Password, Actuality, and Period, and then click the check mark button.
   Tip: For new databases, the default User ID is ADM and the default Password is kbs. If Cognos 8 Controller opens in your Web browser, your Cognos 8 Controller installation is working.

Steps to Run the Cognos 8 Controller Add-in for Excel
1. On a client computer, start Microsoft Excel.
   You must have accessed Cognos 8 Controller at least once from the client computer.
2. From the Controller menu, click Log on.
3. In the Select Database dialog box, select a database and click the check mark button.
4. Enter your logon credentials:
   • In the Cognos Controller - Login dialog box, type the User ID, Password, Actuality, and Period, and click the check mark button.
   Tip: For new databases, the default User ID is ADM and the default Password is kbs. From the Controller menu, the Cognos 8 Controller Add-in for Excel features are available.

Steps to Run Framework Manager
1. Start the Cognos 8 service.
2. To start Framework Manager, from the Start menu, click Programs, Cognos 8, Framework Manager.
   If you see the Welcome page of Framework Manager, your installation is working.

Configuring Distributed Installations

If you distribute Cognos 8 Controller across more than one computer, some additional configuration tasks are required to ensure that the components can communicate with each other. In a distributed installation, you can install the gateway, Report Server, and Content Manager, on separate computers. You can also install Report Server and the gateway on multiple computers.
You can install the Controller Web Services Server and Controller Client Distribution Server, on multiple computers. In DMZ configurations, Controller Client Distribution Server must be installed in the same tier as the gateway.

For information about planning a distributed installation, see the Cognos 8 Controller Architecture and Deployment Guide.

**Communications**

When you install Cognos 8 Controller components on more than one computer, you must configure environment properties so that the distributed components can communicate with each other.

The Content Manager must know the location of the content store and the Controller data mart database.

Each Report Server must know the location of Content Manager and the database to use for job and schedule information.

Each gateway must know the location of at least one dispatcher, which should be located on a Report Server computer.

Each Controller Web Services Server must know the location of the Report Servers and the corresponding Controller Client Distribution Server.

Each Controller Client Distribution Server must know the location of the corresponding Controller Web Services Server.

**Required Sequence**

The sequence in which you configure and start computers is important. You must configure and then start the Cognos 8 service on the computer where you installed Content Manager before you configure other computers in your Cognos environment. We recommend that you configure the Report Server and the gateway next. You must configure the gateway computer after the Report Server computer so that cryptographic keys are shared and secure communication can take place among the Cognos 8 components.

After the Content Manager, Report Server, and gateway components are configured, started, and tested, you can then configure the Controller Client Distribution Server and Controller Web Services Server and test them.

**Prerequisites**

Before you begin configuration, ensure that the following is true on the computers where Controller Client Distribution Server and Controller Web Services Server are installed:

- Microsoft Internet Information Services (IIS) is installed, configured, and running.
- Microsoft .NET Framework is installed and configured.
- Microsoft Data Access Components (MDAC) is installed.
- ASP.NET is installed and configured.

Also ensure that

- you created the database for the content store
- Microsoft .NET Framework is installed and configured on all client computers that will run Cognos 8 Controller
- Microsoft SOAP Toolkit is installed on all computers where Controller Web Services Server is installed
- an Oracle or Microsoft SQL Server database exists for use as a Cognos Controller data source and the database user has create table privileges
- Microsoft Internet Explorer is installed and configured on the client computers that will run Cognos 8 Controller
- an Oracle or Microsoft SQL Server database exists for use as the Controller data mart database and Framework Manager is installed if you want to use the Publish to Data Mart Framework Manager model

Use the following checklist to guide you through the required configuration tasks:
Configure the Content Manager computer.
Configure the Report Server computers.
Configure the gateway computers.
Configure the Framework Manager computers, if required.
Test the Content Manager, Report Server, Gateway, and Framework Manager installation and configuration.
Configure the Controller Web Services Server computers.
Configure the Controller Client Distribution Server computers.
Import the Cognos 8 Controller standard reports package.
Define a data source for the Controller data mart, if required.
Extract and publish the Publish to Data Mart model, if required.
Test the Cognos 8 Controller installation and configuration.

Cognos 8 Controller is operating with the minimum security level. We recommend that you use a higher level of security than the default authentication settings. For more information, see “Configuring Authenticated Access” (p. 101).

After you complete these configuration tasks, you can change the Cognos 8 Controller default behavior (p. 76) to better suit your environment.

### Configuring the Content Manager Computer

In a distributed installation, the computer where you installed Content Manager must be configured, running, and accessible before you configure other computers in your Cognos environment. This ensures that the certificate authority service, which is installed with Content Manager, is available to issue certificates to other Cognos computers.

Before you configure Content Manager, ensure that you created the database for the content store on an available computer in your network.

Use the following checklist to guide you through the required configuration tasks for the Content Manager computer:

- Set database connection properties for the content store
- Start the Cognos 8 services

### Set Database Connection Properties for the Content Store

For all installations, 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.

Some database servers are available with advanced features. When you select an advanced database, Content Manager uses features of the database server to manage the connection. For example, if you select the advanced Oracle database, Content Manager 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.

Because Cognos 8 Controller components require the TCP/IP protocol to access data and the content store, ensure that the database server has the protocol set to TCP/IP.

### Steps

1. On the computer where you installed Content Manager, start 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:JSQLConnect://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.
   Content Manager can now create the required tables in the content store when you start the Cognos 8 service for the first time. If the connection properties are not specified correctly, the tables are not created and you cannot connect to Cognos Connection.

Start the Cognos 8 Services

After setting the database connection properties for the content store, you must start the services on the Content Manager computer. This ensures that the certificate authority service is available to issue certificates to other Cognos computers after you complete the required configuration tasks.

Steps
1. Start Cognos Configuration.
2. In the Explorer window, from the Actions menu, click Start.
   This action starts all installed services that are not running.
   Tip: If you want to start a particular service, click the service node in the Explorer window and then click Start from the Actions menu.
You can continue to configure the Content Manager computer by changing the default property settings (p. 76) so that they better suit your environment.

**Configure the Report Server Computers**

You can install the Report Server component on one or more computers, depending on your environment.

Distributed components must know the location of each other so that they can communicate. The Report Server component must know the location of the gateway. If you install the Report Server component on a different computer from Content Manager, you must configure the Report Server computer so that it knows the location of Content Manager. If you install the Report Server component on a different computer from the Controller Client Distribution Server component, you must configure the Report Server component so that it knows the location of the Controller Client Distribution Server component.

**Steps**

2. In the **Explorer** window, click **Environment**.
3. In the **Environment - Group Properties** window, specify the appropriate value for the **Gateway URI** by changing the localhost portion to the name of the gateway computer.
4. If you use Web aliases other than cognos8, change the **cognos8** element to the name that you used in your Web aliases.
5. If Content Manager is installed on a separate computer from Report Server, identify the location of Content Manager:
   - Under **Other URI Settings**, click the value for **Content Manager URIs** and then click the edit button.
   - Change the localhost portion of the existing URI to the name of the Content Manager computer.
6. From the **File** menu, click **Save**.
7. From the **Actions** menu, click **Start**.
   - This action starts all installed services that are not running.
   - **Tip**: If you want to start a particular service, click the service node in the **Explorer** window and then click **Start** from the **Actions** menu.
8. If the Report Server and Controller Client Distribution Server are on different computers, set the URL to point to Controller Client Distribution Server:
   - In the `c8_location\templates\ps\portal\launch` directory, open the ControllerLaunch.xml file in a text editor.
   - Change the value of the URL parameter from `../controller` to the fully-qualified URI of the computer where Controller Client Distribution Server is installed, such as `http://servername/cognos/controller`
   - Save and close the file.
9. Repeat steps 1 to 8 for each computer that contains a Report Server component.

**Configure the Gateway Computers**

You can install the gateway components on one or more Web server computers. The gateway components for Cognos 8 Controller include Controller Client Distribution Server, Gateway, and Gateway Integration Enabler.

When you install the gateway component on a different computer from Content Manager or Report Server, you must configure the gateway computer so that it knows the location of a dispatcher. A dispatcher is installed with every Content Manager and Report Server component. We recommend that the gateway use the dispatcher on a Report Server computer.

Other configuration tasks are optional and may be performed later.
Chapter 7: Configuring Cognos 8 Controller

Steps
1. Start Cognos Configuration.
2. In the Explorer window, click Environment.
3. In the Properties window, under Gateway Settings, Dispatcher URIs for gateway, change the localhost portion of the URI to the name or IP address of a Report Server computer.
4. In the Properties window, under Gateway Settings, Controller URI for gateway, change the localhost portion of the URI to the name or IP address of a Controller Web Services Server computer, and append /ccrws.asmx to the end of the URI.

For example, type:
http://servername:80/cognos8/controllerServer/ccrws.asmx
If you use Web aliases other than cognos8, change the cognos8 element to the alias name.
5. In the Explorer window, under Security, Cryptography, click Cognos, the default cryptographic provider.
6. Under Certificate Authority settings, set the Password property to match what you configured on the Content Manager computer.
7. Ensure that all other cryptographic settings match those on the Content Manager computer.
8. Test that the symmetric key can be retrieved. In the Explorer window, right-click Cryptography and click Test.
   Cognos 8 Controller components check the common symmetric key store (CSK) availability.
9. From the File menu, click Save.

If you installed all of the gateway components on one computer, the required gateway configuration is complete. You can continue to configure the gateway computers by changing the default property settings so that they better suit your environment. For example, you can configure a gateway to use a namespace.

Configure Framework Manager Computers

If you installed Framework Manager on a different computer from the Application Tier components, you must configure it to communicate with the other Cognos 8 components.

We recommend that you install and configure Cognos 8 components before you configure Framework Manager. You must first install and configure Content Manager and then start the 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.

You must also create a database for the Controller data mart (p. 46) before you configure Framework Manager.

Ensure that the Web server is configured and running (p. 47).

Important: If Cognos 8 was installed in more than one location, ensure that all URIs point to the correct version of Cognos 8. Framework Manager must be configured to use the same version of Cognos 8.

Installations with a Firewall

When the modeling tool is outside a network firewall that protects the Application Tier 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 Application Tier Components or you can install and configure a gateway that is dedicated to modeling tool communications. For more information about network firewalls, see the Cognos 8 Controller Architecture and Deployment Guide.

The steps in this topic describe how to configure the modeling tool computer. If you are using a gateway that is dedicated to the modeling tool, you must also configure the gateway computer (p. 78).

Steps
1. On the computer where you installed Framework Manager, start Cognos Configuration.
2. In the Explorer window, click Environment.
3. In the Properties window, in the Gateway URI box, type the appropriate value.
   - To use ISAPI, replace cognos.cgi with cognosisapi.dll.
   - To use a servlet gateway, type the following syntax:
     \[http[s]://host_name:port/context_root/servlet/Gateway\]
     where context_root is the value you assigned to the ServletGateway Web application
     when you deployed the ServletGateway application.
     
   Note: Ensure that you configured your Web server to support the servlet gateway (p. 78).
   - If you are not using a Web server, to use the dispatcher as the gateway, type the following
     syntax:
     \[http[s]://host_name:port/p2pd/servlet/dispatch\]
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 gateway URI.
6. In the Explorer window, under Cryptography, click 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 Content Manager computer.
8. From the File menu, click Save.
   Framework Manager is now configured to communicate with the other components of Cognos 8.

**Test the Content Manager, Report Server, Gateway, and Framework Manager**

**Installation and Configuration**

You can test your configuration settings by running the test feature before you start the Cognos 8
service. Then you can test the installation by starting the Cognos 8 service and opening Cognos
Connection.

If you installed Framework Manager for use with the Publish to Data Mart Framework Manager
model, you can also test the connection to Framework Manager.

**Steps**

1. Start Cognos Configuration.
2. Save your configuration, otherwise you cannot start the Cognos 8 service.
3. In the Explorer window, click Local Configuration.
4. From the Actions menu, click Test.
   Cognos Configuration checks the common symmetric key store (CSK) availability, tests the
   namespace configuration, and tests the connections to the content store and logging database.
5. If any test fails, reconfigure the affected properties and then test again.
   Do not start the service until all tests pass.
6. From the Actions menu, click Start.
   It may take a few minutes for the 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.
7. Start Microsoft Internet Explorer.
8. Start Cognos Connection by typing one the following, where cognos8 is the virtual directory you created when you configured the Web server:
   • For the CGI gateway, type \http://host_name:port/cognos8
   • For an ISAPI gateway, type \http://host_name:port/cognos8/isapi
   It may take a few minutes for the Web page to open. If you see the **Welcome** page of Cognos Connection, your installation is working.

**Steps for Framework Manager**

1. Start the Cognos 8 service.
2. To start Framework Manager, from the **Start** menu, click **Programs, Cognos 8, Framework Manager**.
   If you see the **Welcome** page of Framework Manager, your installation is working.
   You can now perform some additional configuration tasks to customize the behavior of Cognos 8 Controller components to better suit your Cognos environment (p. 76).

**Configuring the Controller Web Services Server Computers**

You can install Controller Web Services Server on one or more computers. When you install Controller Web Services Server, a Cognos 8 Controller COM+ application is created. You must configure the Controller database connections, enable the COM+ server, and then configure COM+ properties.

You can perform optional configuration tasks later.

If you install Controller Web Services Server on a different computer from Report Server, you must configure the Controller Web Services Server computer so that it knows the location of those components. The distributed components can then communicate with each other.

If users intend to use the automatic e-mail feature in Cognos 8 Controller, your SMTP server must be configured to allow access by the Controller Web Services Server.

If you intend to use the Publish to Data Mart Framework Manager model or import data from flat files that are in a directory on the server, additional configuration is required.

All COM+ applications should run under a designated domain user account. The user must be a local administrator on the servers and in the user domain for the network. The designated domain user account should be used on all Controller Web Services Server computers.

Before you configure the Controller Web Services Server computer, ensure that
   • Microsoft .NET Framework is installed on the computer
   • an Oracle or Microsoft SQL Server database exists as a Cognos Controller data source
   • an empty Oracle or Microsoft SQL Server database exists for use as the Controller data mart
   • the Controller database user has create table privileges
   • the Controller data mart user has create table privileges

Use the following checklist to guide you through the configuration tasks:

- Set database connection properties for the Controller data source.
- Set database connection properties for the Controller data mart, if required.
- Enable COM+ Server.
- Configure COM+ Server.
- Configure access to Report Server and the Controller standard reports package.
- Configure access to Framework Manager models, if required.
- Set import directories for flat files, if required.

After you complete these configuration tasks, you can change the default behavior of Cognos 8 Controller (p. 76) to better suit your Cognos environment. For example, you can configure multiple Controller Web Service Server computers for consolidation load balancing (p. 95) or for shared operation with the reporting database (p. 97).
Set Database Connection Properties for the Controller Data Source

Before you can run Cognos 8 Controller, you must configure a Controller database connection. Cognos Controller databases must be created using either Oracle or Microsoft SQL Server.

To run reports against Controller data sources, the data sources must be configured for Report Server and appear in Cognos Connection.

If you are installing Cognos 8 Controller for the first time, or if you do not want to connect to an existing Controller database, you can create a database connection to an empty Controller database.

If you want to create a connection to an existing Controller database, we recommend that you create a backup of your database prior to creating the Cognos Controller data source connection. This is because the Controller Database Conversion Utility, which runs against the database during the data source connection process, updates the database tables for use with Cognos 8 Controller.

Steps
1. From the Start menu, start Cognos Controller Configuration.
2. In the Explorer window, click Database Connections, and then from the File menu, click New.
3. In the Properties window, click the Database type box, and then use the drop-down arrow to select the database type. You can choose Oracle or SQL Server.
4. In the Name box, type a name for the database connection.
5. In the Provider box, type the name of the database provider. To obtain the database provider information, see the Oracle or SQL Server documentation.
6. In the User ID and Password boxes, type the user name and password for the Controller database.
7. In the Initial catalog box, type the Controller database name.
8. In the Data source box, type the database server computer name. Do not use localhost.
9. From the File menu, click Save.
10. In the Explorer window, under Database Connections, click the database.
11. From the Actions menu, click Run. The Database Conversion Utility opens.
12. If this is a new Controller database, in the Database Conversion Utility dialog box, click Create Db. The Database Conversion Utility initializes the database.
13. In the Database Conversion Utility dialog box, click Run Steps. The Database Conversion Utility updates the database for use with Cognos 8 Controller.
14. Click Close.
15. From the Actions menu, click Check. If the database connection validation fails, review the database connection properties and fix any errors.
16. From the File menu, click Save.
17. In the Explorer window, under Web Services Server, click Report Server.

Set Database Connection Properties for the Controller Data Mart

To prepare for using the Publish to Data Mart Framework Manager model, which is provided with Cognos 8 Controller, you must create a database connection to the empty Controller data mart database, which you previously created.
Before you configure the Publish to data mart connection, you must have set the connection properties for the Controller database. The Controller database contains the data to be published to the data mart.

**Steps**
1. From the **Start** menu, start Cognos Controller Configuration.
2. In the **Explorer** window, click **Database Connections for publish to data mart**.
3. In the **Properties** window, select the Controller database that will be used to publish to the data mart.
4. In the **Provider** box, type the name of the database provider that is appropriate for the database type that is hosting the data mart.
   For information about the database provider, see the Oracle or SQL Server documentation.
5. In the **User ID** and **Password** boxes, type the user name and password for the data mart database.
6. In the **Initial catalog** box, type the data mart database name.
7. In the **Data source** box, type the name of the server computer that hosts the data mart database.
   Do not use localhost.
8. From the **File** menu, click **Save**.
9. From the **Actions** menu, click **Check**.
   If the database connection validation fails, review the database connection properties and fix any errors.
10. In the **Explorer** window, under **Database Connections**, click the Controller database that will be used to publish to the data mart.
11. From the **Actions** menu, click **Run**.
   The Database Conversion Utility opens.
12. Click the **DmConv** tab.
13. In the **Data** box, browse to the location of the UDL file for the Controller data mart database at `c8_location\DMData` and click **Open**.
14. Click **Run Steps**.
   The Database Conversion Utility creates the data mart tables.
15. Click **Close**.
16. From the **File** menu, click **Save**.
17. In the **Explorer** window, under **Web Services Server**, click **Report Server**.
   If the repair button is unavailable, the data mart database is already known to Content Manager. The new data mart database is now configured as a data source for Report Server, and is listed as a data source in Cognos Connection.

**Enable COM+ Server**

By default, installations of Windows 2003 Server and Windows 2003 Server SP1 restrict the functionality of network and communication components. You must enable network access to COM+ Server before Cognos 8 Controller can operate.

**Steps**
1. In the Windows **Control Panel**, click **Add or Remove Programs**, and then click **Add/Remove Windows Components**.
2. Click **Application Server**, and then click **Details**.
3. Click **Enable network COM+ Access**, and then click **OK**.
4. Click **Next**, and then click **Finish**.
Configure COM+ Server

After you install Cognos 8 Controller, you must configure the Cognos 8 Controller COM+ Server to run under the designated domain user account.

Steps
1. From the Start menu, start Cognos Controller Configuration.
2. In the Explorer window, click COM+ Server.
3. In the COM+ Server window, click Specify Account to configure COM+ Server with the designated domain user account.
4. In the User box, type the user name for the designated domain user account.
5. In the Password and Confirm Password boxes, type the password for the account.
6. From the File menu, click New to create a new role in the Controller COM+ roles and users table.
7. Double-click under COM+ Role and type ControllerUsers
8. Double-click under COM+ User and type the following, where XXX is the ID configured in IIS for anonymous access and the same ID under which you configured the Web aliases:
   IUSR_XXX
   Tip: To locate the IIS anonymous access ID, do the following:
   • Go to IIS.
   • Right-click the cognos8 Web alias and then click Properties.
   • Copy the Anonymous AccessID from the User name box.
9. From the File menu, click New.
10. Double-click in the new row under COM+ Role and type ControllerUsers
11. Double-click in the new row under COM+ User and type the following, where XXX is the ID configured in IIS for anonymous access:
    IWAM_XXX
12. From the Actions menu, click Check to validate each user.
    If a user is not valid, the new role cannot be saved.
13. From the File menu, click Save.

Configure Access to Report Server and the Controller Standard Reports Package

If Controller Web Services Server is installed on a different computer from Report Server and the Controller standard reports package, you must configure Controller Web Services Server so that it knows the location of these components.

Steps
1. From the Start menu, start Cognos Controller Configuration.
2. In the Explorer window, click Report Server.
3. In the Properties window, double-click the value for Report Server, and then change the localhost portion of the URI to the name or IP address of the Report Server computer.
4. In the Properties window, double-click the value for Dispatcher URI, and then change the localhost portion of the URI to the name or IP address of the Report Server computer.
5. In the Properties window, in the Package box, click Controller.
6. From the File menu, click Save.

Configure Access to Framework Manager and the Publish to Data Mart Model

If Controller Web Services Server is installed on a different computer from Framework Manager and the Publish to Data Mart model, you must configure Controller Web Services Server so that it knows the location of these components.
Chapter 7: Configuring Cognos 8 Controller

Steps
1. From the Start menu, start Cognos Controller Configuration.
2. In the Explorer window, click External Data - Framework Manager Import.
3. In the Properties window, double-click the value for Dispatcher URI, and then change the localhost portion of the URI to the name or IP address of the Framework Manager computer.
4. In the Namespace box, type the namespace identifier defined for the Cognos 8 authentication namespace.
   The value should match the value for the Namespace ID property in Cognos Configuration, under Security, Authentication, Namespace.
5. In the User ID box, type the user name for the Cognos 8 authentication namespace.
6. In the Password box, type the password for the Cognos 8 authentication namespace.
7. From the File menu, click Save.

Set Import Directories for Flat Files
If a Controller user intends to import external data contained in flat files, you must specify the directories that contain the files so that they are available for selection when importing the data. This step is necessary only if the files are not located on the client computer so that the Controller user can select the Server option for Import file provider.

Steps
1. From the Start menu, start Cognos Controller Configuration.
2. In the Explorer window, click Import Directories.
3. In the Properties window, click the browse button and go to the folder that contains the text files to be imported into Cognos 8 Controller, and click OK.
4. Repeat to the previous step to add more than one folder.
5. From the File menu, click Save.

Configure the Controller Client Distribution Server Computer
You can install the Controller Client Distribution Server on one or more Web server computers.

If you install the Controller Client Distribution Server component on a different computer from the gateway component, you must configure the Controller Client Distribution Server computer so that it knows the location of the gateway computer. The distributed components can then communicate with one another.

If you install the Controller Client Distribution Server component on a different computer than the Controller Web Services Server component, you must configure the Controller Client Distribution Server computer so that it knows the location of the Controller Web Services Server computer.

Note: If for specific reasons you want to set the database selection mode property SelectDb to False, the database connection you previously configured for the Controller database (p. 56) must be named Default or users will not be able to connect to the database.

Before you configure the Controller Client Distribution Server computer, ensure that Microsoft .NET Framework is installed on the computer.

Steps
1. From the Start menu, start Cognos Controller Configuration.
2. In the Explorer window, click Client Distribution Server Configuration.
3. In the Properties window, double-click the value for WSSUrl, and type the following URI, where servername is the name of the gateway computer:
   http://servername/cognos8/cgi-bin/cognos.cgi?controller
4. In the Properties window, double-click the value for HelpUrl, and then change the localhost portion of the URI to the name or IP address of the Controller Web Services Server computer.
5. From the File menu, click Save.
After you complete these configuration tasks, you can change the default behavior of Cognos 8 Controller to better suit your Cognos environment (p. 76). For example, you can enable Enhanced Reporting Optimization (p. 93).

**Import the Cognos 8 Controller Standard Reports Package**

Before you can run Cognos 8 Controller and view reports in Cognos Viewer, you must import the Cognos 8 Controller standard reports package into Content Manager.

**Steps**
1. Start Cognos Connection.
2. On the portal toolbar, click **Tools**, and then click **Content Administration**.
3. On the toolbar, click the **New Import** button. The **New Import** wizard appears.
4. In the **Deployment archive** box, click the **Controller** package, and then click **Next**.
5. Type an optional description and screen tip for the deployment specification, select the folder where you want to save it, and then click **Next**.
6. Select the content that you want to include in the import.
7. Select the options you want, along with your conflict resolution choice for options that you select.
8. In the **Specify the general options** page, select whether to include access permissions and references to external namespaces, and who should own the entries after they are imported in the target environment.
9. Click **Next**.
   The summary information appears.
10. Review the summary information and click **Next**.
11. In the **Select an action** page, select **Save and run once**, and then click **Finish**.

After you run the import, the Cognos 8 Controller reports package appears in your Cognos Connection content.

**Define a Data Source for the Controller Data Mart**

If you are preparing to use the Framework Manager model provided with Cognos 8 Controller, you must define a new data source so that Framework Manager can communicate with the Controller data mart database. You can define data sources in Cognos Connection or in Framework Manager. The data source appears in both places, regardless of where it was defined. Existing data source connections can be edited only in the portal.

**Steps**
1. Start Cognos Connection.
2. On the portal toolbar, click **Tools**, and then click **Directory**.
3. Click the **Data Sources** tab.
4. Click the **New Data Source** button.
5. In the **Name** box, type CCR82_DM, the name of the Controller data mart database.
6. In the **Description** box, type text to describe the database, and then click **Next**.
7. In the **Type** box, select the appropriate database type for the data mart database.
   The connection string page for the selected database appears.
8. Enter any parameters that make up the connection string, and specify any other settings, such as a signon or a timeout.
   **Tip:** To test whether parameters are correct, click **Test**. If prompted, type a user ID and password or select a signon, and then click **OK**.
9. Click **Finish**.
   The data source appears as an entry in the Directory tool in the portal, and can be selected when using the import wizard in Framework Manager.
Chapter 7: Configuring Cognos 8 Controller

Extract the Publish to Data Mart Model and Publish It to Cognos Connection

You must unzip the Publish to Data Mart Framework Manager model and publish it to Cognos Connection so that a report author can use the model in Report Studio for creating custom reports.

You must have Cognos 8 Framework Manager installed and configured before you can open the Publish to Data Mart model.

Steps
1. Copy the CCR82_DM.zip file from the c8_location/deployment directory to a location that is accessible by Framework Manager.
2. Unzip the CCR82_DM.zip file to extract the CCR82_DM.cpf model.
3. In Cognos 8 Framework Manager, from the File menu, click Open and go to the location of CCR82_DM.cpf project file and then click Open.
4. In the Project Viewer, expand the CCR82_DM folder, under Packages, click CCR82_DM, and from the Actions menu, click Package and then select Publish Packages.
5. Click Publish.
   A message informs you that the model is published under Public Folders CCR82_DM in Cognos Connection.
6. Click Finish and then click Close.
7. Close Framework Manager.

Schedule a Performance Optimization Procedure for an Oracle Controller Database

Cognos 8 Controller provides an SQL procedure that analysis the schema in the Controller database and gathers the appropriate statistics, which Oracle requires for optimal performance. This procedure can be run by the Controller user, but we recommend that you create a job to run it automatically on a weekly basis.

Steps
1. Create a file and add the following command lines:
   ```sql
   SQL> DECLARE JOB BINARY_INTEGER;
   BEGIN
     DBMS_SCHEDULER.create_job ( 
       job_name => 'Analyze_Controller_Schema_week',
       job_type => 'PLSQL_BLOCK',
       job_action => 'BEGIN PRC_ANALYZE_SCHEMA; END;',
       start_date => SYSTIMESTAMP,
       repeat_interval => 'freq=weekly; byday=sat; byhour=9; byminute=0; bysecond=0;',
       end_date => NULL,
       enabled => TRUE,
       comments => 'Analyze schema job to be run Saturdays 9:00 AM');
   END;
   ```
2. Run the file on a weekly basis.

Test the Cognos 8 Controller Installation and Configuration

After you configure the Controller database connection and COM+ Server, test your configuration settings to confirm that you can start Cognos 8 Controller and connect to a Controller database.

You can test your Cognos 8 Controller installation and configuration on a client computer by starting Cognos 8 Controller from Cognos Connection or from a URL, and by running the Cognos 8 Controller Add-in for Excel. You can test from Cognos Connection only if you are using Cognos 8 Controller native authentication.
If you installed Framework Manager for use with the Publish to Data Mart Framework Manager model, you can also test the connection to Framework Manager.

Before you can run Cognos 8 Controller from a client computer, you must set up the local environment. To set up the local environment for Cognos 8 Controller, you must install and configure the Microsoft .NET Framework.

**Tip:** To view the Cognos 8 Controller user interface in optimal conditions, we recommend that you set the Display Properties for your monitor to a screen resolution of 1024 X 768 and a DPI setting of 96.

### Steps to Run Cognos 8 Controller from Cognos Connection

1. Start Microsoft Internet Explorer.
2. Start Cognos Connection by typing one the following, where cognos8 is the virtual directory you created when you configured the Web server:
   - For the CGI gateway: type `http://host_name:port/cognos8`
   - For an ISAPI gateway: type `http://host_name:port/cognos8/isapi`
   
   It may take a few minutes for the Web page to open.
3. In the Cognos Connection Welcome page, click the Cognos Controller link.
   
   The Select Database window opens.
4. Select a database in the list, and click the check mark button.
5. Enter your logon credentials:
   - In the Cognos Controller - Login window, type the User ID, Password, Actuality, and Period, and then click the check mark button.
   
   **Tip:** For new databases, the default User ID is ADM and the default Password is kbs.
   
   If Cognos 8 Controller opens in your Web browser, your Cognos 8 Controller installation is working.

### Steps to Run Cognos 8 Controller from a URL

1. On a client computer, start Microsoft Internet Explorer.
2. Type the following URL, where `servername` is the computer where Cognos 8 Controller Client Distribution Server is installed:
   
   `http://servername/cognos8/controller`
   
   The Select Database window opens.
3. Select a database in the list, and click the check mark button.
4. Enter your logon credentials:
   - In the Cognos Controller - Login window, type the User ID, Password, Actuality, and Period, and then click the check mark button.
   
   **Tip:** For new databases, the default User ID is ADM and the default Password is kbs.
   
   If Cognos 8 Controller opens in your Web browser, your Cognos 8 Controller installation is working.

### Steps to Run the Cognos 8 Controller Add-in for Excel

1. On a client computer, start Microsoft Excel.
   
   You must have accessed Cognos 8 Controller at least once from the client computer.
2. From the Controller menu, click Log on.
3. In the Select Database dialog box, select a database and click the check mark button.
4. Enter your logon credentials:
   - In the Cognos Controller - Login dialog box, type the User ID, Password, Actuality, and Period, and click the check mark button.
   
   **Tip:** For new databases, the default User ID is ADM and the default Password is kbs.
   
   From the Controller menu, the Cognos 8 Controller Add-in for Excel features are available.
Changing Cognos 8 Controller Default Configuration Settings

When you install Cognos 8 Controller 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 the Cognos 8 Controller configuration tools to change the value.

If you change the value of a property using Cognos Configuration, you must save the configuration and then restart the Cognos 8 service to apply the new setting to your computer.

If you change the value of a property using Cognos Controller Configuration, you must save the configuration to apply the new setting 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 Cognos computers. For example, using Cognos Configuration, you can

- change a URI
- change the gateway
- configure cryptographic settings
- configure SSL protocol
- configure the reporting components to use Cognos Application Firewall
- configure temporary file properties
- specify where to send log messages
- change the gateway
- configure the gateway to use a namespace
- enable and disable services
- specify the amount of resources the Cognos 8 service uses
- change global settings, such as product locales, and cookie settings

Using Cognos Controller Configuration, you can

- add or remove Controller database Connections
- change the COM+ Server configuration
- enable batch services
- enable Enhanced Reporting Optimization
- change the default installation of the Cognos 8 Controller Add-in for Excel

Using other tools, you can

- configure Controller Web Services Server computers for consolidation load balancing
- configure multiple server access for the Controller database

After you change the default behavior of Cognos 8 Controller to better suit your Cognos environment, you can configure Cognos 8 Controller to use an authentication provider, or test the installation and configuration.

Change a URI

You can change certain elements in a URI depending on your environment. You change the elements of a URI using both Cognos Configuration and Cognos Controller Configuration.

A Cognos 8 Controller 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
Chapter 7: Configuring Cognos 8 Controller

**protocol: \//host_name_or_IP:port/context_root/alias_path**

<table>
<thead>
<tr>
<th>Element</th>
<th>Examples</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol</td>
<td>http</td>
<td>Specifies the protocol used to request and transmit information.</td>
</tr>
<tr>
<td>host name or IP</td>
<td>localhost or 192.168.0.1</td>
<td>Specifies the identity of the host on the network. You can use an IP address, a computer name, or a fully qualified domain name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>In a distributed installation, you must change the localhost element of a URI.</td>
</tr>
<tr>
<td>port</td>
<td>9300 or 80</td>
<td>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.</td>
</tr>
<tr>
<td>context root</td>
<td>p2pd</td>
<td>Used by Tomcat to determine the context of the application so that the request can be routed to the correct Web application for processing</td>
</tr>
<tr>
<td>alias path</td>
<td>servlet/dispatch</td>
<td>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 Cognos 8 Controller components will not function correctly.</td>
</tr>
<tr>
<td>virtual directory</td>
<td>cognos8/</td>
<td>Used by the Web server to map a virtual directory or alias to a physical location. For example, in the default Gateway URI of <a href="http://localhost:80/cognos8/cgi-bin/cognos.cgi">http://localhost:80/cognos8/cgi-bin/cognos.cgi</a>, the virtual directory is cognos8/cgi-bin.</td>
</tr>
<tr>
<td>gateway application</td>
<td>cognos.cgi</td>
<td>Specifies the name of the Cognos gateway application that is used. For example, if you are accessing Cognos 8 Controller components using a Common Gateway Interface (CGI), then the default gateway application would be cognos.cgi.</td>
</tr>
</tbody>
</table>

**Steps to Change a URI Using Cognos Configuration**

1. Start Cognos Configuration.
Chapter 7: Configuring Cognos 8 Controller

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 or Content Manager services on this system.
5. From the **File** menu, click **Save**.

**Steps to Change a URI Using Cognos Controller Configuration**
1. From the **Start** menu, start Cognos Controller Configuration.
2. In the **Explorer** window, click the appropriate group or component.
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.

**Changing the Gateway**

To improve Web server performance, you can configure 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
- *servlet* for an application server or Web server that supports Java

There is no additional Web server configuration required to use ISAPI. To access Cognos 8 components using ISAPI, in 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 a Servlet Gateway**

You can configure the Servlet Gateway to run under a supported application server.

After ensuring that the required components are installed and operating, you copy Cognos security provider files to the JVM environment, configure Cognos 8, change the application server startup script (application servers only), and then deploy the Cognos servlet gateway to the application server.

Cognos 8 cryptographic services use a specific .jar (Java Archive) file, named `bcprov-jdkmm-nnn.jar`, that must be located in your Java Runtime Environment (JRE). This file provides additional encryption and decryption routines that are not supplied as part of a default JVM installation. To ensure security, the encryption file must be loaded by the JVM using the java extensions directory.

Java 1.4.2 is the minimum supported JRE for Cognos 8. Ensure that you installed the correct JRE for the hardware that you are using. The `bcprov-jdkmm-nnn.jar` file is for Java 1.4.2.

**Tip:** If you use Sun JRE 1.4.2 on UNIX, ensure that you are using the correct startup file for the `/dev/random` device. You must use `/etc/init.d` or `/etc/rc3.d/f20random`. For more information, see your UNIX documentation.

Before you set up the Cognos servlet gateway, ensure that
- the application server is installed and operational on each computer where the servlet gateway is to be installed
Chapter 7: Configuring Cognos 8 Controller

- Cognos 8 Gateway components are installed (p. 35) on the same system as the application server
- the Cognos 8 dispatcher and Content Manager components are installed and running in the environment
- the application server user account has full access permissions for the Cognos installation

We recommend that you create a new UNIX or Linux group named cognos8. This group must contain the user that starts the application server and the user that owns the Cognos files. Change the group ownership of the Cognos files to the cognos8 group and change the file permissions for all Cognos files to GROUP READABLE/WRITEABLE/EXECUTABLE. For simplicity, you can also use the application server user account to install and run Cognos components.

**Steps to Copy Cognos Security Provider Files**

1. Ensure that the JAVA_HOME environment variable is set to the JRE location.
   For example, to set JAVA_HOME to the JRE files provided with the installation, the path is `c8_location/bin/jre/version`.

2. Copy the bcprov-jdkmm-nnn.jar file from the `c8_location/bin/jre/version/lib/ext` directory to the `Java_location/lib/ext` directory.

**Steps to Configure Cognos 8**

1. Set the JAVA_HOME environment variable to point to the JVM used by the application server.
   Tip: If the application server ships with a JVM, then the JAVA_HOME environment variable should be set to reference it. Cognos Configuration uses this variable to locate the JVM used by the application server and the security provider files supplied by Cognos.

2. From the `c8_location/bin` directory, start Cognos Configuration:
   - On Windows, type `cogconfig.bat` in a command window or select Cognos Configuration from the Start menu.
   - On UNIX or Linux, type `cogconfig.sh` if you have existing incompatible encryption keys, you will be prompted to automatically generate new ones at this time.

3. In the Explorer window of Cognos Configuration, expand Environment.

4. In the Properties window, under Gateway settings, change the Dispatcher URIs for Gateway property to use the port number and host name or IP address of the server where the dispatcher component is installed.
   The default context root value for the servlet gateway is `/ServletGateway`. For more information, see "Change a URI" (p. 76).

5. Complete other required configuration changes such as enabling security.

6. Save the configuration.
   New cryptographic keys are created using the JVM that is defined by the JAVA_HOME variable.

7. To create the application file to deploy to the application server, from the Actions menu, click Build Application Files.
   The Build Application Wizard opens and allows you to select the type of application to build and the context root to use to access the application.

8. Close Cognos Configuration.
   If you are using an application server, you must now change the application server startup script and then configure the application server properties and deploy Cognos components. A maximum heap memory setting of between 256MB and 512MB is a suggested starting value that you can change to suit your environment. For more information about configuring application servers, see the Cognos 8 Business Intelligence Installation and Configuration Guide.

To access Cognos 8 components using the servlet gateway, enter the gateway URI. For example,
Chapter 7: Configuring Cognos 8 Controller

http[s]:host_name:port/ServletGateway
The servlet gateway URI is case sensitive.

Configure Cryptographic Settings

Cognos 8 Controller components require a cryptographic provider to run. If you delete the default cryptographic provider, you must configure another provider to replace it. After configuring a cryptographic provider, you can test it on the gateway computer.

You can configure cryptographic and 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 Cognos 8 Controller 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 confirm 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.

Cognos 8 Controller requires a cryptographic provider. By default, the 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 or the Enhanced Encryption Module for Entrust, available from Cognos.

Important: In a distributed installation, the Cognos computers obtain the cryptographic keys from Content Manager. If you change the cryptographic keys in Content Manager, such as by reinstalling Content Manager, you must delete the cryptographic keys on the other 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 Cognos 8 Controller components in a distributed installation must be configured with the same cryptographic provider settings.

Steps for Cryptographic Settings

1. Start 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.
   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 Cognos Configuration.
2. In the Explorer window, under Security, Cryptography, click 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 a third-party 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 Cognos 8 components. For example, database passwords entered in 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 third-party 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 a third-party Certificate Authority (CA) server, you must now configure Cognos 8 Controller components to use the CA.

### Configuring the SSL Protocol

The Secure Sockets Layer (SSL) protocol is used to secure communication between Cognos components installed on the same computer or on different computers.

In addition, you may want to set up SSL connections between 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 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 Cognos components (p. 81).
- Set up shared trust between Cognos components and other servers, if required (p. 83).
- Select and rank Cipher Suites to be used in an SSL connection, if required (p. 84).
- Configure Controller Web Services Server for SSL within your Web server. For information about configuring SSL within your Web server, see the documentation provided with the Web server.

### Configure SSL for Cognos 8

You can configure 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, 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 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 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 Cognos certificate authority service, you must first configure all Cognos computers to use the non-secure (http) protocol before you configure 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 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 Content Manager computer and starting the services, you ensure that the certificate authority service on the Content Manager computer can issue certificates to other computers in the 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 Cognos components are working properly. After you test your installation, you can configure the SSL protocol.

When you configure Cognos 8 to use the SSL protocol, ensure that you first configure the Content Manager computer to use the protocol and start the services on the Content Manager computer. After you do this, you can configure the SSL protocol on other 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 Cognos components. If you add the component to a different location on the same computer as other 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 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.

• 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 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 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 Cognos 8 encryption key stores. There are more settings under Security, Cryptography, Cognos.

7. From the File menu, click Save.

## Set Up Shared Trust Between Cognos Servers and Other Servers

If you want to use the default Cognos certificate authority and you want to use SSL for connections from other servers to Cognos servers, you must add the Cognos certificate to the trust store on the other servers.

Note: If you use browsers to connect to Cognos components, the browsers automatically prompt users to update their trust stores.

If you want the connection between 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 Cognos servers.

If you have configured Cognos components to use a third-party certificate authority (CA), you do not have to set up shared trust between Cognos server and other servers.

### Steps to Copy the Cognos Certificate to Another Server

1. Go to the `c8_location\bin` directory.

2. Extract the Cognos certificate by typing the following command:

   • On UNIX or Linux, type
   
   ```bash
   ThirdPartyCertificateTool.sh -E -T -r destination_file -k c8_location/configuration/signkeypair\jCAKeystore -p password
   ```

   • On Windows, type
   
   ```bash
   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 Cognos Servers

1. Copy the certificate from your certificate authority to a secure location on the Cognos server.
Chapter 7: Configuring Cognos 8 Controller

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 e8_location/configuration/signkeypair/jCAKeystore -p password`
   
   • On Windows, type
     
     `ThirdPartyCertificateTool.bat -T -i -r CA_certificate_file -k e8_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.

Cognos provides a list of supported cipher suites for SSL. 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 third-party 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 Cognos Configuration.
2. In the Explorer window, click Cryptography, 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.

Configure Reporting Components to Use Cognos Application Firewall

Cognos Application Firewall analyzes and validates HTTP and XML requests before they are processed by Report Server. Cognos Application Firewall may modify these HTTP and XML requests.

Cognos Application Firewall protects the Cognos Web products from malicious data. The most common forms of malicious data are buffer overflows and cross-site scripting attacks (XSS links), either through script injection in valid pages or redirection to another Web site.

You can change settings for XSS checking. You can also add host and domain names to the Cognos list of validated names.

For more information about Cognos Application Firewall, see the Cognos 8 Controller Architecture and Deployment Guide.
You can track firewall activity by checking the log file, which contains rejected requests only. If firewall validation fails, you can check the log file to find where the failure occurred. By default, log messages are stored in the `c8_location\logs\cogserver.log` file. In a gateway-only installation, the file is named caf.log. If you configure a destination for log messages (p. 86), Cognos Application Firewall log messages are sent to the specified destination.

Cognos Application Firewall also has a Secure Error feature, which gives administrators control over which groups or users can view detailed error messages. For more information, see the Administration and Security Guide.

**Steps**

1. On each computer where Cognos 8 Application Tier Components have been installed, start Cognos Configuration.
2. In the Explorer window, under Security, click Cognos Application Firewall.
3. In the Properties window, for the CAF enabled property, set the appropriate values.
   By default, Cognos Application Firewall is enabled.
   
   **Important:** The Cognos Application Firewall is an essential component of Cognos security, helping to provide protection against penetration vulnerabilities. Disabling the Cognos Application Firewall will remove this protection. Under normal circumstances we recommend that you not disable the Cognos Application Firewall.
4. If you are using a third-party 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 third-party XSS tool. The default characters are », <, and ‘.
5. Add host and domain names to the 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.
   • 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.
   
   **Tip:** If you are using drill-through from Cognos Series 7 to reports in Cognos 8, add the hostnames of the Cognos Series 7 gateway servers to the list.
   • Click OK.

   Cognos Application Firewall validates domain and host names to protect URLs that are created. By default, Cognos Application Firewall considers domain names derived from the environment configuration properties to be safe domain names. You can add names manually to the list of valid domains and hosts. Adding names is useful when you need to redirect requests to non-Cognos computers using the Back or Cancel functions or when using drill-through to different Cognos product installations.
6. Save the configuration.

**Configure Temporary File Properties**

You can change the location where Cognos 8 Controller components store recently viewed reports, and you can choose to encrypt their content. By default, Cognos 8 Controller components store temporary files in the `c8_location\temp` directory and the files are not encrypted.

We recommend that you first set up read-only access for all users to the `c8_location` directory.

**Steps**

1. Start Cognos Configuration.
2. In the Explorer window, click Environment.
3. In the Properties window, for the Temporary files location property, specify the new location.
4. If you require the content of temporary files to be encrypted, set the Encrypt temporary files property to True.
5. Ensure that the user account under which Cognos 8 Controller components run have the appropriate privileges to the temporary files location. For example, on Windows, full control privileges.

**Configuring Log Messages**

You can specify where the local log server sends log messages. For information about log messages, see the Cognos 8 Controller Architecture and Deployment Guide.

A local log server is automatically installed when you install Content Manager or Report Server. The log server can send log messages to one or more destinations, which include, but are not limited to, the following types:

- a remote log server
- a file
- a database

**A Remote Log Server**

In a distributed installation, you can configure the log servers to send log messages to a single log server, which acts as a common log server. You can then configure the common log server to send the log messages to a flat file or database on the same or another computer.

If the remote log server becomes unavailable, log messages are redirected to recovery files on the local computer in the \c8\_location\logs\recovery\remote directory. These recovery files have timestamp information in their file names, and are not readable like regular log files. When the remote log server becomes available, an automatic recovery process moves all log information to the remote log server and deletes the local log files.

**A File**

The log server is configured by default to send log messages to the crnserver.log file located in the \c8\_location\logs directory. You can configure the log server to send log messages to an alternative file, such as the Windows NT Event log.

**A Database**

The log server can also send messages to a database on the same or another computer.

The logging database has the same configuration and user account requirements as the content store database. After you configure Cognos 8 Controller components to send messages to a logging database, and restart the Cognos 8 service, Cognos 8 Controller components create the required tables and table fields. You can test the connection to the logging database before you restart the Cognos 8 service.

**Configuring Log Messages**

To configure log messages:

- Create the logging database using the same procedure as to create the content store database (p. 42).
  - Important: For DB2, you must create an additional regular user tablespace with a page size of 8k for Cognos 8 Controller components to create the logging database.
- Set up the database client, if required.
- Specify the log messages destination.

**Set Up the Database Client for a Logging Database**

After you create a database for your log messages, if you use Oracle, DB2, or Sybase as the database server, additional steps are required.

If you use an Oracle or Sybase database, you must set up the JDBC driver.

If you use a DB2 database, you must set up the database client software and the JDBC 2.0 driver.
If you use a Microsoft SQL Server database, the JSQLConnect.jar file is installed to the appropriate location by default. The only additional step is to ensure that the Microsoft SQL Server uses TCP/IP connectivity.

If you are using the same type of database for the log messages as you use for the content store, you do not have to set up a JDBC driver on the Content Manager computer. You must, however, set up a JDBC driver on the Report Server computers.

**Steps for Oracle**
1. On the computer where Oracle is installed, go to the ORACLE_HOME\jdbc\lib directory.
2. Copy the ojdbc14.zip file to the c8_location\webapps\p2pd\WEB-INF\lib directory on every computer where Content Manager or Report Server are installed.

**Steps for DB2**
1. Install the DB2 client software on the computer where Content Manager or Report Server are installed.
2. If the logging database is on a different computer from the log server, configure a database alias to the logging database by running the DB2 Client Configuration Assistant.
   **Note:** If the logging database and log server are on the same computer, the logging database name is automatically used to create an alias.
3. Stop the DB2 services and the HTML Search Server.
4. To copy the JDBC2 driver, copy the DB2_installation\sqlib\java\db2java.zip file to the c8_location\webapps\p2pd\WEB-INF\lib directory.
5. Rename the db2java.zip file to db2java.jar.
6. Restart the DB2 services and the HTML Search Server.
7. Repeat this entire procedure on every computer where Content Manager or Report Server are installed.

**Steps for Sybase**
1. On the computer where Sybase is installed, enable the JDBC driver using the following script: Sybase_location\jConnect-5_5\sp\sql_server12.5.sql
2. Go to the Sybase_location\jConnect-5_5\classes directory.
3. Copy the jconn2.jar file to the c8_location\webapps\p2pd\WEB-INF\lib directory on every computer where Content Manager is installed.

**Specify the Log Messages Destination**

You can configure a type of destination for the log messages, and then configure properties for the specific destination. You can also configure more than one destination for log messages.

**Steps**
1. If the destination is a database, ensure that you
   - created the logging database (p. 86)
   - set up the database client
2. On the computer where you installed Content Manager or Report Server, start Cognos Configuration.
3. In the Explorer window, under Environment, click Logging.
4. In the Properties window, set the log server properties.
   - If you want to use TCP between Cognos 8 Controller components and the remote log server, set the Enable TCP property to True.
5. In the Explorer window, under Environment, right-click Logging, and click New resource, Destination.
6. In the Name box, type the name of the destination.
7. In the Type list, click the type of destination and then click OK.
8. If the destination is a file or a remote log server, in the **Properties** window, type the appropriate values for the mandatory and optional properties.

For a remote log server, you must later specify the log messages destination when you configure the remote log server.

9. If the destination is a database, add a database resource:
   - In the **Explorer** window, right-click the database, and click **New resource, Database**.
   - In the **Name** box, type the name of the logging database that you created.
   - In the **Type** list, click the database type, and then click **OK**.
   - In the **Properties** window, type the appropriate values for the mandatory and optional properties.
   - Test the connection to the new database. In the **Explorer** window, under **Environment**, right-click **Logging** and click **Test**.

Cognos 8 Controller components connect to the database. If you configured more than one database for logging messages, Cognos 8 Controller components test all of the databases.

10. Repeat steps 5 to 9 for each destination to which you want the log server to send messages.

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

12. In the **Explorer** window, click **Cognos 8 service, Cognos 8**.

13. From the **File** menu, click **Restart**.

   If you selected a database as the destination, Cognos 8 Controller components create the required tables and fields in the database that you created.

   If the destination was a remote log server, configure and start the remote log server. Then restart the Cognos 8 service on the local computer.

   If the destination was a database, you can use Cognos 8 Controller components to run log reports from the database.

   You can also set the logging level, which controls the amount of detail and type of messages that are sent to a log file or database. For instructions, see the *Administration and Security Guide*.

### Changing the Gateway

To improve Web server performance, you can configure Cognos 8 Controller to use alternate gateways that replace the default CGI program. For example, you can use Microsoft Internet Application Programming Interface (ISAPI) for Microsoft Internet Information Services on Windows.

There is no additional Web server configuration required to use ISAPI. To access Cognos 8 Controller components using ISAPI, in 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 to Use a Namespace

If Cognos 8 Controller components use multiple namespaces or if anonymous access is enabled and Cognos 8 Controller 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 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.

### 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 the computer that has 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 Cognos Configuration.
2. In the Explorer window, under Environment, click 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.
5. From the File menu, click Save.

### Specify Resources for the Cognos 8 Service

To improve performance in a distributed environment, you can change the amount of resources that the Cognos 8 service uses by choosing a configuration template.

By default, the Cognos 8 service is configured to use minimal memory resources to optimize startup time.

The Cognos 8 service is available only on the computers where you installed Content Manager or Report Server.

**Steps**

1. Start Cognos Configuration.
2. In the Explorer window, under Environment, Cognos 8 service, right-click Cognos 8, and click Delete.
   
   This deletes the default configuration template for the service.
3. Right-click 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.
Chapter 7: Configuring Cognos 8 Controller

- 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.

Global Settings

You can change global settings to customize the following:
- language support for the user interface
- the default time zone
- cookie settings

By default, Cognos 8 Controller components ensure that all locales, which may come from different sources and in various formats, use a normalized form. That means that all expanded locales conform to a language and regional code setting.

Each computer has a default system locale and one user locale for each user. The user locales may be different from the default system locale.

Customize Language Support to the User Interface

Use the Product Locales table to add or remove the user interface language support. For example, if you do not require a German user interface, you can remove the language from the list.

Before you can add language support to the user interface, you must install the language files on all computers in your distributed installation. For more information, contact your Cognos support representative.

Adding languages to the Cognos environment does not guarantee that your computer has a font that can display Web pages in your preferred languages. Ensure that you install the appropriate language packs to support the character sets you use.

If you change the user interface language of the product, data is not affected.

Steps
1. On the Content Manager computer, start Cognos Configuration.
2. From the Actions menu, click Edit Global Configuration.
3. Click the Product Locales tab.
4. Click Add.
   Tip: To remove support, select the check box next to the Supported Locale and then click Remove.
5. In the second column, type the language portion of a locale.
6. Repeat steps 3 to 5 for other language support that you want to add.
7. Click OK.
8. From the File menu, click Save.

Customize the Server Time Zone

You can customize the time zone used by Content Manager by selecting a different server time zone in Cognos Configuration.

Content Manager is configured to use the time zone of your operating system by default. All scheduled activities in Cognos 8 Controller are set using this time zone. In addition, users in Cognos Connection use this time zone if they set their preferences for the default time zone. For more information about setting user preferences in Cognos Connection, see the Administration and Security Guide.

Steps
1. Start Cognos Configuration.
2. From the Actions menu, click Edit Global Configuration.
3. In the Global Configuration window, click the Server tab.
4. Click the Value column for Server time zone and select another time zone from the list.
5. From the File menu, click Save.

**Customize Cookie Settings**

Based on the requirements of your Cognos environment, you may need to modify the settings that Cognos 8 Controller components use to create cookies. You can use Cognos Configuration to customize the cookie domain, path, and secure flag.

Cognos 8 Controller components determine the cookie domain from the HTTP request submitted by the client, which is typically a Web browser. In most network configurations, HTTP requests pass through intermediaries such as proxy servers and firewalls as they travel from the browser to Cognos 8 Controller components. Some intermediaries modify the information that Cognos 8 Controller components use to calculate the cookie domain, and Cognos 8 Controller components then cannot set cookies. The usual symptom of this problem is that users are repeatedly prompted to log on. To avoid this problem, configure the cookie domain.

To set the correct value for the cookie domain, use the format and value that represents the widest coverage for the host.

<table>
<thead>
<tr>
<th>Host</th>
<th>Format for domain</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>computer or server</td>
<td>computer or server name (no dots)</td>
<td>mycompany</td>
</tr>
<tr>
<td>suffix is .com, .edu, .gov, .int, .mil, .net, or .org</td>
<td>.name.suffix (two dots)</td>
<td>.mycompany.com</td>
</tr>
<tr>
<td>other</td>
<td>.name1.name2.suffix (three dots)</td>
<td>.travelinfo.co.nz</td>
</tr>
</tbody>
</table>

**Steps**
1. On each Content Manager computer, start Cognos Configuration.
2. From the Actions menu, click Edit Global Configuration.
3. Click the Server tab.
4. Click in the Value column under Cookie Settings for each property that you want to change and specify the new value.
   - If you leave the Domain property blank, the dispatcher derives the domain from the host name of the request.
5. Click OK.

**Add or Remove Controller Database Connections**

You must set up a Controller database connection during the Cognos 8 Controller installation and configuration process. After the installation and configuration process is complete, you can add additional data source connections, or delete data source connections.

**Steps**
1. From the Start menu, start Cognos Controller Configuration.
2. In the Explorer window, click Database Connections, and then from the File menu, click New.
3. In the Properties window, click the Database type box, and then use the drop-down arrow to select the database type.
   - You can choose Oracle or SQL Server.
4. In the Name box, type a name for the database.
   - Choose a name that is meaningful for Cognos Controller users.
5. In the **Provider** box, type the name of the database provider.
   To obtain the database provider information, see the Oracle or SQL Server documentation.
6. In the **User ID** and **Password** boxes, type the user name and password for the Controller database.
7. In the **Initial catalog** box, type the Controller database name.
8. In the **Data source** box, type the database server computer name.
   **Tip:** Do not use localhost.
9. From the **File** menu, click **Save**.
10. In the **Explorer** window, under **Database Connections**, click the database.
11. From the **File** menu, click **Run**.
    The Database Conversion Utility opens.
12. In the **Database Conversion Utility** dialog box, click **Run Steps**.
    The Database Conversion Utility updates the database for use with Cognos 8 Controller.
13. Click **Close**.
14. From the **Actions** menu, click **Check**.
    If the database connection validation fails, review the database connection properties and fix any errors.
15. From the **File** menu, click **Save**.
16. In the **Explorer** window, under **Web Services Server**, click **Report Server**.
    The new database is now configured as a data source for Report Server, and is listed as a data source in Cognos Connection.

**Steps to Delete a Database Connection**
1. From the **Start** menu, start Cognos Controller Configuration.
2. In the **Explorer** window, click **Database Connections**, and then click the database connection you want to delete.
3. From the **File** menu, click **Delete**.
4. From the **File** menu, click **Save**.

**Change the COM+ Server Configuration**

You configure the COM+ Server during the initial Cognos 8 Controller installation and configuration. However, you can change the account under which the COM+ service runs at any time.

**Steps**
1. From the **Start** menu, start Cognos Controller Configuration.
2. In the **Explorer** window, click **COM+ Server**.
3. In the **COM+ Server** window, click the **Shutdown** button.
4. In the **COM+ Server** window, configure the **COM+ Server**:
   - Select **System Account** to configure the COM+ server with the computer’s system account.
   - Select **Specify Account** to configure the COM+ server with a user account that has administrator privileges on the computer.
5. If you selected **Specify Account**:
   - In the **User** box, type the user name for the account.
   - In the **Password** and **Confirm Password** boxes, type the password for the account.
6. From the **File** menu, click **Save**.
Enable Batch Services

You can configure the number of batch services that run on the Controller Web Services Server computer. You can run up to four batch services at one time.

Steps
1. From the Start menu, start Cognos Controller Configuration.
2. In the Explorer window, click Batch Services.
3. In the Batch Services window, select a batch process.
4. From the Actions menu, click Run.
5. From the File menu, click Save.

Enable Enhanced Reporting Optimization

When Cognos 8 Controller Microsoft Excel reports contain a significant amount of data, the Enhanced Reporting Optimization feature provides for faster data transfer from the Cognos 8 Controller client to the Controller database.

When a report is run using Enhanced Reporting Optimization, Microsoft Excel sends a string to a file share on the database server. The file is inserted in the Controller database using bulk insert technology, and the report runs from that location.

Enhanced Reporting Optimization uses one of two methods: File Copy or File Transfer (FTP). Use the File Copy method for Microsoft SQL Server databases or for Oracle databases when the Oracle server is installed on a Windows operating system. Use the FTP method for Oracle databases when the Oracle server is installed on an operating system other than Windows, for example a Linux or UNIX operating system.

Configure the File Copy Method

Use the File Copy method for Microsoft SQL Server databases or for Oracle databases when the Oracle server is installed on a Windows operating system.

Before you configure the File Copy method, you must
• create a shared directory on the database server
• provide the Cognos Controller administrator with read and write access permissions to the shared folder on the database server, or create a local account with read and write access permissions to the shared folder on the database server
• set read and write access permissions on the shared folder for the database server
• for Microsoft SQL Server databases, enable the Bulk Insert Administrators server role for the Controller database owner
  In addition, set the Controller database owner as the owner of tempdb and model.
• for Oracle databases, set the UTL_FILE_DIR parameter to point to the local path of the shared directory
• configure reports to use Enhanced Reporting Optimization

Steps to Configure Reports to Use Enhanced Reporting Optimization
2. From the Insert menu, click Name, Define...
3. In the Define Name box, under Names in workbook, type Optimise2, and then click OK.

Steps to Configure the File Copy Method
1. From the Start menu, start Cognos Controller Configuration.
2. In the Explorer window, click Enhanced Reporting Optimizations.
3. In the Enhanced Reporting Optimizations window, in the Select Connection drop-down list, select a database.
4. Under Connection Optimizations, in the File Mode box, click the drop-down arrow and select File Copy.
5. In the Server box, type the name of the server on which you created the shared directory.
6. In the Share box, type the name of the share you created in Step 1.
7. For Oracle databases, in the Server Directory box, type the path to the shared directory that will be used by the Oracle database.
   Example: e:\oracle\ora92\utlfile
   Note: The name of the shared directory is case sensitive. Use the same value that you set for the UTL_FILE_DIR parameter.
8. If the database is in another domain, in the User ID and Password boxes, type the logon user name and password for the domain user.
   The password is encrypted with Cognos Controller standard encryption.
9. From the File menu, click Save.

Configure the File Transfer Protocol (FTP) Method

Use the FTP method for Oracle databases when the Oracle server is installed on an operating system other than Windows, for example a Linux or UNIX operating system.

Before you configure the FTP method, you must:
• set up an FTP server on the database server
• create a shared directory on the database server with a user that has read and write access permissions
• set read and write access permissions on the shared folder for the database server
• for Oracle databases, set the UTL_FILE_DIR parameter to point to the local path of the shared directory
• configure reports to use Enhanced Reporting Optimization

Steps to Configure Reports to Use Enhanced Reporting Optimization
2. From the Insert menu, click Name, Define...
3. In the Define Name box, under Names in workbook, type Optimise2, and then click OK.

Steps to Configure the File Transfer Protocol (FTP) Method
1. From the Start menu, start Cognos Controller Configuration.
2. In the Explorer window, click Enhanced Reporting Optimizations.
3. In the Enhanced Reporting Optimizations window, in the Select Connection drop-down list, select a database.
4. Under Connection Optimizations, in the File Mode box, click the drop-down arrow and select File Transfer (FTP).
5. In the Server box, type the computer name for the FTP Server.
6. In the FTP Sub Directory box, type the name of the FTP sub-directory.
7. In the Server Directory box, type the path to the shared directory that will be used by the Oracle database.
   Example: e:\oracle\ora92\utlfile
   Note: The name of the shared directory is case sensitive. Use the same value that you set for the UTL_FILE_DIR parameter.
8. In the User ID and Password boxes, type the FTP account user name and password.
   The password is encrypted with Cognos Controller standard encryption.
9. In the Access Type box, click the drop-down arrow and select the FTP access type.
   Select Direct, Proxy, or Windows Standard.
10. In the Passive Mode box, click the drop-down arrow and choose whether to enable passive mode:
    • Select True to enable passive mode when connecting to the FTP server.
    • Select False to disable passive mode when connecting to the FTP server.
11. In the Port box, specify the port for the FTP connection.
12. If you selected the Proxy access type, in the Proxy box, type the name for the FTP proxy computer.
13. If you selected the Proxy access type, in the Proxy bypass box, type the names of the FTP proxy computers to avoid.
14. From the File menu, click Save.

**Change the Default Installation of the Cognos 8 Controller Add-in for Excel**

When users first run the Cognos 8 Controller client, the Cognos 8 Controller Add-in for Excel is installed automatically. If you installed the Add-in for Excel remotely for users by using Active Directory or Patchlink, you may want to disable the automatic installation.

**Steps**
1. On the computer where Controller Client Distribution Server is installed, from the Start menu, start Cognos Controller Configuration.
2. In the Explorer window, expand Cognos Controller Configuration, Client Distribution Server.
3. Click Client Distribution Server Configuration.
4. Click InstallExcelLink.
5. Change the value to False.
6. From the File menu, click Save.

**Configuring Consolidation Load Balancing**

You can install Controller Web Services Server on one or more computers. For consolidation load balancing, we recommend that you install this component on two computers. You can then configure one computer to accept user requests and configure the second computer as the consolidation server.

First you must replace the Cognos Controller COM+ application on the consolidation server with a CognosVFP COM+ application. Then you must export the new application to the user request server.

The new CognosVFP COM+ application should run under a designated domain user account. The user must be a local administrator on the servers and in the user domain for the network. The designated domain user account should be used on all Controller Web Services Server computers.

Use the following checklist to guide you through the configuration tasks:
- Create the CognosVFP COM+ application for consolidation load balancing.
- Transfer the CognosVFP COM+ application for load balancing.

**Create the CognosVFP COM+ Application for Load Balancing**

You load balance the consolidation functions of Cognos 8 Controller by moving the COM+ components that are used for consolidation to a second Controller Web Services Server computer. On this second computer, you create a CognosVFP COM+ application, configure users and permissions, select the component to install, and then create a package that contains all of these items. Use the package, a .msi file, to install the new COM+ application on the first Controller Web Services Server computer.

Before you create the new COM+ application, ensure that you installed the Controller Web Services Server component on two computers.

**Steps**
1. On the Controller Web Services Server computer that you want to use for consolidation, in Administrative Tools, start Component Services.
2. In the Console Root tree, expand Component Services and then expand COM+ Applications.
3. Under COM+ Application, delete COGNOSCONTROLLER.
4. Right-click COM+ Applications and click New, Application.
5. In the COM+ Application Install Wizard, click Next.
6. Click Create an empty application.
7. In the name box, type CognosVFP, select Server application, and then click Next.
8. Select This user, type the account information for ControllerCOM, and then click Next.
9. Select CreatorOwner and click Remove.
10. Click Add role and, in the name box, type CognosUsers, and then click Next.
11. Expand CognosUsers.
12. Right-click your account and click Delete.
13. Click Add and enter the information for the designated domain user account.
14. Click OK and then click Next.
15. Click Finish.
16. In the Console Root tree, expand CognosVFP.
17. Right-click Components and select New, Component.
18. In the COM+ Component Install Wizard, click Next.
19. Click Install new components.
20. Click Add, browse to the c8_location\server directory, click the frangovfp.dll file, and then click Open.
21. Click Next and then click Finish.
22. In the Console Root tree, right-click CognosVFP and click Export.
23. In the COM+ Application Export Wizard, click Next.
24. Type CognosVFP.msi, select Application proxy - Install on other machines to enable access to this machine, and then click Next.
   The .msi file is created in the c8_location\server directory.
25. Click Finish.
26. Make the CognosVFP.msi file available on the LAN.

Transfer the CognosVFP COM+ Application

After you create the .msi file for the new CognosVFP COM+ application, you must copy the file to the Controller Web Services Server computer that you are using for user requests and then run the file.

Steps
1. On the Controller Web Services Server computer that you are using for user requests, copy the CognosVFP.msi file to the c8_location\server directory.
   You must copy the file to the computer. You cannot run the .msi file from a shared server on the LAN.
2. In Administrative Tools, start Component Services.
3. In the Console Root tree, expand Component Services and then expand COM+ Applications.
4. Under COM+ Application, expand CognosController and click Components.
5. Delete the frangovfp.cglobvar and frangovfp.main files.
6. In the c8_location\server directory, double-click the CognosVFP.msi file.
7. Confirm that the CognosVFP COM+ application is installed and started:
   • In Component Services, in the Console Root tree, right-click CognosVFP and click Properties.
   • On the Activation tab, confirm that the remote server name is the name of the Controller Web Services Server computer that you are using for consolidation.
8. On the Controller Web Services Server computer that you are using for consolidation, from the Start menu, start Cognos Controller Configuration.
9. In the Explorer window, click Batch Services.
10. For each Controller Batch Process, from the Actions menu, click Stop.
Configuring Multiple Server Operation with the Reporting Database

In a distributed installation, you can scale your Cognos 8 Controller application by sharing operations with the reporting database across multiple computers.

To share the operations, you must first change the user manager for Cognos 8 Controller so that multiple application servers can operate with the same reporting database. Then you must configure each application server to operate with the same reporting database. Finally, you must set up the client computers so that users can log in to Cognos 8 Controller using any of the application servers.

The new COM+ application should run under a designated domain user account. The user must be a local administrator on the servers and in the user domain for the network. The designated domain user account should be used on all Controller Web Services Server computers.

You must first install (p. 35) and configure (p. 68) the Controller Web Services Server component on each of the computers that will operate with the reporting database. For each Controller Web Services Server computer in your network, there must be a corresponding Controller Client Distribution Server computer in a one-to-one mapping.

Use the following checklist to guide you through the configuration tasks:

- Create a new COM+ application for the user manager
- Install the new COM+ application on the servers that operate with the reporting database
- Configure the servers to operate with the reporting database
- Set up trust on the client computers

Create the COM+ Application for the User Manager

The COM+ application for the Controller user manager supports the operation of a single application server with the reporting database. If you want more than one application server to operate with the reporting database, you must delete the existing COM+ application for the user manager and create a new one.

Steps

1. On one of the Controller Web Services Server computers, in Administrative Tools, start Component Services.
2. In the Console Root tree, expand Component Services, Computers, My Computer, COM+ Applications, COGNOSCONTROLLER, Components.
3. Right-click FrLicServerProxy, click Delete, and then click Yes.
4. Right-click COM+ Applications and select New, Application.
5. In the COM+ Application Install Wizard, click Next.
6. Click Create an empty application.
7. In the name box, type a name, select Server application, and then click Next.
   An example of a name is CCRLOADBALANCER.
8. Select This user, enter the information for the designated domain user account, and then click Next.
9. Click Next, click Next, and then click Finish.
10. Expand the new application.
11. Expand Roles.
12. Right-click CreatorOwner and click Delete.
13. Right-click Roles and select New, Role.
14. In the name box, type ControllerUsers and click OK.
15. Expand ControllerUsers.
16. Right-click Users and select New, User.
17. In the Enter the object names to select box, type the name of the designated domain user account and click OK.
18. Under the new application, right-click Components and select New, Component.
Chapter 7: Configuring Cognos 8 Controller

19. In the COM+ Component Install Wizard window, click Next.
20. Click Install new component(s).
21. In the Select files to install window, browse to \c8_installation\server directory, select the FrLicServerProxy.dll file, and then click Open.
22. In the COM+ Component Install Wizard window, click Next, and then click Finish.
23. Right-click the new application, and select Export.
24. In the COM+ Application Export Wizard window, click Next.
25. Browse to a directory that is shared on the network, type the new application name, and click Save.
26. Click the Export user identities with roles check box and click Next.
27. Click Finish.

Install the COM+ Application on Multiple Servers

After you create a new COM+ application for the Controller user manager on one computer, you must export the COM+ application to the other computers that will operate with the reporting database.

You must first install (p. 35) and configure (p. 68) the Controller Web Services Server component on each of the other computers that will operate with the reporting database.

Steps
2. In the Console Root tree, expand Component Services, Computers, My Computer, COM+ Applications, COGNOSCONTROLLER, Components.
3. Right-click FrLicServerProxy, click Delete, and then click Yes.
4. Right-click COM+ Applications and select New, Application.
5. In the COM+ Application Install Wizard window, click Next.
6. Click Install pre-built application(s).
7. In the Install from application file window, browse to the shared directory and select the new COM+ application, and click Open.
8. Click Next.
9. Select This user, enter the information for the designated domain user account, and click Next.
10. Select Default directory (as specified by application file) and click Next.
11. Click Finish.
12. Repeat steps 1 to 11 on every Controller Web Services Server computer that will operate with the reporting database.

Configure Multiple Application Servers to Operate With the Reporting Database

After the user manager is changed on all of the application servers that will operate with the reporting database, you must configure the servers to use the same reporting database instance.

Step
- On the reporting database computer, configure the Controller Web Services Server computers to use the same reporting database instance by editing the UDL files.
  For more information, see the documentation for your database software.

Configure Trust for the Client Computers

Before users on client computers can log on to the appropriate Controller Client Distribution Server, their computer must trust the new servers. On each Controller Client Distribution Server computer, you must create a runtime security policy in Microsoft .NET Framework. You must then create an export package and deploy it to the client computers.

Ensure that you assign unique names to each runtime security policy.
Step

- On each new Controller Client Distribution Server computer, configure a runtime security policy and deploy it to the client computers.
  For instructions, see "Configure Microsoft .NET Framework" (p. 48)
Chapter 8: Configuring Authenticated Access

Cognos 8 Controller uses three methods of authenticated logon: native, Cognos 8, and Windows authentication. When you configure your Cognos 8 Controller environment to use a particular authentication method, you must configure a corresponding authentication level for the reporting components.

By default, Cognos 8 Controller uses native authentication. The corresponding default for the reporting components is anonymous access.

We recommend that you use a higher level of security than the default native authentication settings. If you want to use the Cognos 8 authentication method, you must use a Cognos 8 namespace for authentication with the reporting components. If you want to use the Windows authentication method, you must use NTLM authentication for the reporting components.

The first step for setting up Cognos 8 or Windows authentication is to configure the Cognos 8 Controller components with an authentication namespace for the type of authentication provider you want to use. If you installed Cognos 8 Controller in an environment that includes Cognos 8 Business Intelligence, the namespace is configured for Cognos 8 Business Intelligence. Unless you want to change authentication providers, you do not have to configure an authentication namespace now. For information about configuring a namespace for various third-party authentication providers, see "Configuring Cognos 8 Components to Use an Authentication Namespace" (p. 104).

If you want to use the Cognos 8 authentication method, you must add the Cognos 8 Controller users to the Cognos 8 Controller roles. After you add the users to the roles, the first user to log on to Controller is automatically mapped to the Controller Administrative User account and inherits the privileges of that account.

For both the Cognos 8 and the Windows authentication methods, you must map the users that are defined in Cognos 8 Controller to the users that are defined in the Cognos 8 namespace roles.

After you have configured an authentication namespace, you must complete the following tasks to configure Cognos 8 Controller to run with Cognos 8 or Windows authentication:

- configure the Cognos 8 Controller authentication method
- add Cognos Controller users to Cognos Controller roles, for the Cognos 8 authentication method only
- map Cognos Controller users to Cognos 8 users

Configure the Cognos 8 Controller Authentication Method

After you configure the authentication provider, you must configure the Controller Web Services Server computers with Cognos 8 or Windows authentication. The default authentication method is Native authentication.

Native Authentication

With native authentication, logon information is configured in the Cognos Controller databases and in the Cognos Controller user interface. Native authentication is the authentication method used in previous versions of Cognos Controller.

If you use Native authentication, when users log on to Cognos Controller from Cognos Connection or from a URL and have selected a database to log on to, they are prompted to log in. Users are prompted with the same logon window when they log on to Cognos Controller using the Cognos Controller Microsoft Excel Add-in.
If you want to use Native authentication in your Cognos 8 Controller environment, the reporting components must run under anonymous access. When the reporting components run under anonymous access, no logon is required. In Cognos Connection, anonymous access is enabled by default.

Native authentication provides minimal security in your Cognos 8 Controller environment.

**Cognos 8 Authentication**

Cognos 8 authentication is shared between Cognos Controller and the reporting components. When you use the Cognos 8 authentication method, you can use the Cognos built-in namespace to restrict access to defined users, or you can create an appropriate namespace for the type of authentication provider in your environment. Access is then restricted to users belonging to any group or role defined in the namespace.

If you use the Cognos 8 authentication method, when users log on to Cognos Controller from Cognos Connection or from a URL and have selected a database to log on to, they are prompted to log on. Users are prompted with the same logon window when they log on to Cognos Controller using the Microsoft Excel Add-in.

Cognos 8 authentication uses shared memory for passport IDs. However, if your company security policy prohibits the use of shared memory, you can disable the use of shared memory for passport IDs. If you disable shared memory for passport IDs, users must log on separately to Cognos Controller and to the Cognos Controller Microsoft Excel Add-in.

**Windows Authentication**

Windows Authentication is the built-in authentication provided through the configuration of Internet Information Services (IIS).

When Windows Authentication is enabled, user connections established with the Microsoft Internet Information Services Web server on Controller Web Services Server are validated, and then authenticated against the namespace configured in Cognos Configuration.
If Windows Authentication is enabled, after users log on to client computers with their Windows user name and password, they are not prompted with further logons when they run Cognos Controller or the Cognos Controller Excel Add-in.

Ensure that you have configured the appropriate namespace. For the Cognos 8 authentication method, you may use type of namespace except NTLM. For the Windows authentication method, you must use an NTLM namespace.

**Steps**
1. From the **Start** menu, start Cognos Controller Configuration.
2. In the **Explorer** window, click **Web Services Server**, **Server Authentication**.
3. In the **Select authentication method** box, click the drop-down arrow, and then select the authentication method:
   - Click **Cognos 8** to enable Cognos 8 authentication.
   - Click **Windows Authentication** to enable Windows Authentication.
4. In the **Dispatcher URI** box, type the URI for the Report Server dispatcher. For example, type: `http://<servername>9300/p2pd/servlet/dispatch`
5. From the **File** menu, click **Save**.

### Add Cognos Controller Users to the Cognos Controller Roles

Users, groups, and roles are created for authentication purposes. In Cognos 8 Controller, you can use users, groups, and roles created in third-party authentication providers, and groups and roles created in Cognos 8 Controller. The Cognos Controller groups and roles created in Cognos 8 Controller are referred to as Cognos Controller groups and Cognos Controller roles.

When you use the Cognos 8 authentication method, you must add Cognos Controller users to the Cognos Controller roles.

**Steps**
1. Start Cognos Connection.
2. From the **Tools** menu, click **Directory**.
3. On the **Users, Groups, and Roles** tab, click the **Cognos** namespace.
4. In the **Actions** column, click the properties button for the **Controller Administrators** role.
5. Click the **Members** tab.
6. To add members, click **Add** and choose how to select members:
   - To choose from listed entries, click the appropriate namespace, and then select the check boxes next to the users, groups, or roles.
   - To search for entries, click **Search** and in the Search string box, type the phrase you want to search for. For search options, click **Edit**, **Find**, and click the entry you want.
   - To type the name of entries you want to add, click **Type** and type the names of groups, roles, or users using the following format, where a semicolon (;) separates each entry: `namespace/group_name;namespace/role_name;namespace/user_name;`
     Here is an example: `Cognos/Authors;LDAP/scarter;`
7. Click the right-arrow button and when the entries you want appear in the **Selected entries** box, click **OK**.
8. On the **Members** tab, click the **Everyone** namespace, and then click **Remove**.
9. Click **OK**.
10. Close the **Properties** window to return to the Users, Groups, Roles tab.
11. Repeat steps 4 to 8 for the **Controller Users** role.
    
    **Tip:** The **Controller Administrators** role must be a member of the **Controller Users** role.
12. Click **OK**.

After the users are added to the roles, the first user to log on to Controller is automatically mapped to the Controller Administrative User account and inherits the privileges of that account.
Map Cognos Controller Users to Cognos 8 Users

When you use the Cognos 8 or Windows authentication method, you must create an association between the users defined in the Cognos Controller application and those defined in the Cognos 8 namespace roles.

Cognos 8 Controller supports logons to only one namespace.

**Important:** The first user who logs on to Cognos Controller using Cognos 8 Authentication is automatically mapped to the Cognos Controller Administrative User, the named user defined by default in Controller. Associations between users can be created only by a user who was configured in Cognos Connection as a member of the Controller Administrators role. It is important, therefore, that the first user who logs on was configured to be a member of the Controller Administrators role. Otherwise, the automatic mapping to the Cognos Controller Administrative User will not occur and the user's logon will fail.

For more information about setting user rights and limitations in Cognos Controller, see the Cognos Controller User Guide.

**Steps to Map a Cognos Controller User to a Cognos 8 User**

1. Start Cognos Controller.
   
   **Note:** You must be a member of the Controller Administrators role in Cognos Connection.

2. From the Maintain menu, click Rights, Users.

3. Select the user as defined in the Cognos Controller database.

4. Next to the CAM User box, click Show Valid Choices and then select the user as defined in the Cognos 8 namespace roles.

5. Click Save.

**Steps to Create a Cognos Controller User Based on a Cognos 8 User**

1. Start Cognos Controller.
   
   **Note:** You must be a member of the Controller Administrators role in Cognos Connection.

2. From the Maintain menu, click Rights, Users.

3. Click New.

4. Next to the CAM User box, click Show Valid Choices, and then select the user as defined in the Cognos 8 namespace roles.

5. Change the default values for Name and E-Mail Address, as required.

6. Next to the User Group box, click the browse button, and then click the user group for the Cognos Controller user.

7. Under Options, select the appropriate check box to identify the user:
   
   • Cognos Controller User
   • Cognos Controller Administrator

   If you select Cognos Controller Administrator, ensure that the user is a member of the Controller Administrators role in Cognos Connection.

   You can add other optional information.

8. Click Save.

Configuring Cognos 8 Components to Use an Authentication Namespace

When authenticated access is enabled and configured, user authentication is managed by third-party authentication providers. You must configure 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 which namespace you want to use. Cognos 8 Controller supports logons to only one namespace. For more information, see the Administration and Security Guide.
After you configure new namespaces, you can test namespaces. You can also delete namespaces that you added if they are no longer required (p. 127). After you delete a namespace using Cognos Configuration, you must complete the process by deleting it in the portal.

Important: You must not delete the Cognos namespace. It contains authentication data that pertains to all users and is required to save the configuration.

After Cognos 8 Controller is connected to a namespace, you cannot change the connection to another namespace.

Cognos 8 components support the following types of servers as authentication sources:
- Active Directory Server
- Cognos Series 7
- Custom Authentication Provider
- LDAP
- Netegrity SiteMinder
- NTLM

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 entries that are marked as unknown. 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 Cognos 8 components, you can enable single signon between your authentication provider environment and 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. For more information, see the Cognos 8 Controller Architecture and Planning Guide.

If you are configuring a namespace for use with the Cognos 8 authentication method, you can use any type of server except NTLM. If you are configuring a namespace for use with the Windows authentication method, you must use an NTLM namespace.

Some authentication providers require libraries external to the Cognos 8 Controller environment to be available.

To configure Cognos 8 components to use an authentication namespace, you must
- disable anonymous access
- Enable single signon
- configure Cognos 8 components to use the appropriate namespace:
  - Active Directory Server
  - Cognos Series 7
  - Custom authentication provider
  - LDAP
  - Netegrity SiteMinder
  - NTLM
  for the Windows authentication method only

**Enable Single Signon**

If you want users to log on once to Cognos 8 Controller and then be able to switch to another Cognos 8 product without logging on again, you can enable single signon.

Single signon in Cognos 8 Controller is supported between the Controller client and Controller Excel client only.
Chapter 8: Configuring Authenticated Access

Steps
1. On each computer where you installed Content Manager, start Cognos Configuration.
2. In the Explorer window, under Security, click Authentication.
3. In the Properties window, set the value of Allow session information to be shared between client applications to True.

Disable Anonymous Access

You can use both anonymous and authenticated logon with your Cognos 8 components installation. If you choose to use only authenticated logon, you can disable anonymous access.

By default, Cognos 8 reporting components do not require user authentication. Users can log on anonymously. If you want to use authenticated logon only, you can use Cognos Configuration to disable anonymous access.

To support single signon in Cognos 8 Controller, you must disable anonymous access.

Steps
1. On the computer where you installed Content Manager, start Cognos Configuration.
2. In the Explorer window, under Security, Authentication, click Cognos.
   - The Cognos resource represents the Cognos namespace. The Cognos namespace stores information about 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 Cognos resources.

Restrict User Access to the Cognos Namespace

Access can be restricted to users belonging to any group or role defined in the 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 Cognos built-in roles and groups
- ensure that authorized users belong to at least one Cognos role or group

Steps
1. On the computer where you installed Content Manager, start 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 Cognos built-in roles and groups and then ensure that authorized users belong to at least one Cognos built-in role or group.

For information about adding or removing members of a Cognos group or role, see the Cognos 8 Administration and Security Guide.

Configuring Cognos 8 Components to Use Active Directory Server

When you install Content Manager on a Windows computer, you can configure Active Directory as your authentication source using an Active Directory namespace.

If you want to use Microsoft SQL Server as a data source and use single signon for authentication, you must use Active Directory as your authentication source.
To use an Active Directory Server namespace and to set up single signon, do the following:

- **Configure Cognos 8 Controller components to use an Active Directory Server namespace.**
- **Enable single signon between Active Directory Server and Cognos 8 Controller 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 Cognos 8 Controller components.

**Note:** For Cognos 8 components to work properly with Active Directory Server, 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 data source, the following configuration is required:

- The Cognos 8 gateway must be installed on an IIS Web server that is configured for Windows Integrated Authentication.
- Content Manager must be installed on a Windows 2000 or Windows 2003 server.
- Content Manager, Report Server (Application Tier Components), IIS Web server, and the data source server (Microsoft SQL Server) must belong to the Active Directory domain.
- The data source connection for Microsoft SQL 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 the computer where you installed Content Manager, start 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 Cognos 8 components can locate and use your existing authentication provider.
7. Specify the values for the **Host and port** property.
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**.
    - Cognos 8 Controller loads, initializes, and configures the provider libraries for the namespace.

### Make Custom User Properties for Active Directory Available to Cognos 8 Controller Components

You can use arbitrary user attributes from your Active Directory Server in Cognos 8 components. To configure this, you must add these attributes as custom properties for the Active Directory namespace.

You can also use custom properties 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*. 
Chapter 8: Configuring Authenticated Access

Steps
1. On the computer where you installed Content Manager, start 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 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 the preceding two bulleted steps for each custom parameter.
8. Click OK.
9. From the File menu, click Save.

Include or Exclude Domains Using Advanced Properties
When you configure an authentication namespace for Cognos 8 components, 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 chase_referrals to true, users in the original authenticated domain and all child domains of the domain tree can log in to 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 multi_domain_tree to true, users in all domain trees in the forest can log in to Cognos 8.

Steps
1. On the computer where you installed Content Manager, start 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:

<table>
<thead>
<tr>
<th>Authentication for</th>
<th>chaseReferrals</th>
<th>MultiDomainTrees</th>
</tr>
</thead>
<tbody>
<tr>
<td>One domain</td>
<td>False</td>
<td>False</td>
</tr>
<tr>
<td>One domain tree</td>
<td>True</td>
<td>False</td>
</tr>
<tr>
<td>All domain trees in the forest</td>
<td>True</td>
<td>True</td>
</tr>
</tbody>
</table>

7. Click OK.
Enabling Single Signon Between Active Directory Server and Cognos 8 Controller Components

By default, the Active Directory provider uses Kerberos delegation and integrates with the IIS Web server for single signon if Integrated Authenticated (formerly named NT Challenge Response) is enabled on the IIS Web server.

If Integrated Authenticated is enabled, you are not prompted to reenter authentication information when accessing 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. Microsoft sets REMOTE_USER by default when you enable Windows Integrated Authentication.

Steps for Single Signon Using Kerberos Delegation
2. Install Content Manager on a computer that is part of the domain.
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 the computer where you installed Content Manager, start 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 window, click Add.
5. In the Name column, type singleSignonOption
6. In the Value column, type IdentityMapping.
7. 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 Cognos 8 to Use a Cognos Series 7 Namespace

You can configure Cognos 8 components to use a Cognos Series 7 namespace as the authentication provider. Users are authenticated based on the authentication and signon configuration of the Cognos Series 7 namespace.

Note: You cannot use a Cognos Series 7 Local Authentication Export (LAE) file for authentication with Cognos 8 components.

You can configure Cognos 8 components to use multiple Cognos Series 7 authentication providers. We recommend that all Cognos Series 7 namespaces use the same primary Cognos Series 7 Ticket Server. Otherwise, you may receive errors or be prompted for authentication more than once.

If you change the configuration information stored in the directory server used for Cognos Series 7, you must restart the Cognos 8 service before the changes take effect in the Cognos installation.

A user must be in at least one Access Manager user class to be able to log on to Cognos 8 Controller components.

To use a Cognos Series 7 namespace and to set up single signon, do the following:
- Configure Cognos 8 to use a Cognos Series 7 namespace.
- Enable single signon between Cognos Series 7 and Cognos 8 Controller.
Chapter 8: Configuring Authenticated Access

**Configure a Cognos Series 7 Namespace**

You can configure Cognos 8 components to use a Cognos Series 7 namespaces for authentication.

**Steps**

1. On the computer where you installed Content Manager, start Cognos Configuration.
2. On every computer where you installed Content Manager, open Cognos Configuration.
3. In the **Explorer** window, under **Security**, right-click **Authentication**, and then 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.
7. Specify the values for all other required properties to ensure that Cognos 8 components can locate and use your existing authentication provider.

   If your 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 Series 7 namespace.

   The host value can be a computer name or an IP address. If you are publishing from PowerPlay Enterprise Server to Cognos 8, you must use the same value format that is used in Cognos Series 7 Configuration Manager for the location of the directory server. For example, if the computer name is used in Cognos Series 7 Configuration Manager, the computer name must also be used in Cognos Configuration for Cognos 8.
8. If your namespace environment includes version 15.2 of the 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**.
9. In the **Properties** window, under **Cookie settings**, ensure that the **Path**, **Domain**, and **Secure flag enabled** properties match the settings configured for Cognos Series 7.
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**.

**Steps**

1. On every computer where you installed Content Manager, open 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 Cognos 8 components can locate and use your existing authentication provider.

   If your 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 Series 7 namespace.
The host value can be a computer name or an IP address. If you are publishing from PowerPlay Enterprise Server to Cognos 8, you must use the same value format that is used in Cognos Series 7 Configuration Manager for the location of the directory server. For example, if the computer name is used in Cognos Series 7 Configuration Manager, the computer name must also be used in Cognos Configuration for Cognos 8.

7. If your namespace environment includes version 15.2 of the Series 7 namespace, you must disable the Series7NamespacesAreUnicode setting.
   a. In the Properties window, in the Advanced Properties value, click the edit button.
   b. In the Value - Advanced properties window, click Add.
   c. In the Name box, type Series7NamespacesAreUnicode.
   d. 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 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.

Cognos 8 Controller loads, initializes, and configures the provider libraries for the namespace.

**Enable Single Signon Between Cognos Series 7 and Cognos 8 Components**

If your Cognos Series 7 namespace has been configured for integration with your external authentication mechanisms for single signon, the Cognos Series 7 provider automatically uses this configuration.

By configuring single signon, you are not prompted to reenter authentication information when accessing Cognos content that is secured by the Cognos Series 7 namespace.

**Steps**

1. Ensure that you configured Cognos 8 components to use a Cognos Series 7 namespace as an authentication provider (p. 109).

2. For Cognos Series 7, start Configuration Manager.

3. Click Open the current configuration.


5. In the Properties window, ensure that the Path, Domain and Secure Flag Enabled properties match the settings configured for Cognos 8 Controller.

6. Save and close Configuration Manager.

7. If the Cognos Series 7 namespace uses the Trusted Signon plug-in for single signon, you must now define the SaferAPIGetTrustedSignonWithEnv function.

You can now add Cognos Upfront Series 7 NewsBoxes to your Cognos Connection portal pages.

**Cognos Series 7 Namespaces and the Cognos Series 7 Trusted Signon Plug-in**

If the 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 Cognos 8 Controller components and your authentication mechanism.

The SaferAPIGetTrustedSignonWithEnv function is an updated version of the SaferAPIGetTrustedSignon function. This update is required because Cognos 8 logon is not performed at the Web server as is the case for 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 Cognos Series 7 and Cognos 8 products using the same plug-in, both the SaferAPIGetTrustedSignonWithEnv and SaferAPIGetTrustedSignon functions are required. For information about the SaferAPIGetTrustedSignon function, see the 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(

<table>
<thead>
<tr>
<th>Parameter Type</th>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EnvVar</td>
<td>envVar[]</td>
<td><em>/[IN]</em>/</td>
</tr>
<tr>
<td>char</td>
<td>**reqEnvVarList,</td>
<td><em>/[OUT]</em>/</td>
</tr>
<tr>
<td>void</td>
<td>**trustedSignonName,</td>
<td><em>/[OUT]</em>/</td>
</tr>
<tr>
<td>unsigned long</td>
<td>*trustedSignonNameLength,</td>
<td><em>/[OUT]</em>/</td>
</tr>
<tr>
<td>void</td>
<td>**trustedDomainName,</td>
<td><em>/[OUT]</em>/</td>
</tr>
<tr>
<td>unsigned long</td>
<td>*trustedDomainNameLength,</td>
<td><em>/[OUT]</em>/</td>
</tr>
<tr>
<td>SAFER_USER_TYPE</td>
<td>*userType,</td>
<td><em>/[OUT]</em>/</td>
</tr>
<tr>
<td>void</td>
<td>**implementerData);</td>
<td><em>/[IN/OUT]</em>/</td>
</tr>
</tbody>
</table>

Parameter Description

[in] envVar 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 envVarName and a null envVarValue. Note that the first time this API is called, the envVar array contains only the end of array marker.

[in] reqEnvVarList 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] trustedSignonName A sequence of bytes that identifies the currently authenticated user. This value does not need to be null-terminated. This value is mandatory.

[out] trustedSignonNameLength An integer value that indicates the length of the trustedSignonName. This length should exclude the null terminator, if there is one. This value is mandatory.
Configuring Cognos 8 to Use a Custom Authentication Provider

If you implemented a custom Java authentication provider with your existing security infrastructure, you can configure 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 Cognos 8 components with your security infrastructure.

For more information, see the Custom Authentication Provider Developer Guide.

Configure a Custom Authentication Namespace

You can configure 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 you installed Content Manager, open 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 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.

Cognos 8 loads, initializes, and configures the provider libraries for the namespace.

### Configuring Cognos 8 Components to Use LDAP

You can configure Cognos 8 components to use an LDAP namespace as the authentication provider.

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 Cognos 8 using external identity mapping see the same users, groups, and folders as the Bind user.

**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.

You also have the option of making custom user properties from the LDAP namespace available to Cognos 8 components.

To use an LDAP namespace and set up single signon, do the following:

- Configure Cognos 8 components to use an LDAP namespace
- Make custom user properties available to Cognos 8 components, if required
- Enable secure communication to the LDAP server, if required
- Enable single signon between LDAP and Cognos 8 components, if required

### Configure an LDAP Namespace

You can configure 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 ONE Directory Server, see [Configure an LDAP Namespace for Sun ONE Directory Server](#)
Chapter 8: Configuring Authenticated Access

Steps
1. On every computer where you installed Content Manager, open 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 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. 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 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.
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.
    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 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 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. 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.

<table>
<thead>
<tr>
<th>Mappings</th>
<th>LDAP property</th>
<th>LDAP value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder</td>
<td>Object class</td>
<td>organizationalUnit, organization, container</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>description</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>ou, o, cn</td>
</tr>
<tr>
<td>Group</td>
<td>Object class</td>
<td>group</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>description</td>
</tr>
<tr>
<td></td>
<td>Member</td>
<td>member</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>cn</td>
</tr>
<tr>
<td>Account</td>
<td>Object class</td>
<td>user</td>
</tr>
<tr>
<td></td>
<td>Business phone</td>
<td>telephonenumber</td>
</tr>
<tr>
<td></td>
<td>Content locale</td>
<td>(leave blank)</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>description</td>
</tr>
<tr>
<td></td>
<td>Email</td>
<td>mail</td>
</tr>
<tr>
<td></td>
<td>Fax/Phone</td>
<td>facsimiletelephonenumber</td>
</tr>
<tr>
<td></td>
<td>Given name</td>
<td>givenname</td>
</tr>
<tr>
<td></td>
<td>Home phone</td>
<td>homephone</td>
</tr>
<tr>
<td></td>
<td>Mobile phone</td>
<td>mobile</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>displayName</td>
</tr>
<tr>
<td></td>
<td>Pager phone</td>
<td>pager</td>
</tr>
<tr>
<td></td>
<td>Password</td>
<td>unicodePwd</td>
</tr>
<tr>
<td></td>
<td>Postal address</td>
<td>postaladdress</td>
</tr>
<tr>
<td></td>
<td>Product locale</td>
<td>(leave blank)</td>
</tr>
<tr>
<td></td>
<td>Surname</td>
<td>sn</td>
</tr>
<tr>
<td></td>
<td>Username</td>
<td>sAMAccountName</td>
</tr>
</tbody>
</table>
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.

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. 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 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 Cognos 8 can locate and use your existing authentication namespace.
   
   - For **User lookup**, specify \(\text{cn}=${\text{userID}}\)
   - For **Bind user DN and password**, specify \(\text{cn}=\text{root}\)
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. 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.

<table>
<thead>
<tr>
<th>Mappings</th>
<th>LDAP property</th>
<th>LDAP value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder</td>
<td>Object class</td>
<td>organizationalunit,organization,container</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>description</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>ou,o,cn</td>
</tr>
<tr>
<td>Group</td>
<td>Object class</td>
<td>groupofnames</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>description</td>
</tr>
<tr>
<td></td>
<td>Member</td>
<td>member</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>cn</td>
</tr>
<tr>
<td>Account</td>
<td>Object class</td>
<td>inetorgperson</td>
</tr>
<tr>
<td></td>
<td>Business phone</td>
<td>telephonenumber</td>
</tr>
</tbody>
</table>
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.

9. 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 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 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.

<table>
<thead>
<tr>
<th>Mappings</th>
<th>LDAP property</th>
<th>LDAP value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content locale</td>
<td>(leave blank)</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td>description</td>
<td></td>
</tr>
<tr>
<td>Email</td>
<td>mail</td>
<td></td>
</tr>
<tr>
<td>Fax/Phone</td>
<td>facsimileteleponenumber</td>
<td></td>
</tr>
<tr>
<td>Given name</td>
<td>givenname</td>
<td></td>
</tr>
<tr>
<td>Home phone</td>
<td>homephone</td>
<td></td>
</tr>
<tr>
<td>Mobile phone</td>
<td>mobile</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>cn</td>
<td></td>
</tr>
<tr>
<td>Pager phone</td>
<td>pager</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>userPassword</td>
<td></td>
</tr>
<tr>
<td>Postal address</td>
<td>postaladdress</td>
<td></td>
</tr>
<tr>
<td>Product locale</td>
<td>(leave blank)</td>
<td></td>
</tr>
<tr>
<td>Surname</td>
<td>sn</td>
<td></td>
</tr>
<tr>
<td>Username</td>
<td>uid</td>
<td></td>
</tr>
</tbody>
</table>
8. 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 Cognos Connection, they must have permission to read the ou and o attributes.

<table>
<thead>
<tr>
<th>Mappings</th>
<th>LDAP property</th>
<th>LDAP value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder</td>
<td>Object class</td>
<td>organizationalUnit, organization, container</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>description</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>ou,o,cn</td>
</tr>
<tr>
<td>Group</td>
<td>Object class</td>
<td>groupOfNames</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>description</td>
</tr>
<tr>
<td></td>
<td>Member</td>
<td>member</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>cn</td>
</tr>
<tr>
<td>Account</td>
<td>Object class</td>
<td>inetOrgPerson</td>
</tr>
<tr>
<td></td>
<td>Business phone</td>
<td>telephonenumber</td>
</tr>
<tr>
<td></td>
<td>Content locale</td>
<td>Language</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>description</td>
</tr>
<tr>
<td></td>
<td>Email</td>
<td>mail</td>
</tr>
<tr>
<td></td>
<td>Fax/Phone</td>
<td>facsimileTelephonenumber</td>
</tr>
<tr>
<td></td>
<td>Given name</td>
<td>givenname</td>
</tr>
<tr>
<td></td>
<td>Home phone</td>
<td>homephone</td>
</tr>
<tr>
<td></td>
<td>Mobile phone</td>
<td>mobile</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>cn</td>
</tr>
<tr>
<td></td>
<td>Pager phone</td>
<td>pager</td>
</tr>
<tr>
<td></td>
<td>Password</td>
<td>(leave blank)</td>
</tr>
<tr>
<td></td>
<td>Postal address</td>
<td>postaladdress</td>
</tr>
<tr>
<td></td>
<td>Product locale</td>
<td>Language</td>
</tr>
<tr>
<td></td>
<td>Surname</td>
<td>sn</td>
</tr>
<tr>
<td></td>
<td>Username</td>
<td>uid</td>
</tr>
</tbody>
</table>

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.

9. From the File menu, click Save.
Configure an LDAP Namespace for Sun ONE Directory Server

If you configure a new LDAP namespace for use with Sun ONE Directory Server, you must modify the necessary settings and change the values for all properties of the Sun ONE Directory objects.

**Steps**

1. On every computer where you installed Content Manager, open 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 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. To configure the LDAP advanced mapping properties for use with Sun ONE 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.

<table>
<thead>
<tr>
<th>Mappings</th>
<th>LDAP property</th>
<th>LDAP value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Folder</td>
<td>Object class</td>
<td>organizationalUnit,organization</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>description</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>ou,o</td>
</tr>
<tr>
<td>Group</td>
<td>Object class</td>
<td>groupofuniquenames</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>description</td>
</tr>
<tr>
<td></td>
<td>Member</td>
<td>uniquemember</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>cn</td>
</tr>
<tr>
<td>Account</td>
<td>Object class</td>
<td>inetorgperson</td>
</tr>
<tr>
<td></td>
<td>Business phone</td>
<td>telephonenumber</td>
</tr>
<tr>
<td></td>
<td>Content locale</td>
<td>preferredlanguage</td>
</tr>
</tbody>
</table>
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.

9. From the File menu, click Save.

### Make Custom User Properties for LDAP Available to Cognos 8 Components

You can use arbitrary user attributes from your LDAP authentication provider in 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 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 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.
Chapter 8: Configuring Authenticated Access

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 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. 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 the Cognos Series 7 Supplementary Software CD or from ftp://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.

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 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 Cognos 8 Components

You achieve single signon to 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 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 Cognos 8 using external identity mapping see the same users, groups, and folders as the Bind user.

If you want 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 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)}

Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>str</td>
<td>The string to search.</td>
</tr>
<tr>
<td>old</td>
<td>The substring to be replaced by the new substring.</td>
</tr>
<tr>
<td>new</td>
<td>The substring that replaces the old substring.</td>
</tr>
</tbody>
</table>

Examples

${replace(${environment("REMOTE_USER")},"NAMERICA\",""}  
${replace(${environment("REMOTE_USER")},"NAMERICA\",""})

Configuring Cognos 8 Components to Use eTrust SiteMinder

You can configure Cognos 8 components to use a Netegrity SiteMinder namespace as the authentication source, provided that you installed Content Manager on a non-Linux computer.

To configure an authentication provider in an eTrust SiteMinder environment, you configure an LDAP, NTLM, or Netegrity SiteMinder namespace depending on your eTrust SiteMinder configuration. 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 Cognos 8, you must also add a corresponding LDAP, Active Directory Server, or NTLM namespace to the 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 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 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 Cognos 8 Controller Components" (p. 109).

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 Cognos 8 components with an NTLM namespace or configure 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. 114), Active Directory (p. 115), or NTLM (p. 126) 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 Cognos 8 Controller Components" (p. 109).

To use an eTrust SiteMinder namespace and to set up single signon, do the following:

- Configure 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 Cognos 8
- Protect the Cognos Web alias.

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 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 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 Cognos namespace for the user directory.

For more information, see "Configure an LDAP Namespace" (p. 114).

Enable Single Signon Between eTrust SiteMinder and Cognos 8

By configuring single signon, you are not prompted to reenter authentication information.
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 Cognos Web Alias

eTrust SiteMinder must be configured correctly to protect the 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.
Configuring Cognos 8 Components to Use an NTLM Namespace

You can configure 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 Cognos 8 components

Configure an NTLM Namespace

You can configure 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 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 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.
   Cognos 8 loads, initializes, and configures the provider libraries for the namespace.

Enable Single Signon Between NTLM and Cognos 8 Components

By default, the 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 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.
   Cognos 8 loads, initializes, and configures the provider libraries for the namespace.
Test the Namespaces

After you configure one or more new namespaces for Cognos 8 components, you can test the namespaces. The test can occur before or after you start the Cognos 8 service. You can test all namespaces at the same time or test them individually.

Steps to Test All Namespaces

- In the Explorer window, right-click Authentication and click Test.

  Cognos 8 Controller 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.

Steps for a Single Namespace

- In the Explorer window, under Authentication, right-click the new authentication resource and click Test.

  Cognos 8 Controller 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 Cognos 8 Controller components detected after an upgrade.

Important: You must not delete the 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 the computer where you installed Content Manager, start 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.

You must now log on to the portal and permanently delete the data for the namespace. For more information, see the Cognos 8 Administration and Security Guide.
Chapter 9: Setting Up an Unattended Installation and Configuration

Set up an unattended installation and configuration to
- install an identical configuration on several computers on your network
- automate the installation and configuration process by specifying options and settings for users

Unattended installations for Cognos 8 Controller can only be set up for single-computer installations.

Important: All configuration tasks using Cognos Controller Configuration must be completed manually.

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, you must complete these tasks:
- Configure a transfer specification file (.ats) to specify installation options.
- Run the installation tool in silent mode.
- Use a preconfigured Cognos 8 Controller configuration file from another computer.
- Run Cognos Configuration in silent mode.

After you complete these tasks, you must also do the following:
- Ensure that the Cognos 8 Controller installation directory on all computers is protected from unauthorized or inappropriate access.
- Import the Cognos Controller Framework Manager package.
- Configure the Cognos Controller Configuration settings manually.

You are now ready to use Cognos 8 Controller.

Set Up an Unattended Installation

Use a transfer specification file (.ats) to copy Cognos 8 Controller components to your computer without being prompted for information.

By default, each time you install Cognos 8 Controller components using the installation wizard, the options you select are recorded in a transfer specification file. Therefore, if you already installed Cognos 8 Controller 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 Cognos 8 Controller components on your computer.
2. Go to c8_location\instlog.
3. Locate the transfer specification file (.ats) that was generated.
   The file name is ts-CONTRL-version-yyyyymmdd_hmmm.ats.
4. Copy the transfer specification file to the computer where you plan to install Cognos 8 Controller.

5. On the computer where you plan to install the software, insert the installation CD and copy the contents of the Cognos directory to your computer.

6. Install Cognos 8. From the Start menu, click Programs, Command Prompt to open a Command Prompt window, 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 a return status other than zero (0) is returned, check the log files for error messages. Errors are recorded in the installation directory in the following log file:

   `tl-CONTRL-version-yyyyymmdd-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:

   `tl-CONTRL-version-yyyyymmdd-hhmm.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 Cognos 8 Controller 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 Cognos 8 Controller:

   `appPath=location`

   **Tip:** There should be no space on either side of the equal (=).

4. For the server components of Cognos 8 Controller, in the section named [Component List], next to each component do one of the following:

   - To install the component, type 1.
   - To not install the component, type 0.

5. 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 VISIBLETOALL=property.

6. For the install information in the [Install Conditions] section:

   - To specify the condition is true, type 1
   - To specify 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:

   `issetup -s location/response.ats`

   If a return status other than zero (0) is returned, check the log files for error messages. Errors are recorded in the installation directory in the following log file:

   `tl-CONTRL-version-yyyyymmdd-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:

   `tl-CONTRL-version-yyyyymmdd-hhmm.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 Cognos 8 Controller configuration.
Chapter 9: Setting Up an Unattended Installation and Configuration

Set Up an Unattended Configuration

Before you set up an unattended Cognos 8 Controller configuration, you must export a configuration from another computer that has Cognos 8 Controller installed. You can then run Cognos Configuration in silent mode.

The exported configuration contains the properties of the Cognos 8 Controller 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. Global configuration includes such settings as content locale, product locale, and cookie settings. For more information, see "Global Settings" (p. 90).

Ensure that the configuration settings on the local computer are appropriate to use to configure another Cognos 8 Controller 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 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 c8_location/configuration directory on the computer where you plan to do an unattended configuration.
8. Go to c8_location/bin.
9. Type the configuration command:
   cogconfig.bat -s
   Tip: To view log messages that were generated during an unattended configuration, see the cogconfig_response.csv file in the c8_location/logs directory.

Cognos Configuration applies the configuration settings specified in the local copy of cogstartup.xml, encrypts credentials, generates digital certificates, and if applicable, starts Cognos 8 Controller services or processes.

Import the Cognos 8 Controller Standard Reports Package

Before you can run Cognos 8 Controller and view reports in Cognos Viewer, you must import the Cognos 8 Controller standard reports package into Content Manager.

Steps
1. Start Cognos Connection.
2. On the portal toolbar, click Tools, and then click Content Administration.
3. On the toolbar, click the New Import button. The New Import wizard appears.
4. In the Deployment archive box, click the Controller package, and then click Next.
5. Type an optional description and screen tip for the deployment specification, select the folder where you want to save it, and then click Next.
6. Select the content that you want to include in the import.
7. Select the options you want, along with your conflict resolution choice for options that you select.
8. In the Specify the general options page, select whether to include access permissions and references to external namespaces, and who should own the entries after they are imported in the target environment.
9. Click Next.
   The summary information appears.
10. Review the summary information and click Next.
11. In the Select an action page, select Save and run once, and then click Finish.
After you run the import, the Cognos 8 Controller reports package appears in your Cognos Connection content.

## Configure Start Configuration Settings Manually

After you run an unattended installation and configuration, you must configure the Cognos Controller Configuration settings manually.

Configure the Cognos 8 Controller Configuration settings manually by doing the following:
- Configure the Cognos Controller database connection.
- Configure the COM+ Server.

## Set Database Connection Properties for the Controller Data Source

Before you can run Cognos 8 Controller, you must configure a Controller database connection. Cognos Controller databases must be created using either Oracle or Microsoft SQL Server.

To run reports against Cognos Controller data sources, the data sources must be configured for Report Server and appear in Cognos Connection.

If you are installing Cognos 8 Controller for the first time, or if you do not want to connect to an existing Controller database, you can create a database connection to an empty Controller database.

If you want to create a connection to an existing Controller database, we recommend that you create a backup of your database before you create the Controller data source connection. This is because the Controller Database Conversion Utility, which runs against the database during the data source connection process, updates the database tables for use with Cognos 8 Controller.

### Steps
1. From the Start menu, start Cognos Controller Configuration.
2. In the Explorer window, click Database Connections, and then from the File menu, click New.
3. In the Properties window, click the Database type box, and then use the drop-down arrow to select the database type.
   You can choose Oracle or SQL Server.
4. In the Name box, type a name for the database connection.
5. In the Provider box, type the name of the database provider.
   To obtain the database provider information, see the Oracle or SQL Server documentation.
6. In the User ID and Password boxes, type the user name and password for the Controller database.
7. In the Initial catalog box, type the Controller database name.
8. In the Data source box, type the database server computer name.
   Do not use localhost.
9. From the File menu, click Save.
10. In the Explorer window, under Database Connections, click the database.
11. From the Actions menu, click Run.
   The Database Conversion Utility opens.
12. If this is an empty Controller database, in the Database Conversion Utility dialog box, click Create Db.
   The Database Conversion Utility initializes the database.
13. In the Database Conversion Utility dialog box, click Run Steps.
   The Database Conversion Utility updates the database for use with Cognos 8 Controller.
14. Click Close.
15. From the Actions menu, click Check.
   If the database connection validation fails, review the database connection properties and fix any errors.
16. From the File menu, click Save.
17. In the Explorer window, under Web Services Server, click Report Server.
   The new database is now configured as a data source for Report Server, and is listed as a data source in Cognos Connection.

**Configure the COM+ Server**

After you configure network access to the COM+ Server, you must configure the Controller COM+ Server to run under a dedicated user.

**Steps**
1. From the Start menu, start Cognos Controller Configuration.
2. In the Explorer window, click COM+ Server.
3. In the COM+ Server window, click Specify Account to configure the COM+ Server with a user account that has administrator privileges on the computer.
4. In the User box, type the user name for the account.
5. In the Password box, type the password for the account.
6. In the Confirm Password box, retype the password for the account.
7. Click in the space under COM+ Role, and then from the File menu, click New.
8. Under COM+ Role, type ControllerUsers.
9. Under COM+ User, type IUSR_XXX, where XXX is the ID configured in IIS for anonymous access.
   This ID must be the same ID under which you configured the Web aliases.
   To locate the IIS anonymous access ID, in IIS, right-click the cognos8 Web alias, and then click Properties. On the Directory Security tab, click the Edit button. Copy the Anonymous AccessID in the User name box.
10. From the File menu, click New.
11. Under COM+ Role, type ControllerUsers.
12. Under COM+ User, type IWAM_XXX, where XXX is the ID configured in IIS for anonymous access.
13. From the Actions menu, click Check to validate each user.
14. From the File menu, click Save.
Appendix A: Troubleshooting

Use this troubleshooting reference information as a resource to help you solve specific problems you may encounter during or after the installation of Cognos 8 Controller components.

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 Global Customer Services Web site (http://support.cognos.com). The Knowledge Base is a database of problems and solutions for all Cognos products.

When you cannot resolve a problem, the final resource is your Cognos 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

When you are troubleshooting, several files can help 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-C8BISRV-8.1-0.0-20050901_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-C8BISRV-8.1-0.0-20050901_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_200211231540.xml
```
Appendix A: Troubleshooting

**The Startup Configuration Lock File**
This file is created each time you open Cognos Configuration. It prevents you from opening more than one Cognos Configuration window. If you experience problems opening Cognos Configuration, you can check the `c8_location/configuration` directory for the cogstartup.lock file. If the file exists and Cognos Configuration is not open, it means that Cognos Configuration did not shut down properly the last time you used it. You can delete the lock file and then open Cognos Configuration.

**The Locale Configuration File**
This file records the configuration choices you make in 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_200211231540.xml`

**The Run-Time Log File**
The default 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 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 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.
`gwgateway_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_uninstall_log.htm and is located in the Temp directory. You can use the log file to troubleshoot problems related to uninstalling Cognos 8 components.

**The Silent Mode Log File**
This file records the activities that 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.

**Windows Event Viewer**
Windows Event Viewer provides information about program, security, and system events. For example, if the Cognos 8 service fails to start, this fact is recorded in the event log.
For information about how to use Windows Event Viewer, see the Windows help.

**Microsoft Internet Information Services (IIS) Log File**
This file records Microsoft Internet Information Services (IIS) activities. The log file is found in the `installation_location/windows/system32/logFiles/W3SVC1` directory. You can use this log file to troubleshoot problems related to your IIS Web server. For example:
- Code 404 is a page not found error.
  Your virtual directory may not be configured correctly.
- Code 304 is a security credential error.
Your directory security may not be configured correctly.
- Code 200 indicates that IIS is working correctly.
  The problem you are encountering is not related to your IIS Web server.
For more information, see the Microsoft Internet Information Services help.

**Problems Starting Cognos 8 Controller**

You may encounter problems when you try to start Cognos 8 Controller or log on to Cognos 8 Controller. Solutions are provided for specific problems.

**The Controller Link Is Missing in Cognos Connection**

You completed a distributed installation integrating Cognos 8 Controller with Cognos 8 Business Intelligence. When you access Cognos Connection to start Cognos 8 Controller, the Controller link does not appear on the Cognos Connection start page or on the studio bar.

Ensure that you installed the Gateway Integration Enabler on the Cognos 8 Gateway computer, and the Cognos Connection Integration Enabler on the Cognos 8 application servers.

If you started the Cognos 8 service before the Cognos Connection Integration Enabler was installed, you must restart the Cognos 8 service.

You may also need to verify that the URI for Cognos Connection is correct. The URL parameter in the ControllerLaunch.xml file sets the link associated with Controller in Cognos Connection. For a distributed installation, this must be the full URL for the Controller Client Distribution Server.

**Steps to Restart the Cognos 8 Service**

1. Start Cognos Configuration.
2. From the **Actions** menu, if the service is currently running, click **Restart**, or if the service is stopped, click **Start**.

**Step to Verify That the Cognos Connection Integration Enabler Is Installed**

1. In the `c8_location/webapps/p2pd/WEB-INF/service` directory, verify that the `ControllerStudio.xml` file exists.

**Step to Verify the URI for Cognos Connection**

1. If the Report Server and Controller Client Distribution Server are on different computers, set the URL to point to Controller Client Distribution Server:
   - In the `c8_location/templates\ps\portal\launch` directory, open the `ControllerLaunch.xml` file in a text editor.
   - Change the value of the URL parameter from `../controller` to the fully-qualified URI of the computer where Controller Client Distribution Server is installed, such as `http://servername/cognos/controller`.
   - Save and close the file.

**Warning! You Are About to Navigate Away from This Page**

When you try to start Cognos 8 Controller, an error message may state that you are about to leave this page. There may be an error in the Code Group settings of the Microsoft .NET Framework runtime security policy that you configured.

Verify that you have installed the supported version of Microsoft .NET Framework as listed on the Cognos Global Customer Services Web site ([http://support.cognos.com](http://support.cognos.com)). Review the steps for configuring Microsoft .NET Framework (p. 48) and ensure that the URL to the Controller Client Distribution Server is correct.
Appendix A: Troubleshooting

You Receive No Response When Starting Cognos 8 Controller

When you try to start Cognos 8 Controller, you receive no response. There may be an error in the configuration of the Microsoft .NET Framework runtime security policy that you configured.

Verify that you have installed the supported version of Microsoft .NET Framework as listed on the Cognos Global Customer Services Web site (http://support.cognos.com). Review the steps for configuring Microsoft .NET Framework (p. 48) and ensure that the settings are correct. You can also delete the security policy on the client computer, reconfigure the security policy, and then deploy a new package (p. 50) to the client computer.

Error - Page Cannot Be Found When Starting Cognos 8 Controller

When you try to start Cognos 8 Controller, an error message may state that the page cannot be found.

Ensure that the ControllerServer virtual directory is defined on the Controller Web Services Server, that it points to the c8_location/ControllerProxyServer folder, and that you have access privileges for that folder.

You may also want to verify that you installed the supported versions of Microsoft .NET Framework as listed on the Cognos Global Customer Services Web site (http://support.cognos.com) and that ASP.NET is installed and configured.

Steps to Verify That ASP.NET Is Installed and Configured
1. In Administrative Tools, start Internet Information Services (IIS) Manager.
2. In the left pane, expand Internet Information Services (local computer), Web Sites, Default Web Site and verify that the aspnet_client folder exists.
3. If this folder is missing, complete the steps (p. 35) to install and configure ASP.NET.
4. In the left pane, expand Internet Information Services (local computer), and then click Web Services Extensions, and verify that ASP.NET V2.0.50727 is set to Allowed.

After Upgrading, You Cannot Start Cognos 8 Controller

After upgrading your version of Cognos 8 Controller, you experience problems with starting Controller that are not documented elsewhere.

You may need to delete some leftover files from the Microsoft .NET Framework cache on the Controller client computer.

Steps to Delete Files from the Microsoft .NET Framework Cache
1. Close all instances of Internet Explorer.
2. Run Windows Task Manager and stop any iexplore.exe process that is running.
3. In the C:\documents and settings\username\application data\Cognos directory, delete the ccr folder.
4. In Internet Explorer, return to Cognos Connection, and then restart Cognos 8 Controller.
5. In Internet Explorer, from the Tools menu, click Internet Options.
6. On the General tab, under Temporary Internet files, click Delete Files, select the Delete all offline content check box, and then click OK.

Error - VMWare Can’t Run the ccr.exe File

You are trying to start Cognos 8 Controller in a VMWare environment and a message prompts you to confirm that you want to run the ccr.exe file. When you click Run, an error occurs.

Because VMWare cannot resolve the host name of an IP address, you must add it to the hosts file.

Steps to Add IP Addresses of Server Computers to the Hosts File
1. On the VMWare virtual computer, in a text editor, open the C:\windows\system32\drivers\etc\hosts file.
2. Add the IP address and the name of each server computer that you are using in your distributed installation to the hosts file.

   Tip: Use the other entries in the hosts file as an example of correct syntax.

An Error Occurred While Trying to Access the Server

While trying to start or log on to Cognos 8 Controller, a message states that an error occurred while trying to access the server.

This error can occur for several reasons:
- The Controller Web Services Server may not be running.
- The COM+ Server may not be running.
- The Controller database connection logon credentials may need to be reset.
- There may be errors with the configuration of authenticated access.

   Tip: If the error occurs after you start Cognos 8 Controller, then in Administrative Tools use the Event Viewer on both the Cognos 8 Controller client computer and the Controller Web Services Server computer for internal errors.

Steps to Verify That the Controller Web Services Server Is Running

1. On the Controller Web Services Server computer, start Internet Explorer and go to http://computername/cognos8/controllervserver/ccrws.asmx

2. If the CCRWS operations page does not appear, verify that ASP.NET is installed and configured (p. 138). If it is not, install and configure ASP.NET (p. 35) and then repeat steps 1 and 2.

3. On the CCRWS operations page, click the ConnectionBusiness SelectDB method link.

4. Click Invoke.

5. If a Web page containing XML data with the list of databases does not appear, ensure that the directory security settings in Microsoft Internet Information Services (IIS) are configured correctly so that remote users can connect and verify that the COM+ Server is running. Then repeat steps 1 to 3 on a client computer.

   If this still fails, it may be a network connection problem.

Steps to Verify That the COM+ Server Is Running


2. In the left pane, under Console Root, expand Component Services, Computers, My Computer, Running Processes.

3. If the COGNOSCONTROLLER process is not listed under Running Processes, the credentials are probably incorrect, and you must redo the configuration of the COM+ Server (p. 60) and then repeat steps 1 and 2.

4. In the left pane, expand COGNOSCONTROLLER, and also expand the next level of COGNOSCONTROLLER.

   If components are listed under this level, the COM+ Server is running.

   If you still have a problem after verifying that the COM+ Server is running, the problem may be related to the configuration of the database connection files (UDL) or logon problems. You can troubleshoot further by redoing the configuration of the Controller database connection (p. 56) and the configuration of the Controller Client Distribution Server (p. 72).

Step to Reset the Microsoft SQL Server Logon Credentials

1. In SQL*Plus, type the following command to run a stored procedure that resets the database user name and password:

   `sp_change_users_login 'Update_one', 'username', 'password'

Steps to Test the Database Connection

1. From the Start menu, start Cognos Controller Configuration.
2. In the **Explorer** window, under **Web Services Server**, click **Database Connections** and select the problem connection for the Controller database.
3. From the **Actions** menu, click **Run**.
   The Database Conversion Utility opens.
4. Under **Db Version**, verify that the **DBConv** version is the same as the **Actual** version of the database.

**Steps to Map a Cognos Controller User to a Cognos 8 User**
1. Start Cognos Controller.
   You must be a member of the Controller Administrators role in Cognos Connection.
2. From the **Maintain** menu, click **Rights, Users**.
3. Select the user you defined for the Cognos Controller database.
4. Next to **CAM User** box, click **Show Valid Choices** and then select the user you mapped to the Cognos 8 namespace roles.
5. Click **Save**.

**Error - No Database Configured**
While trying to log on to Cognos 8 Controller, a message states that no database is configured. This is the result when the Controller Web Services Server cannot find any UDL files. Verify that you created a database connection for the Controller database. For more information, see "Set Database Connection Properties for the Controller Data Source" (p. 56).

**Error - The File Is Not a Valid Compound File**
While trying to log on to Cognos 8 Controller, a message states that the file is not a valid compound file. This can occur when the UDL file for the Controller database is corrupted. You can try to repair the database connection, or delete it and create a new one. For information about creating a database connection for the Controller database, see "Set Database Connection Properties for the Controller Data Source" (p. 56).

**Steps to Repair the Database Connection**
1. From the **Start** menu, start Cognos Controller Configuration.
2. In the **Explorer** window, under **Web Services Server**, click **Database Connections** and select the problem connection for the Controller database.
3. From the **Actions** menu, click **Check**.
4. If the database connection validation fails, review the database connection properties and fix any errors.
5. From the **File** menu, click **Save**.
6. In the **Explorer** window, under **Web Services Server**, click **Report Server**.

**Problems Starting the Cognos 8 Controller Add-in for Excel**
You may encounter problems during your testing of the Cognos 8 Controller Add-in for Excel. Solutions are provided for specific problems.
If the specific problems identified do not include your issue, you can use the **Control Panel, Add or Remove Programs** window to uninstall the Cognos 8 Controller Link Add-In, and then restart the Controller client computer.
Appendix A: Troubleshooting

**Request Failed Error When Starting Microsoft Excel**

You accessed Cognos 8 Controller at least once from the same client computer, and are now trying to start Microsoft Excel. A request failed error appears followed by a long error message related to security. A possible cause may be that the client computer has two versions of Microsoft .NET Framework installed and Microsoft Excel is configured to access a version not supported by Cognos 8 Controller.

You must verify that Microsoft Excel is configured to use Microsoft .NET Framework v2.0.50727.

**Steps to Configure Microsoft Excel to Use the Current Version of Microsoft .NET Framework**

1. On the client computer, go to the Microsoft Office installation directory, such as C:\program files\Microsoft Office\Office11 and look for the Excel.exe.config file.
2. If the Excel.exe.config file exists, open the file in a text editor and verify that the version statement is exactly as follows:
   
   
   ```
   supportedRuntime version="v2.0.50727"
   ```
   
   If the file does not exist, use a text editor to create a new file named Excel.exe.config and copy and paste the following lines into the file:
   
   ```
   <configuration>
   <startup>
   <supportedRuntime version="v2.0.50727"/>
   </startup>
   </configuration>
   ```

**After Upgrading, ControllerXLPusher Error Occurs When Starting Microsoft Excel**

You accessed Cognos 8 Controller at least once from the same client computer, and are now trying to start Microsoft Excel. An error message states that the ControllerXLPusher.dll file or one of its dependencies was not found. The registry may have more than one version listed for the ControllerXLPusher.dll file.

You must verify that the version used by the registry key is the current version of the ControllerXLPusher.dll file.

**Steps to Identify the Current Version of the ControllerXLPusher.dll File**

1. On the client computer, in the c8_location\webcontent\ccr directory, right-click the ControllerXLPusher.dll file, and then click Properties.
2. Click the Version tab and record the File version number for comparing against the registry key.

**Steps to Verify the Version Used by the Registry Key**

1. Open the Registry Editor and search for ControllerXLPusher using the registry Find feature. The key HKEY_CLASSES_ROOT\CLSID\id_number should be found.
2. Click the InprocServer32 key and check whether only the version number that matches the current version of the ControllerXLPusher.dll file exists.
3. If more than one version exists, delete all entries except the current version, which you recorded earlier.

**Problems Starting Cognos 8**

You may encounter problems when you try

- to start the Cognos 8 service
Appendix A: Troubleshooting

- to open the Welcome page for Cognos Connection for the first time

<table>
<thead>
<tr>
<th>Symptoms</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>You do not see the splash screen for Cognos Connection when you start Cognos 8.</td>
<td>Check your Web server configuration.</td>
</tr>
<tr>
<td>The service starts but no tables are created in the content store database.</td>
<td>Check your content store configuration.</td>
</tr>
<tr>
<td>The service does not start.</td>
<td>Ensure that you wait a few moments before submitting a request.</td>
</tr>
</tbody>
</table>

Ensure that you use third-party software that is supported by 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 Global Customer Services Web site (http://support.cognos.com).

**CFG-ERR-0106 Error When Starting the Cognos 8 Service in Cognos Configuration**

When you start the 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.`

By default, Cognos Configuration checks the progress of the start request every half second for three minutes. If 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 Cognos Configuration waits to receive a response from the 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 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 Cognos Configuration checks the progress of the start request. By default, its value is 360.

**Steps to Configure the ServiceWaitInterval and ServiceMaxTries Properties**

1. Using Cognos Configuration, stop the Cognos 8 service.
2. Open the `c8_location/configuration/cogconfig.prefs` file in an editor. This file is created automatically the first time you start 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 Cognos Configuration, start the Cognos 8 service.

**Cognos 8 Server Not Available When Starting Cognos Connection**

After you configure Cognos components and start the Cognos 8 services, when you open 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 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 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.

<table>
<thead>
<tr>
<th>Database</th>
<th>Character encoding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle 9i</td>
<td>AL32UTF8</td>
</tr>
<tr>
<td></td>
<td>AL32UTF16</td>
</tr>
<tr>
<td>DB2 UDB</td>
<td>Codeset UTF-8</td>
</tr>
<tr>
<td>Sybase ASE</td>
<td>UTF-8</td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>UTF8</td>
</tr>
<tr>
<td></td>
<td>UTF16</td>
</tr>
</tbody>
</table>

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 vendor 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:
Appendix A: Troubleshooting

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 vendor documentation.

Invalid Configuration Settings

If the following or similar messages appear in the log file, you did not configure the content store correctly in 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:JSQLConnect://localhost:1433/cm".
  Failed Logon:com.microsoft.jdbc.sqlserver.jdbc.JsSQLServerException: Cannot open database requested in login '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 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 Cognos 8 service is started.

Steps

1. On the computer where you installed Content Manager, start 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:JSQLConnect://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.

Cognos 8 Services Fail to Restart After a Network Outage

The Cognos Bootstrap Service restarts 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 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 Cognos Configuration to use localhost or the network host name.

DPR-ERR-2058 Error Appears in Web Browser When Starting Cognos 8

After you start the services in 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.
Appendix A: Troubleshooting

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.

**Cognos Services are Not Done Initializing**
After you start the services in 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 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 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 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 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.companyname:1534 to match the name in the tnsnames.ora file.

**DPR-ERR-2022 Error Appears in Web Browser When Starting Cognos Connection**
After you start the services in 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 Cognos services are initialized.
To avoid this problem, after you start the services in 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 Cognos application if Cognos 8 Controller 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 naming convention.

**Problems Configuring Cognos 8**

After you install Cognos 8 Controller components, you may encounter problems when you save changes in Cognos Configuration.

Ensure that you

- configure and start the services on the computer where Content Manager is located before you configure other components
- restart the Cognos 8 service after you make any configuration changes

**Run Database Cleanup Scripts**

In some troubleshooting situations, you may be advised to start with new configuration data. You can run an SQL script to delete all the tables in any of the following databases that Cognos 8 Controller components use:

- **content store** for data that Cognos 8 Controller needs to operate
- **log database** for log messages

When you delete a table, its structural definition and data are deleted permanently from the database.

When you restart the Cognos 8 service, a new set of required database tables is created automatically in the location specified by your configuration settings.

**Steps to Run Database Cleanup Scripts**

1. On the computer where Content Manager is located, stop the Cognos 8 service.
2. Go to the appropriate directory:
   - To delete tables from the log database, go to `c8_location\configuration\schemas\logging`.
   - To delete tables from the content store, go to `c8_location\configuration\schemas\content`.
3. Go to the appropriate database directory.
4. Depending on the database and database type, run one of the following scripts in the appropriate database tool to delete the tables.

<table>
<thead>
<tr>
<th>Database</th>
<th>Database Type</th>
<th>Script Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content store</td>
<td>DB2</td>
<td>dbClean_db2.sql</td>
</tr>
<tr>
<td></td>
<td>Microsoft SQL Server</td>
<td>dbClean_mssqlserver.sql</td>
</tr>
</tbody>
</table>
Start the Cognos 8 service.

Error Trying to Encrypt Information When Saving Your Configuration

When you save your configuration using the configuration tool, you may see an error message that the cryptographic information cannot be encrypted. An error occurred when requesting a certificate from the Certificate Authority.

The cryptographic information cannot be encrypted. Do you want to save the configuration in plain text?

Before you can encrypt your configuration settings, the computer where Content Manager is installed must be configured and running. In addition, ensure that your Java environment is configured correctly and the URIs are correct.

Also, an error message similar to the following may appear:


The cryptographic error usually means the Java environment is not configured correctly. Ensure that the JAVA_HOME environment variable is set correctly and the appropriate security providers are installed, such as JSSE for JRE 1.31.

Steps to Check the Configuration
1. On the Content Manager computer, start Cognos Configuration.
2. In the Explorer window, click Environment.
3. In the Properties window, verify these properties:
   - Under Gateway Settings, Gateway URI
   - Under Dispatcher Settings, External dispatcher URI and Internal dispatcher URI
   - Under Other URI Settings, Dispatcher URI for external applications and Content Manager URIs
4. Save the configuration and restart the Cognos 8 service.

Unable to Save Your Configuration

You may be unable to save your configuration because you are missing a resource. For example, you delete a resource such as the Cognos namespace, a cryptographic provider, or the content store. You can replace the default database type for the content store with Oracle, DB2, or Sybase. You cannot replace the Cognos namespace. You can recreate it, but you must then recreate your Cognos groups and roles.

For more information about creating groups and roles in Cognos Connection, see the Administration and Security Guide.

Steps to Recreate the Cognos Namespace
1. Start Cognos Configuration.
2. In the Explorer window, under Security, right-click Authentication and then click New resource, Namespace.

<table>
<thead>
<tr>
<th>Database</th>
<th>Database Type</th>
<th>Script Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle</td>
<td></td>
<td>dbClean_oracle.sql</td>
</tr>
<tr>
<td>Sybase</td>
<td></td>
<td>dbClean_sybase.sql</td>
</tr>
<tr>
<td>Log</td>
<td>DB2</td>
<td>LS_dbClean_db2.sql</td>
</tr>
<tr>
<td></td>
<td>Microsoft SQL Server</td>
<td>LS_dbClean_mssql.sql</td>
</tr>
<tr>
<td></td>
<td>Oracle</td>
<td>LS_dbClean_oracle.sql</td>
</tr>
<tr>
<td></td>
<td>Sybase</td>
<td>LS_dbClean_sybase.sql</td>
</tr>
</tbody>
</table>
3. In the Name box, type a name for the resource.
4. In the Type box, click Cognos, and then click OK.
   The Cognos namespace appears in the Explorer window.
5. From the File menu, click Save.

Java Error When Starting Cognos Configuration

When you start Cognos Configuration, you may receive an error message that the Java Runtime Environment (JRE) has changed and that the current cryptographic information is not compatible with the new JRE. You may then be prompted to regenerate the cryptographic information for the new JRE or exit to switch back to the previous JRE.

This error may occur for one of these reasons:

- Your configuration data was encrypted using a different JRE than the one Cognos 8 Controller components are currently using.
- The cryptographic information may have been corrupted.

If you click Regenerate in the error dialog, the Cognos 8 service is stopped and the cryptographic information is regenerated.

If you click Exit in the error dialog, you must set the JAVA_HOME environment variable to point to the JRE that you used to save your configuration.

In Windows, if you want Cognos 8 Controller components to use the JRE that is installed by default, unset JAVA_HOME or set JAVA_HOME to c8_location/bin/jre.

Cryptographic Error When Starting Cognos Configuration

When you start Cognos Configuration, the following error message may appear:

The cryptographic information may have been corrupted or the cogstartup.xml file is invalid. You may have to fix this file or remove it from disk. For more information, see the Installation and Configuration Guide.

This error occurs when Cognos 8 Controller components detect an error in the cogstartup.xml file. This can occur when the cogstartup.xml file is manually edited and there is an error in the changed text.

To resolve the problem, replace the cogstartup.xml file with a copy from your backup location.

Current Configuration Settings Are Not Applied to Your Computer

You change default property values or add a resource to your installation in Cognos Configuration. After saving the current configuration, you may not see the changes or be able to use the resource in the run-time environment.

To apply the new settings to your computer, you must restart the Cognos 8 service.

Steps to Restart the Cognos 8 Service

1. Start Cognos Configuration.
2. From the Actions menu, click the appropriate command:
   - If the Cognos 8 service is currently running, click Restart.
     This action starts all installed services that are not running and restarts services that are running. If you want to restart a particular service, select the service node in the Explorer window and then click Restart from the Actions menu.
   - If the Cognos 8 service is stopped, 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.
     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.
Appendix A: Troubleshooting

Some Users Are Prompted to Log On When Using Active Directory Server

You configured Cognos 8 Controller components to use Microsoft Active Directory Server as an authentication provider. There is only one domain and all users are members of that domain. Some users can log on to the system without being prompted again in Cognos 8 Controller components. Other users get the Cognos logon prompt.

Single signon for some users may not work if they use Internet Explorer and the option to enable Integrated Windows Authentication is not enabled.

Steps to Enable Integrated Windows Authentication
1. In Internet Explorer, from the Tools menu, click Internet Options.

Users Are Repeatedly Prompted to Log On

You configured Cognos 8 Controller according to your organization’s requirements. Users are prompted to log on to the system repeatedly.

Cognos 8 Controller components determine the cookie domain from the HTTP request submitted by the client, which is typically a Web browser. In most network configurations, HTTP requests pass through intermediaries such as proxy servers and firewalls as they travel from the browser to Cognos 8 Controller components. Some intermediaries modify the information that Cognos 8 Controller components use to calculate the cookie domain, and Cognos 8 Controller components then cannot set cookies. To avoid this problem, configure the cookie domain.

Steps to Configure the Cookie Domain
1. Use the format and value that represents the widest coverage for the host to set the correct value for the cookie domain.

<table>
<thead>
<tr>
<th>Host</th>
<th>Format for domain</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>computer or server</td>
<td>computer or server name (no dots)</td>
<td>mycompany</td>
</tr>
<tr>
<td>suffix is .com, .edu, .gov, .int, .mil, .net, or .org</td>
<td>.name.suffix (two dots)</td>
<td>.mycompany.com</td>
</tr>
<tr>
<td>other</td>
<td>.name1.name2.suffix (three dots)</td>
<td>.travelinfo.co.nz</td>
</tr>
</tbody>
</table>

CGI Timeout Error While Connected to Cognos 8 Components Through a Web Browser

When performing operations through your Web browser, you receive the following error message: CGI Timeout, process will be deleted from server.

The error occurs when you use Windows Internet Information Services (IIS) as your Web server and the gateway is configured to use CGI. IIS has a default timeout for CGI applications.

To resolve this problem, you can configure the gateway to use ISAPI. IIS does not have a default timeout for ISAPI applications. Or, if you want to keep using a CGI gateway, you can increase the CGI timeout in IIS.

Steps to Change the Gateway to ISAPI
1. On the gateway computer, start Cognos Configuration.
2. Under Environment, for the Gateway URI property, change the cognos.cgi portion of the URI to cognosisapi.dll
3. In your Web browser, specify the ISAPI URI:
   http://computer_name/cognos8/isapi

Steps to Increase the CGI Timeout
1. In Administrative Tools, start Internet Information Services (IIS).
2. Under the local computer node, right-click Websites and select Properties.
3. In the Home Directory tab, click Configuration.
4. In the Process Options tab, increase the CGI script timeout.
Appendix A: Troubleshooting
**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.

**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 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 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 Cognos component that issues certificates identification to each computer on which components are installed. You can also use a third-party certificate authority.

**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 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 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 Cognos namespace.

**content store**
The database that contains data that 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 Cognos namespace itself; and information about scheduling and bursting reports.

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

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

**credentials**
Information stored about the identity of a 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 Cognos components. If a user schedules or programs an action, then 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 though Cognos 8.

**deployment archive**
A file used for deployment. A deployment archive contains the data from the content store that is being moved.

**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.

**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 third-party authentication sources or can be local to 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 a 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.
**job**
A group of runnable objects, such as reports, agents, and other jobs that you run and schedule as a batch.

**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 Cognos products, you can specify a locale for the product interface (product locale) and for the data in the report (content locale).

**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 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.

**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.

**response file**
An ASCII file that contains the setup data that is needed to automate an installation. For Cognos installations, the response file automates only the process of copying files with the default configuration.

**security provider**
See Authentication Provider.

**smart client**
An Internet technology that allows the user's local applications to interact with server-based applications through the use of Web services. For example, a smart client running a word processing application can interface with a remote database over the Internet in order to collect data from the database to be used in the word processing document.

**user**
A person accessing a Cognos 8 application. Authenticated user definitions and information, such as first and last names, passwords, IDs, locales, and email addresses, are maintained in third-party authentication sources.
Other user information, such as the location of personal folders or preferred formats for viewing reports, is stored in Cognos 8.
Symbols
.jar file
   error when starting configuration, 149
.NET Framework
   deleting files in cache, 138
   verifying whether running supported version, 141

A
access permissions
   definition, 153
   granting, 101
Active Directory Server
   authenticating in multiple domains, 108
   enabling single signon, 109
   single signon problems, 150
   using for authentication, 106
   with an LDAP namespace, 115
Add-in for Excel
   configuring the default installation, 95
   troubleshooting, 140
add-in for Excel
   installing, 38
adding
   namespaces, 101
advanced properties
   for Active Directory Server, 108
aliases
   configuring on Web servers, 47
   definition, 153
anonymous access
   definition, 153
   disabling, 104
anonymous logon
   disabling, 106
application data
   backing up, 26
   upgrading, 27
application server startup script fails, 147
application servers
   enabling network COM+ access, 59, 70
   servlet gateways, 78
application tier components
   definition, 153
   installing, 35
applications
   COM+, 68
   ASP.NET, 35
   installing, 35
   verifying whether installled, 138
authentication
   Active Directory Server, 150
   custom authentication providers, 113
   authentication (cont’d)
   custom user properties for LDAP, 121
   definition, 153
   disabling anonymous logon, 106
eTrust Siteminder, 123, 124, 125
   in domain trees for Active Directory Server, 108
   LDAP, 114
   LDAP using Active Directory Server, 115
   LDAP using IBM Directory Server, 117
   LDAP using Novell Directory Server, 118
   LDAP using Sun ONE Directory Server, 120
   mapping Controller users to Cognos 8 users, 104
   NTLM, 126
   SaferAPIGetTrustedSignon function, 112
   single signon for NTLM, 126
   single signon using eTrust SiteMinder, 125
   single signon using LDAP, 123
   SSL for eTrust SiteMinder, 125
   SSL using LDAP, 122
authentication method
   Controller Web Services Server, 101
authentication namespaces
   deleting, 127
   trusted signon plug-in for Cognos Series 7, 111
   using, 101
authentication providers
   definition, 153
authentication with single signon
   for Active Directory Server, 109
   for Cognos Series 7, 111
B
backups
   application data, 26
   the content store, 42
Bind user DN and password property
   special characters for LDAP namespace, 114
C
cache
   deleting files from Microsoft .NET Framework, 138
   ccr.exe
   troubleshooting, 138
   CCR82_DM.zip, 59, 74
   ccrws operations page
   troubleshooting, 139
certificates
   definition, 153
   certification authority
   definition, 153
   CFG-ERR-0106 error, 142
   CGI program, 78, 88
Index

CGI timeout error, 150
changing a URL, 76
Cognos 8 gateway, 78
configuration template, 89
Controller database connections, 91
default configuration settings, 76
default time zone, 90
characters unsupported, 142
chase referrals, 108
choosing Controller consolidation model, 29
cipher suites setting a priority for SSL connections, 84
client computers troubleshooting Add-in for Excel, 140
client installation add-in for Excel, 38
Cognos 8 authentication, 102
Cognos 8 Business Intelligence integration, 18
Cognos 8 Controller components, 9 configuring, 53
connecting from a Web browser, 61, 75
connecting from Cognos Connection, 60, 75
connecting from Microsoft Excel, 61, 75
copying components, 129
default settings, 31
installation options, 13
problems starting, 138
problems starting under VMWare, 138
standard reports package, 58, 73, 131
system requirements, 31
troubleshooting logons, 140
troubleshooting missing link in Cognos Connection, 137
uninstalling, 31, 39
Cognos 8 Controller Add-in for Excel troubleshooting, 140
Cognos 8 service restarting, 137
specifying resources, 89
starting, 64, 149
testing, 67
Cognos 8 users mapping to Controller users, 104
Cognos Application Firewall configuring, 84
Cognos BI server server not available, 142
Cognos Configuration, 53
cannot save changes, 147
component description, 9
invalid settings, 142
problems opening, 136
running in unattended mode, 131
Cognos Connection component description, 9
connecting from a Web browser, 55
troubleshooting missing Controller link, 137
Cognos Connection Integration Enabler component, 10
Cognos Connection Integration Enabler (cont’d)
verifying whether installed, 137
Cognos Controller, 103
groups, 103
Cognos Controller Configuration, 53
Cognos Controller database creating, 41
Cognos namespace recreating, 148
Cognos Series 7 enabling single signon, 111
trusted signon plug-in, 111
using for authentication, 109
Cognos Viewer component description, 9
COGNOSCONTROLLER process troubleshooting, 139
cogstartup.lock file, 136
cogstartup.xml file invalid file, 149
collation sequences case-sensitive, 142
COM+ application, 68
COM+ Server, 68 configuring, 60, 71, 133
credentials, 60, 71, 133
enabling, 59, 70
verifying whether running, 139
common gateway interface (CGI)
definition, 153
replacing, 78, 88
common symmetric key in cryptographic provider, 80
communications distributed components, 65
components Cognos Configuration, 9
Cognos Connection, 9
Cognos Viewer, 9
configuration requirements on multiple computers, 17
configuration requirements on one computer, 14
configuration requirements on two computers, 15
Content Manager, 10, 35
Controller Client Application Server, 10
Controller data mart database, 11
Controller Web Services Server, 10
distributing on multiple computers, 14
Framework Manager, 11
gateway, 35
installing, 35
installing on one computer, 13
load balancing distribution example, 16
modeling, 11
Report Server, 10, 35
role-based distribution example, 15
third-party, 9
used by Cognos 8 Controller, 9
compound file error, 140
Confidentiality algorithm, 81
configuration changing the template, 89
cryptographic information cannot be encrypted, 148
configuration (cont’d)
error when encrypting information, 148
lock file, 136
requirements for single signon with Microsoft Analysis
Server or Microsoft SQL Server, 107
settings not applied, 149
testing, 55
troubleshooting, 147
unable to open Cognos Configuration, 136
unable to save, 148
upgrading, 27
workflows, 21
configuration files
exporting, 131
configuration requirements
on multiple computers, 17
on one computer, 14
on two computers, 15
configuration settings
changing, 76
default, 37
configuration tools, 129
configuring
a Cognos Series 7 namespace, 110
an Active Directory namespace, 107
Cognos 8 Controller, 53
COM+ Server, 60, 71, 133
Content Manager computers, 63
Controller database connections, 56, 69, 132
custom authentication providers, 113
destination for log messages, 86
distributed installations, 61
Enhanced Reporting Optimization, 93
eTrust SiteMinder namespace, 124
Framework Manager, 66
gateway computers, 65
ISAPI for the gateway, 66
JDBC drivers, 45
LDAP namespace, 114
LDAP namespace for Active Directory Server, 115
LDAP namespace for IBM Directory Server, 117
Microsoft .NET Framework, 48
NTLM namespace, 126
Report Server components, 65
routers, 51
services for the gateway, 66
shared trust with other servers, 83
single computer installations, 53
SSL protocols
temporary file location, 85
transfer specification files (.ats), 129
Web browsers, 50
Web server, 47
connecting to Cognos 8 Controller
from a Web browser, 61, 75
from Cognos Connection, 60, 75
from Microsoft Excel, 61, 75
connecting to Cognos Connection, 55
connection management
for the content store, 54, 63
connections
Controller database, 56, 69, 132
connections (cont’d)
definition, 154
consolidation
load balancing, 16
consolidation model, 29
content locales, 90
definition, 154
Content Manager
changing the time zone, 90
component description, 10
definition, 154
installing, 35
setting up a database, 42
Content Manager computer
configuring, 63
Content Manager URIs property
on Report Server computers, 65
content store
backing up, 26, 42
creating, 31, 42
DB2, 43
definition, 154
deleting tables from the database, 147
invalid settings, 142
Microsoft SQL Server, 43
Oracle, 43
setting up database clients, 45
setting up JDBC drivers, 45
Sybase Adaptive Server Enterprise, 44
third-party components, 11
upgrading, 27
content stores
connection management, 63
setting database connections, 63
Controller
server components, 9
Controller application
verifying whether COM+ Server running, 139
Controller Client Application Server
components, 10
Controller Client Distribution Server
verifying URI for Cognos Connection, 137
Controller Configuration
server components, 9
Controller consolidation model
choosing, 29
Controller data
upgrading, 27
Controller data mart, 11
creating, 46
database connection properties, 57, 69
define data source, 58, 72, 73
installing JDBC driver, 34
Controller database connections
changing, 91
configuring, 54, 69, 132
Controller databases
creating Microsoft SQL Server, 41, 46
creating Oracle, 42, 46
Controller Framework Manager Model
components, 11
Controller standard reports package, 10
Controller users
  mapping to Cognos 8 namespaces, 104
Controller Web Services Server
  authentication method, 101
  components, 10
  verifying whether running, 139
ControllerLaunch.xml, 137
ControllerLaunch.xml file, 65
  troubleshooting, 137
ControllerProxyServer
  troubleshooting, 138
ControllerStudio.xml, 137
ControllerXLPusher.dll, 141
cookies
  customizing, 91
  enabling in Web browsers, 50
copying
  Cognos 8 Controller components, 129
copyright, 2
creating
  Cognos Controller database, 41
  content store, 31, 42
  Controller data mart database, 46
credentials
  COM+ Server, 60, 71, 133
  definition, 154
  resetting for Microsoft SQL Server, 139
cross-script checking
  configuring in Cognos Application Firewall, 84
cryptographic error, 149
cryptographic information cannot be encrypted, 148
custom authentication providers, 113
custom user properties
  from Active Directory Server, 107
  LDAP, 121
customizing cookie settings, 91
data entry forms
  upgrading, 28
data mart database
  define data source, 58, 73
  installing JDBC driver, 34
  setting connection properties, 57, 69
data source connections
  repairing, 140
  troubleshooting, 140
data sources
  definition, 154
  third-party components, 11
database client
  setting up for a content store, 45
  setting up for a logging database, 86
database connection strings
  IBM DB2, 63
  Microsoft SQL Server, 63
  Oracle, 63
database connection strings for content store
  IBM DB2, 54
  Microsoft SQL Server, 54
  Oracle, 54
database connections
  troubleshooting, 139
database connections, See data source connections
databases
  creating Controller tablespaces, 42, 46
  creating for Cognos Controller, 41
  creating for Controller data mart, 46
  deleting tables, 147
  destination for log messages, 86
  performance optimization for Oracle, 27, 74
  upgrading, 27
DB2
  content store, 43
  environment variables, 43
DB2 databases
  setting up JDBC drivers, 45, 87
default configuration settings, 37, 76
  Tomcat, 37
deleting
  anonymous access, 104
distributed installation, 14
distributed installations
  configuring, 61
  configuring Framework Manager, 66
  installation and configuration workflows, 22
  load balancing example, 16
  role-based example, 15
  scenarios, 13
domains
  authentication in domain trees for Active Directory Server, 108
  setting for cookies, 91
DPR-ERR-2022 error, 146
data source connections, See database connections
development environments, 33
environment properties
  configuring for Report Server components, 65
environment variables
  DB2, 43
  Oracle, 43
environments
  supported, 33
  supported operating systems, 33
error messages
  An error occurred while trying to access the server, 139
  CFG-ERR-0106, 142
Index

error messages (cont’d)
  CGI timeout, 150
  ControllerXLPusher.dll, 141
  corrupt cryptographic information, 149
  cryptographic information cannot be encrypted, 148
  DPR-ERR-2002, 146
  DPR-ERR-2058, 145
  Java Runtime Environment, 149
  No database configured, 140
  Page cannot be found, 138
  The file is not a valid compound file, 140
  VMWare cannot run the ccr.exe file, 138
  You are about to navigate away from this page, 137

cTrust SiteMinder
  configuring namespaces, 124
  enabling single signon, 125
  protecting the Cognos 8 Web alias, 125
  SSL, 125
  using for authentication, 123

event log
  destination for log messages, 86

Excel
  installation of add-in, 38
  remote installation of the Add-in for Excel, 95

Excel Add-in
  troubleshooting, 141

Excel add-in
  troubleshooting, 140

Excel link report formulas
  upgrading, 29

Excel.exe.config, 141

exporting
  configuration files, 131

External identity mapping property
  special characters for LDAP namespace, 114
  external identity mapping property
  editing for an LDAP namespace, 123

files
  destination for log messages, 86
  response.ats, 130
  using a previous installation version, 129

firewalls
  access between Framework Manager and Cognos 8, 66
  flat files
    specify import directories, 59, 72
  forms
    upgrading data entry, 28
  Framework Manager
    accessing Cognos 8 outside a firewall, 66
    component description, 11
    configuring, 66
    installing, 38
    testing installation and configuration, 56, 61, 68
  Framework Manager model
    extract and publish, 59, 74

Gateway
  configuring to use a namespace, 88

Gateway (cont’d)
  installing, 35
  recommended settings for Microsoft IIS, 150
  server components, 10
  using alternate, 88
  when to use ISAPI, 150

Gateway computers
  configuring, 65

Gateway Integration Enabler component, 10

Gateways
  configuring a servlet, 66
  configuring for Cognos 8, 78
  configuring ISAPI, 66
  definition, 154

Global configuration
  setting, 90

granting
  access permissions, 101

groups
  Cognos Controller, 103
  definition, 154

hosts file
  troubleshooting, 138

HTML cookies
  customizing settings, 91

IBM DB2
  creating connection strings, 63
  creating connection strings for content store, 54

IBM Directory Server
  with an LDAP namespace, 117

IIS Web server
  single signon with Active Directory, 109

import directories
  for flat files, 59, 72

importing
  Controller standard reports package, 58, 73, 131

installation
  all components on one computer, 13
  checklist, 31
  testing, 55
  workflows, 21

installation files
  transfer specification file (.ats), 129

installation tools
  running, 129

installing
  add-in for Excel, 38
  application tier components, 35
  ASP.NET, 35
  changing the default for Add-in for Excel, 95
  Cognos 8 Controller, 31
  during an upgrade, 26
  Framework Manager, 38

Microsoft .NET Framework, 35

integrating
  third-party components, 9
integration with Cognos 8 BI, 18
interface
customizing language support, 90
Internet Explorer
browser settings, 50
connecting to Cognos 8 Controller, 61, 75
interoperability with Cognos 8 BI, 18
invalid cogstartup.xml file, 149
invalid settings
Cognos Configuration, 142
content store, 142
iPlanet Web Server See Sun Java System Web Server
ISAPI
accessing Cognos 8, 78
configuring for gateway, 66
when to use for a gateway, 150

J
Java
configuring servlet gateway for Java-compatible Web servers, 78
Java error when starting configuration, 149
Java Runtime Environment (JRE), 47
Java scripts
enabling in Web browsers, 50
JAVA_HOME setting, 149
JDBC drivers, 45
installing for Controller data mart, 34
setting up DB2 databases, 45, 87
setting up Oracle databases, 45, 87
job steps
definition, 155
jobs
definition, 155

L
language
customizing for user interface, 90
LDAP
Active Directory Server, 115
configuring a namespace, 114
custom properties, 121
editing the External identity mapping property, 123
enabling single signon, 123
enabling SSL, 122
IBM Directory Server, 117
Novell Directory Server, 118
Sun ONE Directory Server, 120
using for authentication, 114
load balancing
enabling and disabling services, 89
for consolidation, 16
load sharing
multiple server access to reporting database, 97
locales
content, 90
definition, 155
global configuration setting, 90
localhost
changing, 76
log database
deleting tables, 147
log files, 135
configuring a destination, 87
locale configuration, 136
run-time, 136
silent mode, 136
startup configuration, 135
transfer, 135
transfer summary, 135
uninstallation, 136
log messages
destination, 86
enabling for Cognos Application Firewall, 84
log server
messages, 86
logging database
creating, 42
logging databases, 86
configuring, 87
logons, 140
repeated, 150
resetting for Microsoft SQL Server database, 139
troubleshooting, 139, 140
M
messages
log server, 86
You are about to navigate away from this page, 137
Microsoft .NET Framework, 35
configuring, 48
deleting files in cache, 138
installing, 35
upgrading, 25
verifying whether running supported version, 141
Microsoft .NET Framework SDK
installing, 35
Microsoft Analysis Server
namespace requirement, 107
Microsoft Excel
connecting to Cognos 8 Controller, 61, 75
installation of add-in, 38
troubleshooting ControllerXLPusher.dll error, 141
Microsoft IIS Web servers
recommended gateway settings, 150
Microsoft SQL Server
content store, 43
creating connection strings, 63
creating connection strings for content store, 54
creating Controller databases, 41, 46
database connectivity, 33
namespace requirement, 107
modeling components, 11
modifying
response.ats file, 129
multi_domain_tree, 108
multiple computer installation, 14
N
namespace
recreating, 148
namespaces
adding, 101
configuring custom authentication providers, 113
configuring for a gateway, 88
definition, 155
deleting, 127
mapping Cognos 8 users to Controller users, 104
native authentication, 101
Netegrity SiteMinder
See eTrust SiteMinder
cross-script checking in Cognos Application Firewall, 84
network COM+ access
enabling, 59, 70
network outage
services fail to start, 145
No database configured - error, 140
no response generated - error, 146
notification database
deleting tables, 147
Novell Directory Server
with an LDAP namespace, 118
NTLM, 126
configuring, 126
enabling single signon, 126
NTLM, See also Windows native security (NTLM)

O
Oracle
content store, 43
creating connections strings, 63
creating connections strings for content store, 54
creating Controller databases, 42, 46
creating Controller tablespaces, 42, 46
database connectivity, 33
database JDBC drivers, 45, 87
environment variables, 43
performance optimization job, 27, 74

P
Page cannot be found - error, 138
passports
definition, 155
IDs, 101
password
resetting for Microsoft SQL Server database, 139
path
setting for cookies, 91
performance
Oracle optimization, 27, 74
portal
errors in starting, 145, 146
ports
changing, 76
default configuration settings, 37
problems opening Cognos Configuration, 136
product locales
definition, 155
proof of concept, 53, 66
properties
temporary file location, 85
Publish to Data Mart model, 11
extract and publish, 59, 74
Q
quality of protection in SSL connections, 84
R
recreating the Cognos namespace, 148
remote installation
Add-in for Excel, 95
add-in for Excel, 38
remote log servers
configuring, 87
destination for log messages, 86
repairing database connections, 140
repeated logons, 150
replacing
common gateway interface (CGI), 88
Report Server
components, 10
configuring, 65
installing, 35
reporting components
testing, 55, 67
reporting database
access using multiple servers, 97
reporting package
importing, 58, 73, 131
reports
upgrading, 28
resources
specifying for the Cognos 8 service, 89
response files
definition, 155
response.ats, 129
using, 130
response.ats file
modifying, 129
restarting services, 137
roles, 103
Cognos Controller, 103
routers
configuring, 51
running
configuration tools, 129
installation tools, 129
Microsoft Internet Application Programming Interface, 88
S
SaferAPIGetTrustedSignon function
using for authentication, 112
scripts
to delete tables from databases, 147
SDK, .NET Framework, 35
secure flag
setting for cookies, 91
secure LDAP communication, 122
Secure Sockets Layer, See SSL protocol
security providers
definition, 155
security providers (cont'd)
  third-party, 104

server authentication
  Cognos 8 Controller, 101

server components
  Controller, 9
  Controller Configuration, 9
  gateway, 10

server time zones
  changing, 90

servers
  COM+, 68

services
  enabling and disabling, 89
  fail to start after network outage, 145
  restarting, 137
  starting, 64

servlet gateway
  configuring, 78

setting
  communication, 65
  global configuration, 90

shared trust
  setting up between Cognos 8 and other servers, 83

silent configurations, See unattended configurations

silent installations, See unattended installations

silent mode, See unattended mode

single computer installation
  installation and configuration workflows, 22

single computer installations, 13
  configuring, 53

single signon
  Active Directory Server, 150
  enabling, 105
  eTrust SiteMinder user directory, 125
  for a Cognos Series 7 namespace, 111
  for an Active Directory namespace, 109
  LDAP namespace, 123
  NTLM namespace, 126

SiteMinder
  cross-script checking in Cognos Application Firewall, 84

special characters
  in LDAP namespace properties, 114

SQL Server databases
  creating content store, 43
  creating Controller databases, 41, 46
  resetting logon credentials, 139

SSL
  eTrust SiteMinder user directory, 125
  LDAP namespace, 122
  quality of protection, 84
  setting up shared trust with other servers, 83

SSL protocols
  configuring

staged upgrade, 30

standard reports package
  importing, 58, 73, 131

starting
  Cognos 8 Controller See testing Cognos 8 Controller
  Cognos 8 service, 55
  Cognos 8 services, 64
  problems, 141

starting (cont'd)
  troubleshooting Cognos 8 Controller, 137, 138

startup
  Cognos 8 service, 149
  configuration lock file, 136
  problems, 141
  startup script fails, 147
  studio bar
    troubleshooting missing Cognos 8 Controller link, 137

Sun Java System Web Server
  servlet gateway, 78

Sun ONE Directory Server
  with an LDAP namespace, 120

Sun ONE Web Server See Sun Java System Web Server

supported environments, 33

Sybase Adaptive Server Enterprise
  content store, 44

system requirements, 31

T

tables
  deleting from a database, 147

tablespaces
  creating for Controller database, 42, 46

temporary file location
  configuring, 85
  properties, 85

testing
  Cognos 8 Controller configuration, 60, 74
  Cognos 8 Controller database connection, 139
  Cognos 8 service, 67
  reporting components, 55, 67

text files
  specify import directories, 59, 72

third-party components
  content store, 11
  data sources, 11

third-party products
  upgrading, 25

time zones
  changing in configuration, 90

Tomcat
  default configuration settings, 37
  transfer specification files (.ats)
  troubleshooting, 140

U

UDB, See DB2

UDL
  troubleshooting corrupted file, 140
  troubleshooting missing file, 140

unable to open Cognos Configuration, 136

unattended configuration
  setting up, 129, 131

unattended configurations, 129

unattended installations, 129

response files, 130

setting up, 129

transfer specification files, 129
unattended mode, 129
  running Cognos Configuration, 131
uninstalling
  before upgrading, 26
  Cognos 8 Controller, 31, 39
unsupported characters, 142
upgrading, 25
  application databases, 27
  data entry forms, 28
  Excel link report formulas, 29
  in a new directory, 30
  Microsoft .NET Framework, 25
  third-party products, 25
  troubleshooting subsequent problems, 138
  user-defined reports, 28
URI
  changing, 76
  default configuration settings, 37
  verifying for Cognos Connection, 137
user interface
  customizing language support, 90
User lookup property
  special characters for LDAP namespace, 114
user-defined reports
  upgrading, 28
users
  definition, 155
  using
    preconfigured configuration files, 129
V
version of document, 2
virtual directories
  setting up, 47
VMWare
  problems running ccr.exe file, 138
W
warning messages
  You are about to navigate away from this page, 137
Web aliases
  setting up, 47
Web browsers
  configuring, 50
  errors in starting the Web portal, 146
  errors when starting the web portal, 145
Web server
  configuring, 47
Web servers
  servlet gateways, 78
  single signon with Active Directory and IIS Web server, 109
WebLogic
  startup script fails, 147
WebSphere
  startup script fails, 147
Windows
  system requirements, 31
  Windows authentication, 102
Windows event log
  destination for log messages, 86
Windows IIS
  recommended gateway settings, 150
Windows native security (NTLM)
  enabling single signon, 126
  using for authentication, 126
workflows
  installation and configuration, 21
Y
You are about to navigate away from this page - warning, 137
Z
zip file CCR82_DM, 59, 74