# COGNOS(R)
# ACCESS MANAGER

## ADMINISTRATOR GUIDE

COGNOS®
THE NEXT LEVEL
OF PERFORMANCE™

## Product Information

This document applies to Access Manager 7.3 and may also apply to subsequent releases. To check for newer versions of this document, visit the Cognos support Web site (http://support.cognos.com).

## Copyright



Information about Cognos Products and Accessibility can be found at www.Cognos.com

# Table of Contents

# Chapter 1: Security and Access Manager

Access Manager provides a centralized environment to define, store, and maintain security information for Cognos business information applications.

In one central location, you can set up and maintain secure user access to data, such as cubes and reports, that are created in other Cognos applications. With Access Manager, you can also set up and maintain user signon information and auto-access privileges for the data sources and servers that contain the required data.

You must use Access Manager with:

- Architect
- Cognos Query
- Upfront
- Impromptu Web Reports
- Visualizer
- NoticeCast

You can choose to use Access Manager with:

- Impromptu
- PowerPlay
- Transformer

You should plan your security strategy and implement it in Access Manager before you start using other Cognos products. First, you must identify and create users. Then you must decide how you want to group users with similar needs for access to information, and give them memberships in user classes. These user classes are given access privileges to the required application servers, such as PowerPlay Enterprise Server and Transformer Server, and data sources, such as Oracle, Sybase, and local cubes.

After you set up your security information in Access Manager, you apply that information in the other Cognos products.

In this version of Access Manager, you can store authentication data in one of the following sources:

- a namespace on an LDAP directory server
- a local authentication export file (.lae)

For information about each type of authentication source, see "Set Up An Authentication Source" (p. 21).

### Related Topics

- "Automate Administration" (p. 19)
- "Delegate Administration" (p. 19)
- "Set Up a Namespace: Overview" (p. 26)
- "Basic Signons" (p. 15)
- "Common Logon or Single Signon" (p. 16)
- "External Signons" (p. 15)
- "Identify Users: Overview" (p. 14)

# Access Manager Components

When you install a Cognos product, several Access Manager components are available:

### Access Manager Administration

Administrators use this Windows-based tool to set up and maintain user classes, users, server connection information, and access to data sources. There are also two automation interfaces, Access Manager Batch Maintenance, and OLE Automation.

### Access Manager Server

The Access Manager Server is a Cognos security component that manages two services:

- a ticket service

  The service that issues tickets used to maintain single signons for users of Web-based Cognos applications. The tickets are issued for a specified period of time so that users can access multiple Cognos applications without having to re-enter authentication data.

- an authentication service

  The service used for authenticating users of Web-based Cognos applications. By default, this service is not enabled.

An Access Manager Server can be configured as either a ticket service or an authentication service, or both.

At least one Access Manager Server is needed for each Cognos application. We recommend that you install it on the same computer as the directory server. To implement failover and load balancing for the Access Manager Server, install additional Access Manager Servers and configure load balancing in Configuration Manager.

### SunONE Directory Server

Access Manager supports SunONE Directory Server, which is an LDAP-compliant data store. You can use a directory server to store and distribute your security information. Although not a Cognos product, SunONE Directory Server is distributed with Access Manager.

For more information about SunONE Directory Server, see the installation and configuration guide for your product.

### Directory Server Configuration

Use Configuration Manager to configure your directory server to work with your Cognos product.

For more information about directory server configuration, see the installation and configuration guide for your product.

### Access Manager Trusted Services Plug-in Software Development Kit

This software development kit (SDK) allows you to extend Access Manager functionality so you can use your existing security infrastructure with Access Manager.

### Configuration Manager

All users can run Configuration Manager when they work in a secured environment to specify the source for their security information. They can specify whether they will use a directory server or a local authentication export file (.lae).

For more information see, "Configure an Authentication Source" (p. 13).

### Windows Common Logon Server

A server that records information about the users of a Windows-based application so that they can log on once and access multiple data sources.

### Related Topics

- "Apply Security in Other Cognos Applications" (p. 10)
- "Available Security Options" (p. 9)
- "Configure an Authentication Source" (p. 13)
- "How Cognos Applications Use Authentication Data" (p. 11)
- "Secure Sockets Layer (SSL) Security" (p. 13)

# Available Security Options

Access Manager provides user class protection for and auto-access to data sources and servers. You can combine these with any security options you may already have, such as

- password protection for data sources provided by the application
- relational database management system (RDBMS) passwords
- server passwords

When users select a data source, the application prompts them for user ID and password information depending on the combination of security options you define.

### User Class Protection

User class protection is a type of security that prevents a user from viewing a data source unless the user provides a user name and password when prompted by the application. If the user is a member of the user class that has access to the data source, they are given access.

Setting up user classes helps you to specify what information users may access and to prevent unauthorized users from accessing the information. For example, a Transformer administrator protects a cube by applying user classes (created in Access Manager) to specific dimensions in the cube. PowerPlay users who access the cube are able to view only those dimensions that their user class has access privileges to.

For more information about user classes, see "Set Up User Classes: Overview" (p. 56).

### Auto-Access

Auto-access is a method of accessing a password-protected cube, database, or server without being prompted for logon information. Access Manager works with your application to implement auto-access.

The advantages of using auto-access are that it eliminates the need to remember and enter user IDs and passwords for multiple locations, batch processes can run without interruption, and it is easier to update user signon information because you store the information in one central location.

For more information about auto-access, see "Provide Auto-Access for a User" (p. 52).

### Password Protection

Password protection is a type of security that prevents a user from viewing a data source (such as a cube or catalog) unless the user enters a password when prompted by the application. The advantages of using password protection as a form of security are that it is easy to implement and it provides more secure data. You do not need Access Manager to implement password protection.

For more information about the available password protection options in an application, see the online help for that application.

### Related Topics

- "Access Manager Components" (p. 8)
- "Apply Security in Other Cognos Applications" (p. 10)
- "Configure an Authentication Source" (p. 13)
- "How Cognos Applications Use Authentication Data" (p. 11)
- "Secure Sockets Layer (SSL) Security" (p. 13)

# Apply Security in Other Cognos Applications

After you plan your security strategy and implement it in Access Manager, you apply it from within Cognos applications. Access Manager security works in Cognos applications in the following ways:

### Access Manager, Transformer, and PowerPlay

You can use Access Manager user classes within Transformer to apply restrictions to Transformer models, and then restrict user classes from accessing specific dimensions of the cubes created from those models. When users subsequently view the cubes in PowerPlay reports, their view is restricted, based on the security applied in Transformer.

### Access Manager and PowerPlay Enterprise Server

You can apply security to a PowerPlay Enterprise server to prevent unauthorized access. You can then add cubes to the server, and specify the source of security, specified in Transformer, which is used to secure cubes.

### Access Manager and Upfront

You can apply restrictions on NewsBoxes and NewsItems in Upfront using the pre-defined user classes. These restrictions apply in addition to any cube- or report-specific restrictions that you applied in other Cognos applications. You can also specify in Access Manager whether or not you want your users to have a personal NewsBox.

### Access Manager and Impromptu

You can use pre-defined user classes to restrict access to portions of data in a catalog.

### Access Manager and Architect

You use pre-defined user classes to restrict access to portions of and allowable activities on specific models. These restrictions apply to the model in Architect, and to the model after it is exported to other Cognos applications for report or query creation.

### Access Manager and Visualizer

You secure the database or cube that the Visualization file references. You can secure the data source using Access Manager Administration.

### Access Manager and NoticeCast

You use pre-defined user classes to restrict access to your alerts and email lists.

### Related Topics

- "Access Manager Components" (p. 8)
- "Available Security Options" (p. 9)
- "Configure an Authentication Source" (p. 13)
- "How Cognos Applications Use Authentication Data" (p. 11)
- "Secure Sockets Layer (SSL) Security" (p. 13)

# How Cognos Applications Use Authentication Data

Each Cognos application that uses Access Manager follows the same process to identify a user's access to secure data.

| Process | Details |
|---|---|
| The user selects a secure data source, such as a cube or report. | The application reads user and user class information from an authentication source which you have defined to the application:<br>If the source is a namespace, the application looks to see if you specified a particular namespace to use. If you did not specify a namespace, the application uses the default namespace specified in Configuration Manager. If it does not find a default namespace there, it uses the default namespace specified in Access Manager Administration.<br>If the source is a local authentication export file (.lae) the user must have access to the file before the application can open it (p. 43). |
| If the Access Manager namespace authentication is configured for OS signons, Access Manager compares system information to the OS signon defined in the authentication source. | If there is a match, Access Manager identifies which user class the user belongs to and what access privileges the user has in accordance with the OS signon. It then automatically grants or denies the user access to the data source without the user having to provide a user ID or password.<br>If there is no match, or you have not defined an OS signon for that user, Access Manager prompts the user for basic signon information. |
| If the Cognos product is using a basic signon, Access Manager prompts the user for basic signon information, as defined in the authentication source. | Access Manager prompts the user for a user ID and password and compares them to the basic signon defined in the authentication source. If there is a match, Access Manager identifies which user class the user belongs to and what access privileges the user has in accordance with the basic signon. It then grants or denies the user access to the data source. |

| Process | Details |
| --- | --- |
| For products that do not support the union of user classes, if the user belongs to more than one user class, Access Manager prompts the user to specify which user class they want to use during the current session. | Access Manager identifies the access privileges for the user class, and then grants or denies the user access to the data source. If the user needs to change user classes, they must exit the data source and then reopen it again using a different user class. |
| For products that support the union of user classes, the user's access rights are the union of all of the rights of the user classes to which the user belongs. | |
| If Access Manager does not find a match for an OS signon, or if there is no valid basic signon, it considers the user not valid. | The application denies the user access to the data source. |

For more information about using Access Manager with Cognos applications, see "Set Up Security Across Applications" (p. 69).

### Related Topics

- "Access Manager Components" (p. 8)
- "Apply Security in Other Cognos Applications" (p. 10)
- "Available Security Options" (p. 9)
- "Configure an Authentication Source" (p. 13)
- "Secure Sockets Layer (SSL) Security" (p. 13)

# Configuration Options for Access Manager Authentication Components

Access Manager Components can be configured in different ways to interact with other components when authenticating users.

### Client and Default Web Authentication

By default, the Access Manager login and run-time components communicate directly with the directory server to authenticate users. To maintain session information, the Access Manager login and run-time components communicate with the Common Logon Server on Windows and for administration tools on UNIX and web applications, the Access Manager run-time component communicates with an Access Manager Server configured as a Ticket Service.

### Alternate Web Authentication

In web deployments, you can configure the Access Manager login component to communicate to an Access Manager Server configured as an Authentication Service. The Access Manager Server then communicates with the directory server to authenticate the user and to an Access Manager Server configured as a Ticket Service to maintain session information.

In a single machine deployment, the Access Manager server acts both as an Authentication Service and Ticket Service, both services communicating on different ports. In a multi-machine installation, multiple Access Manager Servers can be configured for either service. You may wish to set up more than one Authentication Service or Ticket Service for fail over and/or load balancing.

For more information, please refer to Cognos Planning Advanced Installations Guide.

# Configure an Authentication Source

To use the security information stored in Access Manager, users must indicate to their Cognos products what they intend to use as an authentication source. Otherwise, the products will not be able to locate and validate user privileges at runtime.

Users specify the authentication source by using the Access Manager - Runtime component in Configuration Manager, which is installed with all Cognos Series 7 products.

There are two main types of authentication sources:

- a directory server
- a local authentication export file (.lae)

### Related Topics

- "Access Manager Components" (p. 8)
- "Apply Security in Other Cognos Applications" (p. 10)
- "Available Security Options" (p. 9)
- "How Cognos Applications Use Authentication Data" (p. 11)
- "Secure Sockets Layer (SSL) Security" (p. 13)

# Secure Sockets Layer (SSL) Security

Access Manager supports SSL for the following types of communication:

- Communications that use secure hypertext transfer protocol (HTTPS) between a browser and the Web server. For more information about setting up SSL for your web server, see the installation and configuration guide for your product.
- Communications of confidential information to and from a directory server.
  - For client and default web authentication configurations, SSL can be used to secure the communication from the login process and Access Manager runtime to the directory server.
  - For alternate web authentication configurations, SSL can be used to secure the communication from the Access Manager Server Authentication Service to the directory server.
- Communications that exchange confidential information to and from the Access Manager Server Authentication Service. For alternate web authentication configurations, SSL can be used to secure the communication from the login process to the Access Manager Server Authentication Service.

For more information on configuring your directory server and Access Manager Server Authentication Service for SSL, see "Configure Secure Sockets Layer (SSL) on a Directory Server" (p. 24).

### Related Topics

- "Access Manager Components" (p. 8)
- "Apply Security in Other Cognos Applications" (p. 10)

- "Available Security Options" (p. 9)
- "Configure an Authentication Source" (p. 13)
- "How Cognos Applications Use Authentication Data" (p. 11)

# Identify Users: Overview

Access Manager allows different signon strategies for identifying users. Signon strategies can be identified at the namespace or user level. A signon strategy can use basic signons, operating system (OS) signons, or both. If more than one signon strategy is chosen at the namespace level, users within that namespace can be assigned either strategy.

You can also define logon attempts, lockout durations, and user ID preferences using namespace and user properties. Use namespace properties to define rules for passwords.

For more information, see "Access Manager Namespaces" (p. 14).

### Related Topics

- "Access Manager Namespaces" (p. 14)
- "Basic Signons" (p. 15)
- "Common Logon or Single Signon" (p. 16)
- "External Signons" (p. 15)
- "Integrated Windows Authentication" (p. 16)

## Access Manager Namespaces

A namespace in Access Manager contains the security information for one or more Cognos applications. Namespaces can be stored on a directory server, or in a local authentication export file (.lae). Using a directory server eliminates the need to distribute separate files to each user to enforce security. SunONE Directory Server is included as part of the Access Manager installation. Local authentication export files are generally used in situations where a user does not have access to a network, or in a demonstration environment. Local authentication export files are appropriate for single-user operations.

Except for testing purposes, use one namespace for all applications in your business enterprise platform. This approach will decrease maintenance effort. For example, if you use one namespace for PowerPlay Enterprise Server and another namespace for Upfront, the information for your users must exist in both namespaces.

If more than one namespace is being used, please note that if the same user exists in more than one namespace, changing any of the following fields will cause the change to appear in all namespaces:

- description
- surname
- given name
- mail
- telephone #
- preferred language

### Related Topics

- "Set Up a Namespace: Overview" (p. 26)
- "Basic Signons" (p. 15)
- "Common Logon or Single Signon" (p. 16)
- "External Signons" (p. 15)
- "Identify Users: Overview" (p. 14)

- "Integrated Windows Authentication" (p. 16)

## Basic Signons

For basic signons, Access Manager stores and manages both the user ID and password for each user.

You choose and enter basic signon information in Access Manager Administration. When users open a secured application, they are prompted for their assigned user ID and password.

### Related Topics

- "Set Up a Namespace: Overview" (p. 26)
- "Common Logon or Single Signon" (p. 16)
- "External Signons" (p. 15)
- "Identify Users: Overview" (p. 14)
- "Integrated Windows Authentication" (p. 16)

## External Signons

If your users already have signons for operating systems or other applications, you may not want to assign them additional signons for Access Manager. There are several ways to use existing signon information with Access Manager.

In addition, the Access Manager trusted services plug-in software development kit (SDK) can help address external authentication requirements.

For more information, see the Access Manager Trusted Services Plug-In *Software Development Kit Guide*.

### For Windows Users

If your users sign on to Windows, you can enter the Windows signon information for each user in Access Manager Administration. When a user opens a secured application, Access Manager looks for the Windows signon information and compares it to the signon information entered for each user in Access Manager Administration. If a match is found, the user is granted access to the secured application.

### For Web Users

If your users access secure applications through the Web, Access Manager can take advantage of Integrated Windows Authentication as well as credentials stored in the REMOTE_USER CGI environment variable.

To use the REMOTE_USER CGI environment variable, Access Manager matches the OS signon for a user to the value the environment variable returns.

For more information about Integrated Windows Authentication, see "Integrated Windows Authentication" (p. 16).

### Related Topics

- "Set Up a Namespace: Overview" (p. 26)
- "Basic Signons" (p. 15)
- "Common Logon or Single Signon" (p. 16)
- "Identify Users: Overview" (p. 14)
- "Integrated Windows Authentication" (p. 16)

## Common Logon or Single Signon

Users can access multiple secured Cognos applications in one session using common logon or single signon. Windows products use common logon, and Web-based products use single signon.

Common logon or single signon maintains user authentication data so users who have access can open multiple secure data sources using different Cognos products. This means users only have to provide a user ID and password once, even if they drill through different Cognos applications or navigate from one Cognos application to another. After a user opens a secure data source, common logon or single signon tracks the user and controls their access to multiple data sources.

### For Windows Users

In Windows, the Windows Common Logon server identifies the user and stores relevant security information locally on the user's computer. When a user invokes authentication for any Windows-based component of the Cognos platform, if the user has installed the Windows Common Logon server, a key icon appears in the system tray of the Windows taskbar. When the user opens another Cognos application, the second application uses the stored information to identify the user, and to enforce any security restrictions. The information to identify the user remains in the Windows Common Logon server until the user has closed all Cognos applications, or has logged off the Windows Common Logon server.

### For Web Users

For Web users, the ticket service issues a ticket when a user is identified. A reference to the ticket is stored in a cookie in the user's Web browser. When the user opens another Cognos application, the application uses the stored ticket information to identify the user, and to enforce any security restrictions. When the user's browser session ends, the cookie is deleted.

For more information about common logon or single signon, see the installation and configuration guide for your product.

### Related Topics

- "Set Up a Namespace: Overview" (p. 26)
- "Basic Signons" (p. 15)
- "External Signons" (p. 15)
- "Identify Users: Overview" (p. 14)
- "Integrated Windows Authentication" (p. 16)

## Integrated Windows Authentication

Integrated Windows Authentication is known as Windows NT Challenge Response.

Integrated Windows Authentication is a feature of the Microsoft Internet Information Server (IIS) that enables users who are already logged on to open other applications without typing their user ID and password again. It can be used with your Web products to simplify user logon. It does not affect access to administration utilities.

Integrated Windows Authentication works by allowing the Microsoft Internet Information Server (IIS) to get a user's Windows Domain Login Name from an Internet Explorer Web browser. If users connect with a different Web browser, such as Netscape, they must enter their user ID and password.

For more information about Integrated Windows Authentication, see the installation and configuration guide for your product.

You can also provide users with traditional signons, such as basic or operating system signons. For more information, see "Provide a User With a Signon" (p. 49).

### Notes

Access Manager supports Integrated Windows Authentication or Windows NT Challenge Response. For Microsoft Information Server (IIS) 5.x, this method of authentication is called Integrated Windows Authentication; for IIS 3.x and 4.x it is called Windows NT Challenge Response.

### Related Topics

- "Set Up a Namespace: Overview" (p. 26)
- "Basic Signons" (p. 15)
- "Common Logon or Single Signon" (p. 16)
- "External Signons" (p. 15)
- "Identify Users: Overview" (p. 14)

## Users

Namespaces contain users. Users are added and managed with the Access Manager administration interfaces. You can choose to link to users defined elsewhere in the directory server, rather than create them in the namespace. For more information about linking users, see "Enable External User Support" (p. 41).

All Access Manager users must belong to at least one user class, and can belong to many.

Users have properties that allow you to enter personal information, signon preferences, connection information for PowerPlay and Transformer servers, user class memberships, regional settings, and personal NewsBox availability in Upfront.

You can adopt one of two basic strategies when defining the types of users you want.

### All Users Have the Same Restrictions

You may want to give all of your users the same restrictions to secured information.

You do this by defining an anonymous user for your namespace. If your namespace is set up for anonymous users, all users are considered as a group, and share the same security restrictions. Those security restrictions are determined by the user classes that the anonymous user belongs to. Because anonymous users are considered as a group, no signon information is required to identify individual users.

If you choose to have anonymous users in a namespace, you do not need any other types of users except administrators.

### Users Have Different Restrictions

You may want to give different users different restrictions to secured information.

You do this by setting up your namespace for named users, or named users with guest users. Named users are considered individually, and have different security restrictions, depending on which user classes they belong to. Guest users are similar to anonymous users because they are considered as a group, and share the same security restrictions. Those security restrictions are determined by the user classes that the guest user belongs to.

Because named users do not share the same restrictions to information, they must be identified using one of the various signon strategies available. Because guest users are considered as a group, no signon information is required to identify individual users.

If you choose to have named users, or named users with guest users in a namespace, you cannot have anonymous users.

### Related Topics

- "User Classes" (p. 18)

## User Classes

User classes represent groups of users with identical authorization rights. Access Manager applies security at the user class level. You create user classes and add users to those user classes in Access Manager. Then you apply security for other Cognos products based on the existing user classes. User classes are arranged hierarchically, and commonly reflect your company's organizational structure.

You can restrict access to reports, cubes, NewsItems, and so on with user classes. User class security is different and separate from application-specific security such as a filter on a cube in PowerPlay.

If you have information that everyone needs access to, you can designate an existing user class to be the public user class. All users are automatically included in this user class. When you secure information against the public user class, all users have access to this information.

You can set time restrictions for system access and delegate administration duties for each user class, using user class properties.

For more information, see "Available Security Options" (p. 9).

### Related Topics

- "Users" (p. 17)

## Store Connection Information for Cognos Servers

You can store connection information for PowerPlay Enterprise and Transformer servers.

Storing connection information creates a list of valid servers for users to choose from when using Transformer or PowerPlay client applications.

You can also store signon information for Transformer servers in Access Manager. When users access a Transformer server, Access Manager supplies the necessary signon information.

### Related Topics

- "Store Signon Information for Secured Cubes" (p. 19)
- "Store Signon Information for Secured Databases" (p. 18)
- "Store Signon Information for Third Party Cubes" (p. 19)

## Store Signon Information for Secured Databases

If you have secured databases, you may not want users to have to supply signon information every time they access the databases. You can store information about secured databases in Access Manager, including the required signon information. You can then associate the stored signon information with individual users. This is convenient for users, and is essential for running batch jobs that access a secured database.

For example, if you have a user who runs batch jobs after regular business hours using a secured database, you can store the required signon information in Access Manager. You then associate the information with the user who runs batch jobs. When the batch job runs and accesses the secured database, Access Manager supplies the necessary signon information.

### Related Topics

- "Store Connection Information for Cognos Servers" (p. 18)
- "Store Signon Information for Secured Cubes" (p. 19)
- "Store Signon Information for Third Party Cubes" (p. 19)

## Store Signon Information for Secured Cubes

If you have secured PowerPlay cubes, you may not want users to have to supply signon information every time they access the cube. You can store information about secured PowerPlay cubes in Access Manager, including the required signon information. You can then associate the stored signon information with individual users.

For example, you may have a PowerPlay cube that is secured. You can store the required signon information in Access Manager. You then associate the information with individual users. When those users access the secured cube, Access Manager supplies the necessary signon information.

### Related Topics

- "Store Connection Information for Cognos Servers" (p. 18)
- "Store Signon Information for Secured Databases" (p. 18)
- "Store Signon Information for Third Party Cubes" (p. 19)

## Store Signon Information for Third Party Cubes

Cognos applications work with third party data that may be secured by the third party application. You may not want users to have to supply signon information every time they access the data. You can store the required signon information and other information about secured data in Access Manager. You then associate the stored signon information with individual users.

For example, you may have an Hyperion Essbase cube that is secured. You can store the required signon information in Access Manager. You then associate the information with individual users. When those users access the secured cube, Access Manager supplies the necessary signon information.

### Related Topics

- "Store Connection Information for Cognos Servers" (p. 18)
- "Store Signon Information for Secured Cubes" (p. 19)
- "Store Signon Information for Secured Databases" (p. 18)

## Delegate Administration

You can allow members of selected user classes to perform administrative tasks within Access Manager Administration. These administrative rights are carried forward to Access Manager's Web-based administration in Upfront.

User classes have properties that allow you to define whether or not members of a user class can see, add, and remove users, user classes, data sources, and PowerPlay and Transformer servers.

You can also specify whether or not the member of a user class can change various personal settings in Upfront.

### Related Topics

- "Automate Administration" (p. 19)
- "Set User Class Permissions" (p. 59)

## Automate Administration

You can automate the administration tasks you perform in Access Manager Administration. Use the batch command processor for simple automation tasks when ease of use is a consideration. Use OLE automation for more complex automation tasks that require a knowledge of computer programming.

### Batch Maintenance

Windows and UNIX users can use the batch command processor in Access Manager to create or delete users and user classes, and to set the properties of namespaces, users, user classes, PowerPlay and Transformer servers, and data sources.

The batch command processor can set values, but cannot return them. This means that conditional processing is not possible. The batch command processor can only execute scripts in which all object names are known. It cannot process collections of objects.

For more information about batch maintenance, see the Access Manager Batch Maintenance Guide.

### OLE Automation

Windows users with a knowledge of computer programming can use object linking and embedding (OLE) automation. OLE automation allows access to all functionality in the Access Manager Administration user interface. With OLE automation, you can use collections of objects, and you can set and return values for conditional processing.

For more information about OLE Automation, see the Access Manager Macro Reference Guide.

### Related Topics

- "Delegate Administration" (p. 19)

# Chapter 2: Set Up An Authentication Source

An authentication source contains security information about users, user classes, and the servers and data sources that users can access. You store connection information about your authentication sources in a Cognos Security Administration file (.csa).

Access Manager supports the following types of authentication sources:

- a namespace on an LDAP directory server
- a local authentication export file (.lae)

Use namespaces on a directory server when you have a large number of users who are connected to the same network as the directory server. Use .lae files when you have users who are not connected to the same network as the directory server, such as remote users or users working offline. You can also use .lae files as an alternate source, regardless of whether the user is connected to the network (p. 43).

The Cognos Security Administration file (.csa) contains all the connection information for directory servers and .lae files.

For more information about saving connection information, see "Save Authentication Source Connections" (p. 21).

### Related Topics

- "Access a Directory Server: Overview" (p. 22)
- "Alternate Authentication Sources: Overview" (p. 43)
- "Save Authentication Source Connections" (p. 21)
- "Set Up a Namespace: Overview" (p. 26)

## Save Authentication Source Connections

### Description

The first time you use Access Manager, an empty Cognos security administration file (.csa) automatically opens and is ready for use. Use this file to store connection information for all your authentication sources.

If you add new connection information to the file, and you have not saved it, Access Manager prompts you to save the file before you exit.

### Steps

1. From the File menu, click Save As.
2. In the File Name box, type the name of the file.
3. In the Save In box, select the location where you want to store the file.
4. Click Save.

### Tip

- To automatically open a specific Cognos security administration file (.csa) each time you open Access Manager, set the appropriate .csa file as the default. With the appropriate .csa file open in Access Manager, from the File menu, click Set As Default.

### Related Topics

- "Set Up An Authentication Source" (p. 21)

# Access a Directory Server: Overview

Access Manager uses an LDAP directory server as the main location for storing your authentication data. You need to install and configure a directory server. SunONE directory server can be obtained from your product installation. If you are already using a directory server to deploy authentication data for PowerPlay, Impromptu Web Reports, or PowerPlay Web, you can use your existing authentication database. Whether you use an existing directory server or install a new one, you will have to extend the server schema to include the object classes and attributes that Access Manager uses.

To store authentication data on a directory server, you must use Access Manager to set up a connection to the directory server. After you define a connection, you can create namespaces in which to store your user, user class, application server, metadata source, and data source information.

For information about setting up a directory server, see the installation and configuration guide for your product.

### Related Topics

- "Connect to a Directory Server" (p. 22)
- "Modify a Directory Server Connection" (p. 23)
- "Test a Directory Server Connection" (p. 24)
- "Set Up An Authentication Source" (p. 21)
- "Configure Secure Sockets Layer (SSL) on a Directory Server" (p. 24)

## Connect to a Directory Server

### Description

Before you can create namespaces in which to store your authentication data, you must create a connection to each directory server you intend to use. To successfully connect to a directory server, you need the required connection information, such as the server

- host (name or IP address)
- port
- base distinguished name (DN)

If you do not have this information, contact your directory server administrator.

After you connect to a directory server, you should test the connection to ensure that it is working properly.

For more information, see "Test a Directory Server Connection" (p. 24).

### Notes

It is recommended that you do not store the same authentication data in multiple directory servers. Otherwise, if you have to make modifications to the authentication data, you have to make the same modifications in every directory server. Using one directory server for all your security information not only guarantees that the information is always up-to-date, but also requires less maintenance.

### Steps

1. In the Authentication Information pane, click the Directory Servers folder.
2. From the Action menu, click Add Connection.

   The Directory Server Properties dialog box appears.
3. On the General tab, in the Host box, type the name or IP address of the server where the directory server is installed.
4. In the Port/SSL Port box, type the port the directory server uses.

   By default, the port is 389. The directory server installation assigns this port to LDAP servers. If you have more than one server on a computer, the port name distinguishes between the two servers.
5. In the Timeout box, type the maximum amount of time (in seconds) the user has to establish a connection to the directory server.
6. In the Base Distinguished Name (DN) box, type the DN for the root of the directory according to the LDAP standard.

   This DN is the name you typed in the Directory Suffix box when you installed the SunONE directory server (for example, o=Cognos, c=CA). If you did not install the directory server, contact the administrator for the required DN.
7. Click Log On.
8. Click OK.

### Related Topics

- "Access a Directory Server: Overview" (p. 22)
- "Modify a Directory Server Connection" (p. 23)
- "Test a Directory Server Connection" (p. 24)
- "Configure Secure Sockets Layer (SSL) on a Directory Server" (p. 24)

## Modify a Directory Server Connection

### Description

You may occasionally have to modify your directory server connection, or view the connection properties. For example, the directory server administrator may have changed the properties of the server, such as the base distinguished name (DN). Unless you make the same change to your directory server connection, you won't be able to use the connection.

After you modify a directory server connection, you should test the connection to ensure that it works properly.

For more information, see "Test a Directory Server Connection" (p. 24).

### Steps

1. In the Authentication Information pane, double-click the Directory Servers folder to list the contents.
2. Select the appropriate directory server.
3. From the Edit menu, click Properties.

   The Directory Server Properties dialog box appears.
4. Modify the connection properties as required.

### Related Topics

- "Access a Directory Server: Overview" (p. 22)
- "Connect to a Directory Server" (p. 22)

- "Test a Directory Server Connection" (p. 24)
- "Configure Secure Sockets Layer (SSL) on a Directory Server" (p. 24)


## Test a Directory Server Connection

### Description

You can test a directory server connection to verify whether it is working properly. Typically, you perform this task immediately after you set up or modify a new connection. However, there may be times when you have trouble working with namespaces. Testing the directory server connection will help you determine if the problem is connection-related.

If the test is not successful, contact your directory server administrator.

### Steps

1. In the Authentication Information pane, double-click the Directory Servers folder to list the contents.
2. Select the appropriate directory server.
3. From the Edit menu, click Properties.

   The Directory Server Properties dialog box appears.
4. On the General tab, click Test.

   A message appears indicating whether your directory server is responding.

### Related Topics


- "Access a Directory Server: Overview" (p. 22)
- "Connect to a Directory Server" (p. 22)
- "Modify a Directory Server Connection" (p. 23)
- "Configure Secure Sockets Layer (SSL) on a Directory Server" (p. 24)


## Configure Secure Sockets Layer (SSL) on a Directory Server

### Description

Secure Sockets Layer (SSL) is a standard protocol for providing a secure environment for communications over networks. Access Manager supports SSL for exchanging confidential information to and from your directory server, and between the Access Manager login process and the Access Manager Server Authentication Service.

To configure an SSL connection, you must either purchase certificates from a third-party certificate authority, or set up a certificate authority (CA) such as Netscape Certificate Server or Microsoft Certificate Server to issue and manage your own certificates. Refer to the documentation provided by the third-party certificate authority for additional information.

Certificates are stored in a certificate database. Access Manager requires that a cert7.db file format be used for the certificate database. Use a tool such as Netscape Navigator 4.x to add or update certificates in the cert7.db file.

For alternate web authentication configurations, configure SSL with the directory server, and then configure SSL between the Access Manager login process and the Access Manager Server Authentication Service:

### Steps to Configure SSL with a Directory Server

1. Enable SSL on the directory server. For more information, see your directory server documentation.
2. Obtain a cert7.db file, and ensure that the CA used in step 1 is trusted in this certificate database.
3. To administer the directory server in Access Manager Administration:
   - In the Authentication Information pane, double-click the Directory Servers folder to list the contents, and click the appropriate directory server in the list.
   - From the Edit menu, click Properties, and on the General tab, select Enable SSL check.
   - If the certificate database has not been configured, the SSL Configuration dialog box appears. Enter the location of your Netscape certificate database file (Cert7.db), and type the SSL port number in the Port/SSL Port box. By default, the port is 636.
   - Select the Require SSL for all connections check box if you want all communication with the directory server over an SSL port. This stops all communication over the directory server's non-secure port (by default 389).

     **Note:** If you select Require SSL for all connections, directory server clients can not connect through a non-secure port.
4. Configure the Access Manager runtime for SSL communication to the directory server on all computers that use Cognos security. For more information, see the Configuration Manager User Guide.

### Steps to Configure SSL Between Access Manager Login Process and the Access Manager Server Authentication Service

1. Generate the private key and certificate signing request (CSR) using AmKeyTool found in the *Cognos_installation*/bin directory on the computer that has an Access Manager Server installed:
   - Set your CLASSPATH environment variable:

| Environment | Environment variable |
|---|---|
| JRE 1.3 and Windows | set CLASSPATH=.;AmKeyTool.jar;sunjce_provider.jar ;bcprov-jdk13-113.jar;jce1_2_1.jar |
| JRE 1.3 and Unix | setenv CLASSPATH .:AmKeyTool.jar:sunjce_provider.jar:bcprov-jdk13 -113.jar:jce1_2_1.jar |
| JRE 1.4 and Windows | set CLASSPATH=.;AmKeyTool.jar;bcprov-jdk13-113. jar |
| JRE 1.4 and Unix | setenv CLASSPATH .:AmKeyTool.jar:bcprov-jdk13-113.jar |

   - On the command line, type: java AmKeyTool -c -f <generated CSR file> -k <private key location> -p <private key password> -d <certificate dn>

   For more information about the command line usage of AmKeyTool, type AmKeyTool on the command line.

   **Note:** Do not close this command line window until you complete the entire procedure.
2. Use the CSR generated in step 1 to obtain a certificate from your CA.

3. Import the certificate generated by the CA in step 2 into the keystore for the Access Manager Server. On the command line, type: java AmKeyTool -i -f <certificate file> -k <private key location> -p <private key password>.

   For more information on the command line usage of AmKeyTool, type AmKeyTool on the command line.
4. Enable SSL on the Access Manager Server Authentication Service. For more information, refer to the Configuration Manager User Guide.
5. Obtain a cert7.db file, and ensure that the CA used in step 2 is trusted in this certificate database.
6. Configure the Access Manager Web Authentication for SSL communication to the Access Manager Server Authentication Service on each computer with an installed Cognos gateway. For more information, see the Configuration Manager User Guide.

**Note:** If you install more than one Access Manager Server Authentication Service, you must repeat these steps for each service.

### Related Topics

- "Access a Directory Server: Overview" (p. 22)
- "Connect to a Directory Server" (p. 22)
- "Modify a Directory Server Connection" (p. 23)
- "Test a Directory Server Connection" (p. 24)

# Set Up a Namespace: Overview

If you intend to use a directory server to store your authentication data, you need to set up a namespace (also known as a directory) on the directory server. A namespace is where you actually maintain authentication data, such as user signons, user classes, and access privileges to data sources, metadata, and application servers.

For more information about modifying the authentication data in a namespace, see "Set Up An Authentication Source" (p. 21).

Preparing a namespace for use with Access Manager involves adding, logging on to, and setting the properties for the namespace.

### Related Topics

- "Add a Namespace" (p. 27)
- "Add a Namespace Administrator" (p. 30)
- "Define Regional Settings for Users in a Namespace" (p. 35)
- "Export a Namespace for Remote Users" (p. 37)
- "Log On to a Namespace" (p. 28)
- "Log On to a Namespace as Another User" (p. 29)
- "Provide Summary Information for a Namespace" (p. 30)
- "Set a Default Namespace for a Directory Server" (p. 36)
- "Set Password Properties for Users in a Namespace" (p. 34)
- "Set Signon Properties for Users in a Namespace" (p. 33)
- "Transfer Namespace Information Between Directory Servers" (p. 38)
- "Upgrade Namespaces" (p. 40)
- "Set Up An Authentication Source" (p. 21)

# Add a Namespace

### Description

You must create a namespace on a directory server before you can create users or user classes, or before you can add signon information for application servers or data sources that users need to access.

There is no limit to the number of namespaces you can create on a directory server. However, to simplify administration, we recommend that you use one namespace for all applications in your business enterprise platform.

To set up a namespace and add authentication data to it before you add the namespace to the directory server, you can create a namespace in a local authentication export file (.lae). You can then import the .lae file into an empty namespace on the directory server.

For more information, see "Import a Local Authentication Export File into a Namespace" (p. 44).

### Notes

You cannot have a space as the first character in the name of a namespace.

### Steps

1. In the Authentication Information pane, double-click the Directory Servers folder to list the contents.
2. Select the directory server you want to add a namespace to.
3. From the Action menu, click Add Namespace.

   The Administrator Access dialog box appears.
4. In the Runtime Administrator Distinguished Name (DN) box, type the name that you use to log onto the directory server.
5. In the Runtime Administrator Password box, type the password.
6. Click Log On.
7. In the Name box, type a name for the namespace.
8. In the Description box, type a description of the namespace if required.
9. Click other tabs to set other namespace properties.
10. Click OK.

    The new namespace appears in the directory server and contains a default user called Administrator.

### Tip

- To delete a namespace, select it and click Delete from the Action menu. You can only delete those namespaces that you have access to as an administrator. Deleting a namespace permanently removes it, and the authentication data it contains, from the directory server. If you delete a namespace from a directory server, then the action cannot be undone and there is no means of recovering the data.

  You cannot delete a namespace that is set as default.

### Related Topics

- "Add a Namespace Administrator" (p. 30)
- "Define Regional Settings for Users in a Namespace" (p. 35)
- "Export a Namespace for Remote Users" (p. 37)
- "Log On to a Namespace" (p. 28)
- "Log On to a Namespace as Another User" (p. 29)
- "Provide Summary Information for a Namespace" (p. 30)
- "Set a Default Namespace for a Directory Server" (p. 36)
- "Set Password Properties for Users in a Namespace" (p. 34)
- "Set Signon Properties for Users in a Namespace" (p. 33)
- "Set Up a Namespace: Overview" (p. 26)
- "Transfer Namespace Information Between Directory Servers" (p. 38)
- "Upgrade Namespaces" (p. 40)

## Log On to a Namespace

### Description

To access and modify the contents of a namespace, you must be able to log on to the namespace. Using Access Manager, you can only log on to a namespace if you have a basic signon and belong to a user class that has permissions to view or edit the contents of the namespace.

By default, each namespace contains an administrator user ID called Administrator. This user ID does not have a password and belongs to the root user class. Use this default user ID to initially log on to the namespace.

After you log on to a namespace, you remain logged in for the entire session (until you exit Access Manager).

For more information about creating additional administrator user IDs, see "Add a Namespace Administrator" (p. 30).

### Steps

1. In the Authentication Information window, double-click the Directory Servers folder to open it.
2. Double-click the directory server that contains the namespace you want to access.
3. Select the namespace.
4. In the right pane of the Access Manager window, do the following:
   - In the User ID box, type your user ID.
   - In the Password box, type the corresponding password.
5. Click Log On.

   The contents of the namespace appear in the right pane of the Access Manager window.

### Tip

- If you double-click a namespace, the Cognos Logon dialog box appears and prompts you for a user ID and password. You can also right-click the namespace and click Log On to open the Cognos Logon dialog box.

### Related Topics

- "Add a Namespace" (p. 27)
- "Add a Namespace Administrator" (p. 30)

- "Define Regional Settings for Users in a Namespace" (p. 35)
- "Export a Namespace for Remote Users" (p. 37)
- "Log On to a Namespace as Another User" (p. 29)
- "Provide Summary Information for a Namespace" (p. 30)
- "Set a Default Namespace for a Directory Server" (p. 36)
- "Set Password Properties for Users in a Namespace" (p. 34)
- "Set Signon Properties for Users in a Namespace" (p. 33)
- "Set Up a Namespace: Overview" (p. 26)
- "Transfer Namespace Information Between Directory Servers" (p. 38)
- "Upgrade Namespaces" (p. 40)


## Log On to a Namespace as Another User

### Description

When you are using Access Manager Administration, you often need to log on to a namespace as the administrator. This is usually the easiest way to make changes to a namespace, since the administrator has full access to a namespace. The administrator user ID belongs to the root user class and, by default, does not have a password.

You can also log on to a namespace as any user in the namespace. When you log on as a user other than the administrator, you have that user's access rights. This allows you to check that you have given the user appropriate access permissions.

If the namespace uses basic signons, then you can log on as any user using the Login As command.

If the namespace uses operating system (OS) signons, or both basic and OS signons, then you are automatically logged on to the namespace with your network ID. To access the namespace as another user, use the Login As command to log in using a basic signon. When a namespace uses only OS signons, only the administrator or a member of the root user class can access the namespace with a basic signon.

If you have already logged on to the namespace, you must log off before logging in as another user.

### Steps

1. In the Authentication Information window, double-click the Directory Servers folder.
2. Double-click the directory server that contains the namespace you want to access.
3. Select the namespace.
4. From the Action menu, click Login As.

   The Cognos Logon dialog box appears.
5. In the User ID box, type the user ID you want to log on as.
6. In the Password box, type the corresponding password.
7. Click Log On.

   The contents of the namespace appear in the right pane of the Access Manager Administration window.

### Related Topics


- "Add a Namespace" (p. 27)
- "Add a Namespace Administrator" (p. 30)
- "Define Regional Settings for Users in a Namespace" (p. 35)
- "Export a Namespace for Remote Users" (p. 37)

- "Log On to a Namespace" (p. 28)
- "Provide Summary Information for a Namespace" (p. 30)
- "Set a Default Namespace for a Directory Server" (p. 36)
- "Set Password Properties for Users in a Namespace" (p. 34)
- "Set Signon Properties for Users in a Namespace" (p. 33)
- "Set Up a Namespace: Overview" (p. 26)
- "Transfer Namespace Information Between Directory Servers" (p. 38)
- "Upgrade Namespaces" (p. 40)

## Add a Namespace Administrator

### Description

By default, each namespace contains an administrator user ID called Administrator. This user ID does not have a password and belongs to the root user class. You can use this user ID to set up additional namespace administrators, as well as your authentication data.

To properly set up a namespace administrator, you must provide the administrator with a basic signon, and they must belong to the root user class. It is the root user class that gives the administrator full access privileges to the namespace.

For more information about creating user signons, see "Provide a User With a Signon" (p. 49).

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. Double-click the Users folder to list the contents.
3. Drag the user that you want to add as a namespace administrator to the Root User Class icon.

### Related Topics

- "Add a Namespace" (p. 27)
- "Define Regional Settings for Users in a Namespace" (p. 35)
- "Export a Namespace for Remote Users" (p. 37)
- "Log On to a Namespace" (p. 28)
- "Log On to a Namespace as Another User" (p. 29)
- "Provide Summary Information for a Namespace" (p. 30)
- "Set a Default Namespace for a Directory Server" (p. 36)
- "Set Password Properties for Users in a Namespace" (p. 34)
- "Set Signon Properties for Users in a Namespace" (p. 33)
- "Set Up a Namespace: Overview" (p. 26)
- "Transfer Namespace Information Between Directory Servers" (p. 38)
- "Upgrade Namespaces" (p. 40)

## Provide Summary Information for a Namespace

### Description

You can provide detailed information about each namespace, which may be useful for other administrators or if you are administering a large number of namespaces. This information is optional.

You can add keywords to use with a future version of Access Manager for keyword searches. You can also use the Keywords property in your OLE automation scripts to access and use these keywords.

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. From the Edit menu, click Properties.

   The Namespace Properties dialog box appears.
3. Click the Summary tab.
4. Provide the required summary information.
5. Click OK.

### Related Topics

- "Add a Namespace" (p. 27)
- "Add a Namespace Administrator" (p. 30)
- "Define Regional Settings for Users in a Namespace" (p. 35)
- "Export a Namespace for Remote Users" (p. 37)
- "Log On to a Namespace" (p. 28)
- "Log On to a Namespace as Another User" (p. 29)
- "Set a Default Namespace for a Directory Server" (p. 36)
- "Set Password Properties for Users in a Namespace" (p. 34)
- "Set Signon Properties for Users in a Namespace" (p. 33)
- "Set Up a Namespace: Overview" (p. 26)
- "Transfer Namespace Information Between Directory Servers" (p. 38)
- "Upgrade Namespaces" (p. 40)

## Set Up Anonymous Access to a Namespace

### Description

You can set up anonymous access to a namespace so that users are never prompted for a user ID and password. You can restrict access to a data source by setting user permissions for the anonymous users, as you would for any other user.

Anonymous users are usually granted minimal access privileges, such as access to Public folders. Anonymous users cannot change IDs or passwords for secure resources.

The anonymous user

- must be a member of at least one user class
- can have auto-access
- can exist in the public user class

The administrator accesses the namespace by logging in as the administrator from other Cognos applications.

If you enable anonymous users in a namespace, other Cognos products will not prompt users for a user ID or password.

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).

2. From the Edit menu, click Properties.
3. Click the Settings tab.
4. In the Authentication box, click Use the Following Account for Anonymous Access.
5. Enter the name of the user account you want.
6. Click OK.

### Related Topics

- "Add a User" (p. 48)
- "Assign a User to a User Class" (p. 51)
- "Display the User Classes and Accesses for a User" (p. 53)
- "Provide a User With a Signon" (p. 49)
- "Provide Access to a Data Source or Application Server" (p. 52)
- "Provide Auto-Access for a User" (p. 52)
- "Set Up Guest Access to a Namespace" (p. 32)
- "Set Up Users: Overview" (p. 47)

## Set Up Guest Access to a Namespace

### Description

You can set up guest access to a namespace so that users have the choice of logging in as named users or as unnamed (guest) users. Guest users do not have to provide a user ID and password. They log in as "guest". Setting up guest users in a namespace allows you to set different levels of security for named users and for guest users.

Guest users cannot modify their user preferences. The guest user

- must be a member of at least one user class
- can have auto-access
- can exist in the public user class

If you enable guest users in a namespace, then Cognos products that support guest access will offer users the option of logging in as guests.

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. From the Edit menu, click Properties.
3. Click the Settings tab.
4. In the Authentication box, click Use the Following Account for Guest Access.
5. Enter the name of the user account you want.
6. Click OK.

### Related Topics

- "Add a User" (p. 48)
- "Assign a User to a User Class" (p. 51)
- "Display the User Classes and Accesses for a User" (p. 53)
- "Provide a User With a Signon" (p. 49)
- "Provide Access to a Data Source or Application Server" (p. 52)
- "Provide Auto-Access for a User" (p. 52)

- "Set Up Anonymous Access to a Namespace" (p. 31)
- "Set Up Users: Overview" (p. 47)

## Set Signon Properties for Users in a Namespace

### Description

You can set common signon properties for all the users that are defined within the same namespace. These properties offer an additional level of security.

You can specify

- the type of signons allowed for all the users. Choosing a basic signon means that the users will be prompted to provide a user ID and password for each secure object they access. Basic signons are administered and maintained by Access Manager. Choosing an operating system (OS) signon means that the user can log on using their operating system or network logon information (user ID and password). OS signons are only as secure as the operating system and network. You can also choose to use both, which means that the user will be prompted for a basic signon if the OS signon is not recognized by Access Manager.
- the minimum number of characters that each user's basic signon must have. For example, if you specify a minimum of four characters, each user ID must contain at least four characters.
- whether user IDs are case-sensitive. For example, with this option selected, each user must use the correct capitalization to log on to secure data. If the correct capitalization is not used, the user will not be found and will not be authenticated.
- the maximum number of times that users may attempt to log on to secure data. For users who are denied access to the secure data, you can also specify the length of time before they can try to log on again.

In addition, you can set common password properties for all the users that are defined within the same namespace.

For more information, see "Set Password Properties for Users in a Namespace" (p. 34).

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. From the Edit menu, click Properties.

   The Namespace Properties dialog box appears.
3. Click the Signons tab and do one or more of the following:
   - To specify the type of signon each user must have, under Active Signons click one of the options.
   - To set a maximum number of logon attempts each user has, under Logon Attempts click the Maximum Number of Attempts option and type a value in the box. Otherwise, click the Unlimited option.
   - To set a time interval between failed logon attempts, under Lockout Duration click the Timeout option and type a value in the box. Otherwise, to disallow users who have been denied access from attempting to log on again, click the Unlimited option.
   - To specify the minimum number of characters each user ID must have, under Basic Signon Options type a value in the Minimum User ID Length box.
   - To specify whether all the user IDs must be case-sensitive, under Basic Signon Options select Make User IDs Case-Sensitive.
4. Click OK.

### Related Topics

- "Add a Namespace" (p. 27)
- "Add a Namespace Administrator" (p. 30)
- "Define Regional Settings for Users in a Namespace" (p. 35)
- "Export a Namespace for Remote Users" (p. 37)
- "Log On to a Namespace" (p. 28)
- "Log On to a Namespace as Another User" (p. 29)
- "Provide Summary Information for a Namespace" (p. 30)
- "Set a Default Namespace for a Directory Server" (p. 36)
- "Set Password Properties for Users in a Namespace" (p. 34)
- "Set Up a Namespace: Overview" (p. 26)
- "Transfer Namespace Information Between Directory Servers" (p. 38)
- "Upgrade Namespaces" (p. 40)

## Set Password Properties for Users in a Namespace

### Description

You can specify minimum character lengths, expiration options, and whether passwords must be case-sensitive for all the passwords that you defined within the same namespace. These properties offer an additional level of security.

In addition, you can set common signon properties for all the users that are defined within the same namespace.

For more information, see "Set Signon Properties for Users in a Namespace" (p. 33).

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. From the Edit menu, click Properties.
3. Click the Passwords tab and do one or more of the following:
   - To specify the minimum number of characters each password must have, under Password Options type a value in the Minimum Password Length box.
   - To specify whether all the passwords must be case-sensitive, under Password Options select Make Passwords Case-Sensitive.
   - To set an expiration date for all passwords, under Password Expiry select the Passwords Expire After option, type a value in the box, and then select the period of time. Otherwise, select the Passwords Do Not Expire option.
4. Click OK.

### Related Topics

- "Add a Namespace" (p. 27)
- "Add a Namespace Administrator" (p. 30)
- "Define Regional Settings for Users in a Namespace" (p. 35)
- "Export a Namespace for Remote Users" (p. 37)
- "Log On to a Namespace" (p. 28)
- "Log On to a Namespace as Another User" (p. 29)
- "Provide Summary Information for a Namespace" (p. 30)

- "Set a Default Namespace for a Directory Server" (p. 36)
- "Set Signon Properties for Users in a Namespace" (p. 33)
- "Set Up a Namespace: Overview" (p. 26)
- "Transfer Namespace Information Between Directory Servers" (p. 38)
- "Upgrade Namespaces" (p. 40)

## Define Regional Settings for Users in a Namespace

### Description

You can set the regional settings for all users that are defined within the same namespace.

You can specify

- the time zone associated with the namespace
- whether daylight savings time is in effect for the namespace
- the time format used for the namespace
- the language associated with the namespace
- the geographical location associated with the namespace

### Steps

1. Log on to a namespace.
   For more information, see "Log On to a Namespace" (p. 28).
2. From the Edit menu, click Properties.
3. Click the Regional Settings tab.
4. In the Time Zone box, click the time zone for the namespace.
5. Click the Daylight Savings Time Is In Effect check box if it applies.
6. In the Time Format box, click the time format for the namespace.
7. In the Language box, click the language for the namespace.
8. In the Locale box, click the geographical location for the namespace.
9. Click OK.

### Related Topics

- "Add a Namespace" (p. 27)
- "Add a Namespace Administrator" (p. 30)
- "Export a Namespace for Remote Users" (p. 37)
- "Log On to a Namespace" (p. 28)
- "Log On to a Namespace as Another User" (p. 29)
- "Provide Summary Information for a Namespace" (p. 30)
- "Set a Default Namespace for a Directory Server" (p. 36)
- "Set Password Properties for Users in a Namespace" (p. 34)
- "Set Signon Properties for Users in a Namespace" (p. 33)
- "Set Up a Namespace: Overview" (p. 26)
- "Transfer Namespace Information Between Directory Servers" (p. 38)
- "Upgrade Namespaces" (p. 40)

# Set a Default Namespace for a Directory Server

### Description

Before a user can access a data source, metadata source, or application server, they must configure their Cognos product so that it knows which authentication source to use at runtime. Typically users configure their Cognos product by specifying the authentication source using the Configuration Manager.

Before you can set up a default namespace, you must log on to the directory server where the namespace is located and be authenticated.

If you want Configuration Manager to automatically use a default namespace, you must also set the directory server that contains the namespace as default.

For more information about using Configuration Manager, see "Configure an Authentication Source" (p. 13).

For more information about namespaces and authentication data, see "Set Up An Authentication Source" (p. 21) and "Set Up a Namespace: Overview" (p. 26).

### Steps

1. In the Authentication Information window, double-click the Directory Servers folder.
2. Click the directory server that you want to set as default.
3. From the Action menu, click Set as Default.

   The directory server you selected appears bold, indicating that it has been set as the default.
4. Double-click the directory server.
5. Select the namespace that you want to set as default.
6. Log on to the namespace.
7. From the Action menu, click Set as Default.
8. In the Administrator Access dialog box, type the administrator distinguished name and password.
9. Click Log On.

   The namespace you selected appears bold, indicating that it has been set as the default.

### Related Topics

- "Add a Namespace" (p. 27)
- "Add a Namespace Administrator" (p. 30)
- "Define Regional Settings for Users in a Namespace" (p. 35)
- "Export a Namespace for Remote Users" (p. 37)
- "Log On to a Namespace" (p. 28)
- "Log On to a Namespace as Another User" (p. 29)
- "Provide Summary Information for a Namespace" (p. 30)
- "Set Password Properties for Users in a Namespace" (p. 34)
- "Set Signon Properties for Users in a Namespace" (p. 33)
- "Set Up a Namespace: Overview" (p. 26)
- "Transfer Namespace Information Between Directory Servers" (p. 38)
- "Upgrade Namespaces" (p. 40)

# Export a Namespace for Remote Users

### Description

When you need to create an authentication source for remote users, you can export the data from a namespace in a directory server into a local authentication export file (.lae). You can either replace the data that already exists in an .lae file with the data in the source namespace, or you can merge the data in the source namespace with the data in the .lae file.

For information about namespace merging rules, see "Transfer Namespace Information Between Directory Servers" (p. 38).

If you enabled external user support (p. 41) for a directory server namespace and you export the namespace to an LAE file, you must specify whether to include the users in the export.

When you are finished exporting the namespace to an .lae file, you can send the file to your remote users.

If you do not want to edit the data in a namespace while the namespace is in use, you can export the namespace to an .lae file and make the required changes. Then you can import the modified namespace in the .lae file into the original namespace on the directory server.

For more information, see "Import a Local Authentication Export File into a Namespace" (p. 44).

### Notes

If you merge namespaces, cubes that were built from either the source or the destination namespace may have to be rebuilt.

### Steps

1. Log on to a namespace (p. 28).
2. From the Action menu, click Export To .LAE File.
3. In the Export To LAE file dialog box, select a local authentication export file into which you want to export the namespace.

   If no files are listed, click Add and complete the following steps. Otherwise, continue with step 5.

   - In the Name box, type a name for the new .lae file.
   - In the File Path box, type a name and a file path for the file, or click Browse to locate an existing file.
   - Click OK.
4. In the Options box, do one of the following:
   - To delete data in the namespace before exporting the authentication data, click Empty the Target Namespace.
   - To add the namespace data to the existing data, click Merge Namespaces.
5. If the external user support is enabled for the namespace, specify whether to include users in the export.

   To include users, select the Export users check box.

   To exclude users, clear the Export users check box.
6. In the Log file box, specify the location for your log file.
7. Click Export.

   You can then send that file to your remote users.

### Related Topics

- "Add a Namespace" (p. 27)
- "Add a Namespace Administrator" (p. 30)

- "Define Regional Settings for Users in a Namespace" (p. 35)
- "Log On to a Namespace" (p. 28)
- "Log On to a Namespace as Another User" (p. 29)
- "Provide Summary Information for a Namespace" (p. 30)
- "Set a Default Namespace for a Directory Server" (p. 36)
- "Set Password Properties for Users in a Namespace" (p. 34)
- "Set Signon Properties for Users in a Namespace" (p. 33)
- "Set Up a Namespace: Overview" (p. 26)
- "Transfer Namespace Information Between Directory Servers" (p. 38)
- "Upgrade Namespaces" (p. 40)


## Transfer Namespace Information Between Directory Servers

### Description

To transfer namespace information between directory servers, you must

- set up a working connection to both directory servers
- create a blank local authentication export file (.lae)
- export the namespace from the original directory server to the local authentication export file (.lae)
- import the .lae file into a namespace on the target directory server

When you merge one namespace into another, the precedence of objects and their property settings depends on the namespace to which you give precedence. For example, the source namespace contains A, B, C, the target namespace contains C, D, E, and you give precedence to the target namespace. When the source namespace is merged into the target namespace, the resulting namespace contains

- A (from source)
- B (from source)
- C (from target)
- D (from target)
- E (from target)

### Notes

- You can have more than one namespace in an .lae file by exporting from more than one namespace and choosing to merge namespaces in the Export LAE dialog box.
- If you merge namespaces, cubes that were built from either the source or the destination namespace may have to be rebuilt.

### Steps

1. In the Authentication Information pane, click the Local Authentication Export Files folder.
2. From the Action menu, click Add .LAE File.

   The LAE File Properties dialog box appears.
3. In the Name box, type a name for the local authentication export file.
4. In the File Path box, type the path of the file or click Browse to specify the location where you want to store the file.
5. Click OK.

6. Export the namespace from the original directory server to the blank .lae file.

   For information, see "Export a Namespace for Remote Users" (p. 37).

7. Import the .lae file into the target directory server.

   For information, see "Import a Local Authentication Export File into a Namespace" (p. 44).

### Related Topics

- "Add a Namespace" (p. 27)
- "Add a Namespace Administrator" (p. 30)
- "Define Regional Settings for Users in a Namespace" (p. 35)
- "Export a Namespace for Remote Users" (p. 37)
- "Log On to a Namespace" (p. 28)
- "Log On to a Namespace as Another User" (p. 29)
- "Provide Summary Information for a Namespace" (p. 30)
- "Set a Default Namespace for a Directory Server" (p. 36)
- "Set Password Properties for Users in a Namespace" (p. 34)
- "Set Signon Properties for Users in a Namespace" (p. 33)
- "Set Up a Namespace: Overview" (p. 26)
- "Upgrade Namespaces" (p. 40)

## Identify All Out of Date Namespaces

### Description

When a namespace on a directory server is exported to a local authentication export file (.lae), or an .lae file is imported to a namespace on a directory server, the exported namespace is linked to its source. Both namespaces store creation and modification times.

The Identify All Out of Date Namespaces command compares the creation times of all exported namespaces with the modification time of the source and then identifies namespaces that are out of date. It also identifies namespaces that have been deleted from one authentication source but not from another.

You can also use the Is Namespace Up To Date? command for a namespace on a directory server or for an .lae file. This verifies whether the creation time of the selected namespace is the same as the modification time of the source namespace. If the times are different, then the namespace is out of date.

If a namespace is out of date, you can update it by re-exporting the source namespace.

For more information about exporting a namespace, see "Export a Namespace for Remote Users" (p. 37).

**Note:** For the namespace version 17.0, the external user information is not verified.

### Steps to Identify All Out of Date Namespaces

- From the Tools menu, select Identify all out of date Namespaces.

  A dialog box appears listing any namespaces in an .lae file that have a creation time that is older than the modification time of the source namespace.

### Steps to Verify Up to Date Namespaces

1. Log on to a namespace in a local authentication export file (.lae).

   For more information, see "Log On to a Namespace" (p. 28).

2. From the Action menu, click Is Namespace up to date?

### Related Topics

- "Add a Local Authentication Export File" (p. 44)
- "Import a Local Authentication Export File into a Namespace" (p. 44)
- "Local Authentication Export Files: Overview" (p. 43)

## Upgrade Namespaces

### Description

The structure and properties of a namespace are determined by the schema version of the LDAP directory server that was used to create it. You may have existing namespaces that were created by using older versions of the schema than the current schema version.

You can upgrade your namespace schema to the current version. The additional functionality provided by the current schema version includes improved performance for large deployments of users and user classes, and support for extended or non-ASCII characters in UTF-8 (UNICODE) format in the directory server through Access Manager. This enables you to build applications that are language-independent and universally accessible.

Before you upgrade to the **current** schema version,

- you may have to upgrade your directory server schema

  For information about upgrading your directory server, see Configure the Directory Server for Cognos Products in your installation documentation.

- you must upgrade your namespaces

  To check the namespace version, in Access Manager - Administration, go to the namespace properties, Genaral tab. If the schema version is not at least 15.2, you must upgrade each namespace to version 15.2 before you can upgrade all namespaces to the current version.

If you want your namespaces to be compatible with Series 7.0 and earlier versions of Cognos products, and with Series 7.1 that uses the namespace version 15.2, you must use the **Compatible with Series 7.0 and earlier versions** schema version. For more information, see the installation guide.

During configuration, you can choose to remain at the **Compatible with Series 7.0 and earlier versions** schema version, or you can upgrade to the **current** version. If you decide to upgrade your namespace schema during the configuration process, you upgrade your namespaces to the most **current** version using the Access Manager Administration tool.

**Note:** After you upgrade your namespaces to the current schema version, the namespaces are no longer compatible with Cognos Series 7.0 and earlier versions, and with any product that uses a namespace version 15.2 and lower.

### Steps to Upgrade a Namespace to Schema Version 15.2

1. Log on to the namespace you want to upgrade.

   For more information, see "Log On to a Namespace" (p. 28).

2. From the Action menu, click Upgrade Namespace.

   A message appears stating that you will be automatically logged out before the namespace can be upgraded.

3. Click OK.

   You are logged out and the namespace is upgraded. To access the upgraded namespace, you must log on again.

### Steps to Upgrade All Namespaces to the Current Version

1. Open Access Manager - Administration.
2. In the **Authentication Information** pane, expand the **Directory Servers** or **Local Authentication Export file** folder.

   For information about adding a directory server connection, see "Connect to a Directory Server" (p. 22). For information about adding a Local Authentication Export file connection, see "Add a Local Authentication Export File" (p. 44).
3. Right-click the directory server or LAE file for which you want to upgrade the existing namespaces, and then click **Upgrade all namespaces to current version**.

   A message is displayed warning that upgrading namespaces to the Current schema version makes the namespaces incompatible with Cognos Series 7.0 and earlier product versions.

   If a warning message is displayed stating that not all namespaces are at the 15.2 schema version, you must upgrade each namespace to that version before you can upgrade them to the current schema version.
4. Click **OK**.

### Related Topics

- "Add a Namespace" (p. 27)
- "Add a Namespace Administrator" (p. 30)
- "Define Regional Settings for Users in a Namespace" (p. 35)
- "Export a Namespace for Remote Users" (p. 37)
- "Log On to a Namespace" (p. 28)
- "Log On to a Namespace as Another User" (p. 29)
- "Provide Summary Information for a Namespace" (p. 30)
- "Set a Default Namespace for a Directory Server" (p. 36)
- "Set Password Properties for Users in a Namespace" (p. 34)
- "Set Signon Properties for Users in a Namespace" (p. 33)
- "Set Up a Namespace: Overview" (p. 26)
- "Transfer Namespace Information Between Directory Servers" (p. 38)

## Enable External User Support

### Description

External users are defined in SunONE and Active Directory directory servers and linked to an Access Manager namespace. You must enable external user support before you can link external users (p. 55).

Enable external user support if all users that access the Cognos namespace are defined and maintained in your directory server. After the users are linked to one or more namespaces, the changes made to these users in your directory server are automatically reflected in Access Manager.

Before you enable external user support, we recommend that you back up the directory server data.

After you enable external user support, you add new users only in your directory server, and then link them to your Access Manager namespace.

With external user support enabled, when you delete users from your directory server, they are automatically disabled in the Access Manager namespace. However, you must remove the links to users who are no longer defined in your directory server.

You must have already configured your directory server for external user support by using Configuration Manager. For more information, see the Configuration Manager *User Guide*.

### Steps

1. Start Access Manager - Administration.
2. In the Authentication Information pane, double-click the Directory Servers folder to open it.
3. Click the directory server that contains the namespace you want, and log on to the namespace (p. 28).
4. If the namespace version is 15.2, right-click the directory server and click Upgrade all namespaces to the current version.
5. Right-click the directory server and click Enable External User Support.
6. If you already created a backup of the directory server data, click OK. If not, click Cancel, create a backup, and begin again.
7. Type the runtime administrator distinguished name (DN) and password.
8. Click Log On.

   All the namespaces in the directory server are upgraded to version 17.0, and the external user configuration is permanently enabled.

You can now link external users (p. 55).

### Related Topics

- "Link External Users" (p. 55)

## Enable Audit Logging

### Description

Access Manager supports audit logging of security administration. You can log changes to namespace objects. In this release, only changes to the user class membership can be logged.

You must set up audit logging for one namespace at a time.

Audit logging is supported for directory server namespaces only. LAE namespaces are not auditable.

When you enable audit logging, you specify how and where the namespace changes will be logged.

Before you can enable audit logging, you must

- implement the audit logging API functions
- register the audit logging API library using Access Manager - Registration Wizard.

For more information, see the Access Manager Trusted Services Plug-In *Software Development Kit Guide*.

### Steps

1. Start Access Manager - Administration.
2. Connect to the directory server that stores the namespace you want to audit.
3. Log on to the namespace (p. 28), and right-click it.
4. Click Properties, and then click the Audit logging tab.
5. In the Administrator Access dialog box, type the administrator distinguished name and password, and click Log on.

   **Note:** The Audit logging tab must be active. If the tab is not active, the trusted services plug-in is not registered, or the audit logging service is not included in the plug-in.
6. In the Logging Option box, click Enable.

7. In the On failure box, click Continue.

   This setting specifies that the auditable changes to the namespace are saved when a problem occurs.

8. In the Custom Configuration box, enter custom configuration information required by your audit logging API library.

   For example, for the audit logging API sample provided with Access Manager, type the star (*) character.

9. Click OK.

10. To test audit logging, make a change to any user class in the namespace, and then check whether the logging source previously specified recorded the change.

    **Note:** If you test the sample audit logging plug-in, log off the namespace before you start testing.

### Related Topics

- "Audit User Session Activity" (p. 80)

# Alternate Authentication Sources: Overview

The main source of authentication data used by Access Manager is a namespace on an LDAP directory server. However, you can also use local authentication export files (.lae), which enable single users to access authentication data remotely, even though they are not connected to the same network as the directory server.

### Related Topics

- "Local Authentication Export Files: Overview" (p. 43)
- "Set Up An Authentication Source" (p. 21)

# Local Authentication Export Files: Overview

Local authentication export files (.lae) provide a portable authentication source for single users who want to open user class-protected data remotely, such as a PowerPlay cube. Use .lae files to distribute and manage authentication data. You can

- export a namespace from a directory server to an .lae file
- import an .lae file into a namespace on a directory server

Similar to directory servers, .lae files contain namespaces that store your authentication data. The tasks required to create users, user classes, and add connection information for servers and data sources are the same whether you use a namespace on a directory server or an .lae file.

You can only use .lae files locally on a single computer, not on a network or with multiple users.

You can use .lae files on a computer running Windows or UNIX.

For information about editing the properties of a namespace see "Set Up a Namespace: Overview" (p. 26). For information about editing the authentication data in a namespace, see "Set Up Authentication Data" (p. 47). For information about using .lae files on a computer running UNIX, see the Configuration Manager *User Guide*.

**Note:** An .lae file is not supported as an authentication source for multi-user server deployments.

### Related Topics

- "Alternate Authentication Sources: Overview" (p. 43)
- "Add a Local Authentication Export File" (p. 44)
- "Identify All Out of Date Namespaces" (p. 39)

- "Import a Local Authentication Export File into a Namespace" (p. 44)
- "Alternate Authentication Sources: Overview" (p. 43)

## Add a Local Authentication Export File

### Description

You can create a blank local authentication export file(.lae) and then create namespaces for your authentication data, or you can create an .lae file when you export a namespace from a directory server.

For more information about creating an .lae file from a namespace on a directory server, see "Export a Namespace for Remote Users" (p. 37).

Regardless of how you create the .lae file, you can create, log on to, and maintain namespaces in the .lae file just as you would for a namespace on a directory server.

For more information, see "Set Up a Namespace: Overview" (p. 26). For more information about adding authentication data to the namespace in the .lae file, see "Set Up Authentication Data" (p. 47).

### Steps

1. In the Authentication Information window, select the Local Authentication Export Files folder.
2. From the Action menu, click Add .LAE File.
3. In the Name box, type a name for the file.
4. In the File Path box, do one of the following:
   - Type the path and file name for the new file.
   - To locate the folder in which you want to create the new file, click Browse. The Open dialog box appears. You must type the name of the new file in the File Name box. Click Open to create the file and return to the properties dialog box.
5. Click OK.

   The new file is created in the specified location and added to the Local Authentication Export Files folder.

### Tip

- To add an existing .lae file to Access Manager, specify the file in the Properties dialog box.

### Related Topics

- Identify All Out of Date Namespaces
- Import a Local Authentication Export File into a Namespace
- Local Authentication Export Files: Overview

## Import a Local Authentication Export File into a Namespace

### Description

If you use a local authentication export file (.lae) for the purpose of updating the authentication data in a namespace on a directory server, you can either replace the data that already exists in a namespace on the directory server with the data in the .lae file, or you can merge the data in the .lae file with the data in the namespace.

For information about namespace merging rules, see "Transfer Namespace Information Between Directory Servers" (p. 38).

If you enabled external user support (p. 41), you must specify if you want to include users in the import. For example, users may be manually added to a namespace in an .lae file and then imported into a directory server namespace that is enabled for external user support. If the users are not included in the import, they are not imported.

After you import users, you may need to relink them. To determine which users must be relinked, you can run the "AM_NamespaceReport Utility" (p. 85).

### Steps

1. Log on to a namespace (p. 28).
2. From the Action menu, click Import From .LAE File.
3. In the Import From .LAE File dialog box, select the required file.

   If no files are listed, click Add and complete the following steps. Otherwise, continue with step 5.

   - In the Name box, type a name for the new .lae file.
   - In the File Path box, type a name and a file path for the file, or click Browse to locate an existing file.
   - Click OK. The namespaces that are contained in the file appear in the Namespaces In The File box.
4. Select the namespace that you want to import.
5. In the Options box, do one of the following:
   - To delete data in the target namespace before exporting the authentication data, click Empty the Target Namespace.
   - To add the namespace data to the existing data, click Merge Namespaces.
6. If the external user support is enabled, specify whether to include users in the import.

   To include users, select the Import users check box.

   To exclude users, clear the Import users check box.
7. In the Log file box, specify the location for your log file.
8. Click Import.

### Related Topics

- "Add a Local Authentication Export File" (p. 44)
- "Identify All Out of Date Namespaces" (p. 39)
- "Local Authentication Export Files: Overview" (p. 43)

# Chapter 3: Set Up Authentication Data

Authentication data is the security information that is stored in an authentication source, such as a namespace in a directory server or a namespace in a local authentication export file (.lae). You use Access Manager Administration to define and maintain authentication data, which enables users to access user class-protected data, such as cubes and reports.

Setting up authentication data involves

- creating user classes and assigning users to them
- defining the data sources, metadata, and application servers that users need access to
- giving users access permissions to the required data sources, metadata, and application servers

### Auto-Access

When you set up user access permissions, you can also set up auto-access. Auto-access enables users to access secure cubes, databases, or servers without being prompted multiple times for a user ID or password. Setting up auto-access for a user is useful if the user needs to access multiple data sources on a database or a server, which would require them to provide their logon information many times.

For more information about auto-access, see

- "Set Up Auto-Access for a Database" (p. 62)
- "Set Up Auto-Access for a Transformer Server" (p. 66)
- "Provide Auto-Access for a User" (p. 52)

### Related Topics

- "Set Up a Data Source: Overview" (p. 60)
- "Set Up a Server: Overview" (p. 65)
- "Set Up User Classes: Overview" (p. 56)
- "Set Up Users: Overview" (p. 47)
- "Search for Authentication Data" (p. 67)
- "Sort Authentication Data" (p. 68)

## Set Up Users: Overview

A user is an object that represents an individual in an organization who uses secure data.

When you set up users, you

- add users
- define basic signons, OS signons, or both for each user
- assign the users to user classes
- assign access to data sources and servers
- assign auto-access to data sources and servers
- define regional settings for users
- determine user access to Upfront

After you set up user classes and users, you can assign the users to any number of user classes.

For more information about setting up user classes, see "Set Up User Classes: Overview" (p. 56).

### Users Assigned to Multiple User Classes

Users who belong to more than one user class may be prompted to select a user class when they log on. Some Cognos applications, such as Impromptu Web Reports, require a single user class. Users who belong to more than one user class are prompted to select a user class each time they log on. Other applications, such as PowerPlay and Upfront, allow the user to log on with all the permissions of the user classes they belong to. This is referred to as a union of user classes.

For example, a user belongs to user class 1 and user class 2. If the user is using Impromptu Web Reports, they are asked to select either user class 1 or user class 2 when they log on. If using Upfront or PowerPlay, users are not prompted for a user class. Instead, they log on with the combined permissions of user class 1 and user class 2.

### Notes

An OS signon relies on the security of the operating system. Basic signons are controlled by Access Manager.

### Related Topics

- "Add a User" (p. 48)
- "Assign a User to a User Class" (p. 51)
- "Display the User Classes and Accesses for a User" (p. 53)
- "Provide a User With a Signon" (p. 49)
- "Provide Access to a Data Source or Application Server" (p. 52)
- "Provide Auto-Access for a User" (p. 52)
- "Set Up Anonymous Access to a Namespace" (p. 31)
- "Set Up Guest Access to a Namespace" (p. 32)
- "Set Up An Authentication Source" (p. 21)
- "Add a User Class" (p. 56)
- "Define Regional Settings for Users of Web Products" (p. 54)
- "Define User Access to Upfront" (p. 54)
- "Display Users Belonging to a User Class" (p. 60)
- "Set Up a Public User Class" (p. 57)
- "Set Up User Classes: Overview" (p. 56)
- "Set User Class Access Times" (p. 58)
- "Set User Class Permissions" (p. 59)

## Add a User

### Description

For each individual who must access secure data, you must create a user with Access Manager Administration, assign the user to one or more user classes, and specify a signon for the user. Access to the secured data is defined for each user class in the client application. To open an authenticated application or data source, a user must belong to at least one user class.

For more information about assigning users to user classes, see "Assign a User to a User Class" (p. 51).

The user name only identifies the individual in Access Manager. The name used to authenticate the user in other applications depends on the basic or OS signon.

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. Double-click the namespace to list the contents.
3. Select the Users folder.
4. From the Action menu, click Add User.
5. Type a name in the Name box.

   This name will only appear in Access Manager Administration.
6. If you want, type a description of the user in the Description box.
7. Click other tabs to set other user properties. Click Related Topics for information about other namespace properties.
8. Click OK.

### Tips

- To delete a user, select it and click Delete from the Action menu.

  You cannot delete yourself when you are logged on to a namespace.
- To add a folder to further group users, select the Users folder, click Add Folder from the Action menu, and then type the name of the folder in the Name box. If you want, you can add a description of the folder in the Description box. You can then drag users into this folder.
- To disable a user's account select the User account is disabled check box on the General tab of the User Properties property sheet. The user will not be able to log on by any authentication method.

### Related Topics

- "Assign a User to a User Class" (p. 51)
- "Display the User Classes and Accesses for a User" (p. 53)
- "Provide a User With a Signon" (p. 49)
- "Provide Access to a Data Source or Application Server" (p. 52)
- "Provide Auto-Access for a User" (p. 52)
- "Set Up Anonymous Access to a Namespace" (p. 31)
- "Set Up Guest Access to a Namespace" (p. 32)
- "Set Up Users: Overview" (p. 47)

## Provide a User With a Signon

### Description

There are two types of signons you can set up for a user:

- a basic signon
- an operating system (OS) signon

A basic signon consists of a user ID and password, both of which are defined and maintained using Access Manager Administration. Before a user with a basic signon can access secure data, they must enter a valid user ID and password during authentication.

Alternatively, you can set up an OS signon if you want Access Manager to recognize a user's network ID for purposes of authentication. An OS signon uses the security of the operating system to give users access to secure data without an additional password.

If a user has both a basic signon and an OS signon, which Access Manager uses is determined by the namespace settings. For more information, see "Set Signon Properties for Users in a Namespace" (p. 33).

### Steps to Set Up a Basic Signon

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. Double-click the namespace to list the contents.
3. Double-click the Users folder to open it.
4. Select the user.
5. From the Edit menu, click Properties.
6. Click the User Signons tab.
7. Select the Basic Signon check box.
8. Type a name in the User ID box.

   The user must provide this user ID during authentication.
9. Type a password in the Password box.
10. Type the password again in the Verify Password box.
11. Click OK.

### Tip

- You can change a user's password by typing the new password in the Password and Verify Password boxes.
- Enhanced password management options are available. You can force a user to change their password at next logon, specify whether a user can change their password and permit a user's password to never expire.

### Steps to Set Up an OS Signon

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. Double-click the namespace to list the contents.
3. Double-click the Users folder to open it.
4. Select the user.
5. From the Edit menu, click Properties.
6. Click the User Signons tab.
7. In the OS Signons box, click the Add button.

   A dialog box appears prompting you for information about the domain and user ID.
8. Type the signon information using one of the following formats:
   - domain\userid (for Windows products)
   - userid (for Windows client products that are not on a domain, and for UNIX products)
9. Click OK.

### Related Topics

- "Add a User" (p. 48)
- "Assign a User to a User Class" (p. 51)
- "Display the User Classes and Accesses for a User" (p. 53)
- "Provide Access to a Data Source or Application Server" (p. 52)

- "Provide Auto-Access for a User" (p. 52)
- "Set Up Anonymous Access to a Namespace" (p. 31)
- "Set Up Guest Access to a Namespace" (p. 32)
- "Set Up Users: Overview" (p. 47)
- "Set Signon Properties for Users in a Namespace" (p. 33)
- "External Signons" (p. 15)

## Assign a User to a User Class

### Description

Assigning a user to a user class gives that user all the permissions of the user class. To open an authenticated application or data source, a user must belong to at least one user class.

If a user is a member of more than one user class, during authentication they may be prompted to select the user class that they want to use for the current session.

For more information about users assigned to multiple user class, see "Set Up Users: Overview" (p. 47).

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. Double-click the namespace to list the contents.
3. Double-click the Users folder to find the user.
4. Select the user.
5. From the Edit menu, click Properties.
6. Click the Memberships tab.

   The user classes defined in the namespace appear in a hierarchical structure with the root user class at the top. To display the user classes, click the plus sign (+) next to each user class.
7. Select the user class that you want the user to belong to.

   A check mark appears in the box next to each user class that the user belongs to.
8. Click OK.

### Tip

- To remove a user from a user class, clear the check box next to each user class.
- You can also assign a user to a user class by dragging the user icon from the Users folder to the user class.

### Related Topics

- "Add a User" (p. 48)
- "Display the User Classes and Accesses for a User" (p. 53)
- "Provide a User With a Signon" (p. 49)
- "Provide Access to a Data Source or Application Server" (p. 52)
- "Provide Auto-Access for a User" (p. 52)
- "Set Up Anonymous Access to a Namespace" (p. 31)
- "Set Up Guest Access to a Namespace" (p. 32)
- "Set Up Users: Overview" (p. 47)

## Provide Access to a Data Source or Application Server

### Description

You provide access to a data source or application server to allow a user to connect to that source. A data source can be a database, a metadata object, or a cube. An application server can be a PowerPlay or Transformer server.

You can also provide users with auto-access to databases and Transformer servers.

For more information, see "Provide Auto-Access for a User" (p. 52).

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. Double-click the namespace to list the contents.
3. Double-click the Users folder to open it.
4. Select a user.
5. From the Edit menu, click Properties.
6. Click the Access tab.
7. Select the data sources or application servers that you want the user to have access to.
8. Click OK.

### Related Topics

- "Add a User" (p. 48)
- "Assign a User to a User Class" (p. 51)
- "Display the User Classes and Accesses for a User" (p. 53)
- "Provide a User With a Signon" (p. 49)
- "Provide Auto-Access for a User" (p. 52)
- "Set Up Anonymous Access to a Namespace" (p. 31)
- "Set Up Guest Access to a Namespace" (p. 32)
- "Set Up Users: Overview" (p. 47)

## Provide Auto-Access for a User

### Description

You set up auto-access for users to allow them to access secure cubes, servers, or databases without being prompted for a user ID or password. Before you set up auto-access for a user, signons for servers or databases must already exist.

You can provide auto-access for a database or a Transformer server.

For more information about setting auto-access for a database, see "Set Up Auto-Access for a Database" (p. 62). For more information about setting auto-access for a Transformer server, see "Set Up Auto-Access for a Transformer Server" (p. 66).

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. Double-click the namespace to list the contents.
3. Double-click the Users folder to open it.
4. Select the user that you want to set up auto access permissions for.

5. From the Edit menu, click Properties.
6. Click the Access tab.
7. Select the data source or server.
8. In the Signon box, click the Set button. Not all data sources have signons.
9. Select the signon you want to apply to the user.
10. Click OK.

    The auto-access signon appears beside the data source or server.
11. Click OK.

### Related Topics

- "Add a User" (p. 48)
- "Assign a User to a User Class" (p. 51)
- "Display the User Classes and Accesses for a User" (p. 53)
- "Provide a User With a Signon" (p. 49)
- "Provide Access to a Data Source or Application Server" (p. 52)
- "Set Up Anonymous Access to a Namespace" (p. 31)
- "Set Up Guest Access to a Namespace" (p. 32)
- "Set Up Users: Overview" (p. 47)

## Display the User Classes and Accesses for a User

### Description

Access Manager Administration shows the user classes and accesses assigned to a user in the right pane of the Access Manager Administration window. Each icon represents a reference to a user class to which the user belongs or a data source or server for which the user has access.

For more information about assigning users to a user class, see "Assign a User to a User Class" (p. 51).

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. Double-click the namespace to list the contents.
3. Double-click the Users folder to open it.
4. Select the user.

   The user classes and accesses assigned to the user appear in the right pane of the Access Manager Administration window.

### Tip

- To view or edit the properties of a reference, select it from the right pane of the Access Manager Administration window and click Properties from the Edit menu.

### Related Topics

- "Add a User" (p. 48)
- "Assign a User to a User Class" (p. 51)
- "Provide a User With a Signon" (p. 49)
- "Provide Access to a Data Source or Application Server" (p. 52)
- "Provide Auto-Access for a User" (p. 52)

- "Set Up Anonymous Access to a Namespace" (p. 31)
- "Set Up Guest Access to a Namespace" (p. 32)
- "Set Up Users: Overview" (p. 47)

## Define Regional Settings for Users of Web Products

### Description

You define regional settings to determine the time, language, and locale settings that appear for users of Cognos Web products. If you don't specify regional settings for a user, Access Manager uses the ones that are defined for the namespace.

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. Double-click the namespace to list the contents.
3. Double-click the Users folder to open it.
4. Click the user you want.
5. From the Edit menu, click Properties.
6. Click the Regional Settings tab.
7. In the Time Zone box, select the user's time zone.
8. Click the Daylight Savings Time Is In Effect check box if it applies.
9. In the Time Format box, click the format in which the time appears.
10. In the Language box, click the user's language.
11. In the Locale box, click the user's location to show the correct regional formats for numbers, dates, and so on.
12. Click OK.

### Related Topics

- "Add a User Class" (p. 56)
- "Define User Access to Upfront" (p. 54)
- "Display Users Belonging to a User Class" (p. 60)
- "Set Up a Public User Class" (p. 57)
- "Set Up User Classes: Overview" (p. 56)
- "Set User Class Access Times" (p. 58)
- "Set User Class Permissions" (p. 59)

## Define User Access to Upfront

### Description

You define access privileges for Upfront users in Access Manager Administration. When you add a user in Access Manager, you determine whether or not they have a personal NewsBox in Upfront.

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. Double-click the namespace to list the contents.

3. Double-click the Users folder to open it.
4. Click the user you want.
5. From the Edit menu, click Properties.
6. Click the Upfront tab.
7. Click the Create Personal NewsBox check box to create a personal NewsBox in Upfront.
8. Click OK.

### Related Topics

- "Add a User Class" (p. 56)
- "Define Regional Settings for Users of Web Products" (p. 54)
- "Display Users Belonging to a User Class" (p. 60)
- "Set Up a Public User Class" (p. 57)
- "Set Up User Classes: Overview" (p. 56)
- "Set User Class Access Times" (p. 58)
- "Set User Class Permissions" (p. 59)

## Link External Users

If you enabled external user support (p. 41), you can link users defined in a directory server to your Access Manager namespace. When you link users, you associate them with an external user distinguished name (DN).

If you link users to more than one namespace, and then change some user attributes, the changes are reflected automatically in each associated namespace.

After the users are linked to the Access Manager namespace, you must ensure that they have a signon and are members of at least one user class. If you are using a basic signon strategy, you must add a basic signon for each user that is linked to your namespace (p. 49).

### Steps

1. Log on to a namespace (p. 28).
2. Right-click the Users folder or any child folder and click Link User.
3. If you want to browse for external users, click the Browse tab.

   **Tip:** To select or clear all users, use the check box next to the top node. To select or clear all users in a folder, select the check box next to the folder.
4. If you want to search for external users, click the Search tab, and select the users you want.
   - In the User Name or LDAP Filter box, type a user name or an LDAP search filter.
     If you type a user name, the search uses the root of the external users as the start DN and the scope of the search is subtree.
     **Tip:** To see a list of all external users, leave this field blank.
   - In the Search By box, select User Name or LDAP Search Filter depending on what you typed in the User Name or LDAP Filter field.
   - If you selected LDAP Search Filter, specify the StartDN and Search Scope.
     StartDN specifies the start of the search in an LDAP directory. Search Scope limits the search to the specified portion of the root DN. The Base option includes the start DN only, the One level option includes the entries under the start DN excluding the start DN, and the Subtree option includes the entries under the start DN including the start DN.
   - Click Search.
     The list of external users appears in the Search Results window.
   - Select the users you want to link.
     **Tip:** To select all entries, click Select All.

5. Click Link Users.
   - If you selected more than one entry in the Search Results box, the selected users are linked to the namespace.
     A message appears that specifies whether the users were successfully linked, and how many users were linked.
   - If you selected only one entry, the Properties dialog box appears for the selected user. Click OK to link the selected user to the namespace.
6. If you want to link a user to a different external DN, in the user's Properties dialog box, on the Genaral tab, click Relink.

   **Tip:** The external user DN appears in red when it must be relinked.

### Related Topics

- "Enable External User Support" (p. 41)

# Set Up User Classes: Overview

A user class is an object that represents a category of users who have similar functions in an organization. Cognos products that use Access Manager to control user access, such as Impromptu Web Reports, Cognos Query, PowerPlay or Transformer, determine which users have access to information depending on the user class to which they are assigned. Each member of a user class has the same access privileges, and users can be assigned to multiple user classes.

For more information about users assigned to multiple user classes, see "Set Up Users: Overview" (p. 47).

A recommended way to organize user classes is according to how your business is structured. You can also build multiple structures because users can belong to more than one user class. In these structures, a user might be a member of both Senior Managers (by function) and National Offices (by region). For example, you may want to set up user classes by function (Vice Presidents, Senior Managers, and Regional Managers), and by region (All Regions, National Offices, District Offices, Plants).

### Related Topics

- "Add a User Class" (p. 56)
- "Define Regional Settings for Users of Web Products" (p. 54)
- "Define User Access to Upfront" (p. 54)
- "Display Users Belonging to a User Class" (p. 60)
- "Set Up a Public User Class" (p. 57)
- "Set User Class Access Times" (p. 58)
- "Set User Class Permissions" (p. 59)
- "Set Up Authentication Data" (p. 47)

## Add a User Class

### Description

When you add a user class, you enable administrators of client applications to restrict access to data or provide auto-access to data sources based on these user classes. Each user class that you create is contained within the root user class.

### Notes

You cannot have a space as the first character in the name of a user class.

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. Double-click the namespace to list the contents.
3. Select the Root User Class icon or any of its children.
4. From the Action menu, click Add User Class.
5. Type a name for the user class in the Name box.

   User class names can only appear once in a namespace.
6. If you want, type a description of the user class in the Description box.
7. Click OK.

For information on setting user class access and permissions, see "Set User Class Access Times" (p. 58) and "Set User Class Permissions" (p. 59).

### Tips

- To nest a user class in another user class, select the user class and then click Add User Class from the Action menu. This enables you to create subsets of users within user classes.
- To remove a user class, select it and click Delete from the Action menu.

### Related Topics

- "Define Regional Settings for Users of Web Products" (p. 54)
- "Define User Access to Upfront" (p. 54)
- "Display Users Belonging to a User Class" (p. 60)
- "Set Up a Public User Class" (p. 57)
- "Set Up User Classes: Overview" (p. 56)
- "Set User Class Access Times" (p. 58)
- "Set User Class Permissions" (p. 59)
- "Set Up Authentication Data" (p. 47)

## Set Up a Public User Class

### Description

A public user class is a user class to which all users in a namespace automatically belong. When you add new users to a namespace, if there is a public user class, they automatically belong to it. Existing users also belong to the public user class.

This user class is carried forward into other Cognos products that recognize public user classes. You do not have to name the public user class "public"; you can name it anything you want.

You can associate users with other user classes, but they always remain members of the public user class. You can assign properties and access to the public user class, as you would for any other user class.

By default, a namespace does not have a public user class associated with it.

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. From the Edit menu, click Properties.
3. Click the Settings tab.
4. In the Public User Class box, click Use the Following Class For All Users.

5. Enter the name of the user class.
6. Click OK.

### Related Topics

- "Add a User Class" (p. 56)
- "Define Regional Settings for Users of Web Products" (p. 54)
- "Define User Access to Upfront" (p. 54)
- "Display Users Belonging to a User Class" (p. 60)
- "Set Up User Classes: Overview" (p. 56)
- "Set User Class Access Times" (p. 58)
- "Set User Class Permissions" (p. 59)

## Set User Class Access Times

### Description

You set access times for user classes when you want to limit user access to secure data to days and to time periods on those days. This means that members of a user class will only be granted access during the time specified for that user class. This restriction applies to accessing Access Manager - Administration as well as to applications accessing user class secured data.

The time restriction is verified against the user's computer and is applied when the user first accesses the data. Users who continue to access data after their time restriction expires will not be automatically logged off.

User class access periods are for a single day and can not pass through midnight. For example, you cannot set a start time of 8:00 P.M. and an end time of 3:00 A.M.

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. Double-click the namespace to list the contents.
3. Double-click the Root User Class icon to list the user classes.
4. Select the user class.
5. From the Edit menu, click Properties.
6. Click the General tab.
7. In the Access Days and Time box, select when the selected user class will have access.
8. In the Time Period From and To boxes, set the time period when the user class will have access.

   The time period is verified against the user's computer.

   To set the time periods, select the hour or minute and type the value or use the arrows at the side of the box to change the value. To change the AM or PM notation, select AM or PM and use the arrows at the side of the box.
9. Click OK.

### Related Topics

- "Add a User Class" (p. 56)
- "Define Regional Settings for Users of Web Products" (p. 54)
- "Define User Access to Upfront" (p. 54)
- "Display Users Belonging to a User Class" (p. 60)

- "Set Up a Public User Class" (p. 57)
- "Set Up User Classes: Overview" (p. 56)
- "Set User Class Permissions" (p. 59)

## Set User Class Permissions

### Description

User class permissions specify what members of that user class can do using Access Manager Administration. You can allow members of a user class to view users, user classes, data sources, and servers, or create and delete users and user classes, and add data sources and servers.

The permissions specified in Access Manager do not determine the access permissions that members of the user class will have when using a client application. Those permissions are defined in the application. For example, permissions within Access Manager Administration determine whether that user, as a member of a user class, can view, create, or delete users and user classes and view, add, or remove connections to data sources and servers within Access Manager Administration. They do not specify whether that user can view a specific dimension while viewing a cube in PowerPlay. Permissions for viewing a cube must be specified in Transformer when the cube is created.

Access Manager allows you to limit the view of users when you set up delegated administration for your user classes. Delegated administrators can see the names of only those users and user classes who belong to the user classes they administer. For example, consider a European user class with children user classes of Italy, France, and Germany. You can delegate administration to the European sales managers so that they only have access to members of the Europe user class and all of its children. The European sales managers could only administer the user classes and users from the Europe, Italy, France, and Germany user classes.

For more information about setting permissions in the client application, see the online help for that application.

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. Double-click the namespace to list the contents.
3. Double-click the Root User Class icon to find the user class.
4. Select the user class.
5. From the Edit menu, click Properties.
6. Click the Permissions tab.

   To delegate administration to members of the user class in the entire namespace, select the **Members can view all users and/or user classes** check box.

   To delegate administration to members of the user class only in its own user class and its children, clear the **Members can view all users and/or user classes** check box.
7. Set the permissions for the selected user class.
8. Click OK.

### Related Topics

- "Add a User Class" (p. 56)
- "Define Regional Settings for Users of Web Products" (p. 54)
- "Define User Access to Upfront" (p. 54)
- "Display Users Belonging to a User Class" (p. 60)
- "Set Up a Public User Class" (p. 57)

- "Set Up User Classes: Overview" (p. 56)
- "Set User Class Access Times" (p. 58)

## Display Users Belonging to a User Class

### Description

Access Manager shows the users that belong to each user class in the right pane of Access Manager Administration window. Each icon represents a reference to a user.

For more information, see "Assign a User to a User Class" (p. 51).

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. Double-click the namespace to list the contents.
3. Double-click the Root User Class icon to list the user classes.
4. Select the user class.

   Each user appears as a User Reference in the right pane of the Access Manager Administration window.

### Tips

- To view the user classes to which a user belongs, select the user. The user classes appear in the right pane of the Access Manager Administration window.
- To view or edit the properties of a user, select the user from the right pane of the Access Manager Administration window and click Properties from the Edit menu.

### Related Topics

- "Add a User Class" (p. 56)
- "Define Regional Settings for Users of Web Products" (p. 54)
- "Define User Access to Upfront" (p. 54)
- "Set Up a Public User Class" (p. 57)
- "Set Up User Classes: Overview" (p. 56)
- "Set User Class Access Times" (p. 58)
- "Set User Class Permissions" (p. 59)

# Set Up a Data Source: Overview

Data sources represent network locations where data is stored. A data source can be a database, a PowerPlay cube, or a cube stored in a database. Access Manager only stores connection information for each data source, not the contents of the data source.

Access Manager also enables you to provide auto-access to password-protected databases for users. With an auto-access signon, users can access a database without being prompted for a database user ID or password.

### Related Topics

- "Add a Cube" (p. 63)
- "Add a Cube Stored in a Database" (p. 64)
- "Add a Database" (p. 61)
- "Add an OLAP Server Database" (p. 62)

- "Add Metadata" (p. 65)
- "Set Up Auto-Access for a Database" (p. 62)
- "Set Up Authentication Data" (p. 47)

## Add a Database

### Description

Before users can access a database, you need to define the database in Access Manager and then give the required users access privileges to that database. Defining a database involves

- referencing the database
- defining the connection string so that the client application can connect to the database

You can create auto-access signons for databases.

For more information, see "Set Up Auto-Access for a Database" (p. 62).

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. Double-click the namespace to list the contents.
3. Select the Data Sources folder and from the Action menu, click Add Database.

   The Database Properties dialog box appears.
4. On the General tab, in the Name box, type a name for the database.
5. Click the Connection tab.
6. In the Database Type drop-down box, select the type of database you are defining.
7. To specify the connection string, click Edit.

   The Edit button only appears for databases that you can edit in this fashion. If the Edit button does not appear for the type of database you select, go to step 9.

   The Database Definition dialog box appears.
8. Enter the required connection information and click OK.
9. Click OK again to close the property sheet.

### Tip

- To add a folder to further group databases, select the Data Sources folder, click Add Folder from the Action menu, and then add or move databases to the new folder.
- To delete a database, select the database, and click Delete from the Action menu.

### Related Topics

- "Add a Cube" (p. 63)
- "Add a Cube Stored in a Database" (p. 64)
- "Add an OLAP Server Database" (p. 62)
- "Add Metadata" (p. 65)
- "Set Up a Data Source: Overview" (p. 60)
- "Set Up Auto-Access for a Database" (p. 62)

## Add an OLAP Server Database

### Description

You can use Access Manager Administration to set up access to an OLAP server database.

For a complete list of supported database versions, see the PowerPlay Readme help.

Before users can access a database, you need to define the database in Access Manager and then give the required users access privileges to that database. Defining a database involves

- referencing the database
- defining the connection string so that the client application can connect to the database

For more information, see the OLAP Server Connection Guide.

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. Double-click the namespace to list the contents.
3. Select the Data Sources folder and click Add Database from the Action menu.

   The Database Properties dialog box appears.
4. On the General tab, in the Name box, type a name for the database.
5. Click the Connection tab.
6. In the Database Type box, select the type of database you are defining.
7. Click Edit to specify the connection string.

   The Edit button only appears if you can edit the database definition. If the Edit button does not appear for the type of database you select, go to step 9.
8. In the Database Definition dialog box, enter the required connection information and click OK.
9. Click OK again to close the property sheet.

### Related Topics

- "Add a Cube" (p. 63)
- "Add a Cube Stored in a Database" (p. 64)
- "Add a Database" (p. 61)
- "Add Metadata" (p. 65)
- "Set Up a Data Source: Overview" (p. 60)
- "Set Up Auto-Access for a Database" (p. 62)

## Set Up Auto-Access for a Database

### Description

To set auto-access to a database that is directly accessed or that stores a cube, you must create a signon for the database using a user ID and password. After the signon is created, it can be applied to any user to provide them auto-access to the database.

For more information, see "Provide Auto-Access for a User" (p. 52).

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).

2. Double-click the namespace to list the contents.
3. Double-click the Data Sources folder to open it.

   If no databases appear, you will have to add one.

   For more information about adding databases, see "Add a Database" (p. 61).
4. Double-click the database that you want to create an auto-access signon for.
5. Select the Signons folder.
6. From the Action menu, click Add Database Signon.
7. Type a user ID in the User ID box.

   This is the user ID required to access the database.
8. Type the database password in the Password and Verify Password boxes.

   **Note:** The Password and Verify Password boxes will not appear, if the trusted services database signon password plug-in is registered.
9. If you want, type a description in the Description box.
10. Click OK.

### Tip

- If the password for the database has changed you can change the password stored in Access Manager by typing the password in the Password and Verify Password boxes.
- To delete a database reference, select the database, and click Delete from the Action menu.

### Related Topics

- "Add a Cube" (p. 63)
- "Add a Cube Stored in a Database" (p. 64)
- "Add a Database" (p. 61)
- "Add an OLAP Server Database" (p. 62)
- "Add Metadata" (p. 65)
- "Set Up a Data Source: Overview" (p. 60)

## Add a Cube

### Description

You add a cube to a namespace so you can control access to the cube using Access Manager.

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. Double-click the namespace to list the contents.
3. Select the Data Sources folder.
4. From the Action menu, click Add Local Cube.
5. Type a name for the cube in the Name box.
6. Type the cube password in the Password and Verify Password boxes.

   **Note:** The Password and Verify Password boxes will not appear, if the trusted services cube password plug-in is registered.
7. If you want, type a description of the cube in the Description box.
8. Click OK.

### Tip

- If the password for the cube has changed, you can change the password stored in Access Manager by typing the current password in the Current Password box, and then typing the new password in the Password and Verify Password boxes.
- To delete a cube reference, select the cube, and click Delete from the Action menu.

### Related Topics

- "Add a Cube Stored in a Database" (p. 64)
- "Add a Database" (p. 61)
- "Add an OLAP Server Database" (p. 62)
- "Add Metadata" (p. 65)
- "Set Up a Data Source: Overview" (p. 60)
- "Set Up Auto-Access for a Database" (p. 62)

## Add a Cube Stored in a Database

### Description

Adding a cube that is stored in a database creates a reference to the database and the cube so that you can control access using Access Manager.

You can create auto-access signons for the database in which the cube is stored.

For more information, see "Set Up Auto-Access for a Database" (p. 62).

### Steps

1. Add a database.

   For more information, see "Add a Database" (p. 61).
2. Double-click the database to open it.
3. Select the Cubes folder.
4. From the Action menu, click Add In-Database Cube.
5. Type a name for the cube in the Name box.
6. If you want, type a description of the cube in the Description box.
7. In the Connection String box, click Edit to set the connect string for the database that the cube is stored in.
8. Enter the connection information in the PowerPlay Connect dialog box.
9. Click OK to save the connection information.
10. Click OK.

### Tip

- To delete a reference to a cube stored in a database, select the cube, and click Delete from the Action menu.

### Related Topics

- "Add a Cube" (p. 63)
- "Add a Database" (p. 61)
- "Add an OLAP Server Database" (p. 62)
- "Add Metadata" (p. 65)
- "Set Up a Data Source: Overview" (p. 60)
- "Set Up Auto-Access for a Database" (p. 62)

## Add Metadata

### Description

Before you give users access privileges to a metadata source, you must define the source in Access Manager.

Architect defines what types of metadata can be used, for example, Architect Model, ERwin Model, or Informatica Model. Ensure that you specify a valid metadata type because Access Manager does not validate this parameter.

For more information about metadata sources (types), see your Architect documentation.

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. Double-click the namespace to list the contents.
3. Select the Data Sources folder and click Add Metadata from the Action menu.
4. On the General tab, type a name for the metadata in the Name box.
5. In the Description box, type a description of the metadata if required.
6. In the Additional Information area, select the type of metadata to add from the Metadata Type list.
7. Click the Details tab.

   A dialog box appears.

   Use this box to specify a metadata source to make available to Architect.
8. Click OK.

   The metadata object appears in the Data Sources folder.

### Related Topics

- "Add a Cube" (p. 63)
- "Add a Cube Stored in a Database" (p. 64)
- "Add a Database" (p. 61)
- "Add an OLAP Server Database" (p. 62)
- "Set Up a Data Source: Overview" (p. 60)
- "Set Up Auto-Access for a Database" (p. 62)

# Set Up a Server: Overview

Servers represent server locations on a network. Access Manager stores the connection information for PowerPlay and Transformer servers so that you can control user access to them.

You can also use Access Manager to provide auto-access to Transformer servers for users. With an auto-access signon, users can access the server without being prompted for a server user ID or password.

### Related Topics

- "Add a PowerPlay Server" (p. 67)
- "Add a Transformer Server" (p. 66)
- "Set Up Auto-Access for a Transformer Server" (p. 66)
- "Set Up Authentication Data" (p. 47)

## Add a Transformer Server

### Description

When you add a Transformer server, you set up a reference to a server that users can access using Transformer.

You can also create auto-access signons for Transformer servers.

For more information, see "Set Up Auto-Access for a Transformer Server" (p. 66).

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. Double-click the namespace to list the contents.
3. Select the Application Servers folder.
4. From the Action menu, click Add Transformer Server.
5. Type the name of the server in the Name box.

   The name must be the name by which the server is identified on the network.
6. If you want, type a description of the server in the Description box.
7. Click OK.

   The server appears in the Application Servers folder.

### Related Topics

- "Add a PowerPlay Server" (p. 67)
- "Set Up a Server: Overview" (p. 65)
- "Set Up Auto-Access for a Transformer Server" (p. 66)

## Set Up Auto-Access for a Transformer Server

### Description

Auto-access to a Transformer server requires the user ID needed to access the server. After a signon is created, it can be applied to any user.

For more information about assigning auto-access to a user, see "Provide Auto-Access for a User" (p. 52).

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. Double-click the namespace to list the contents.
3. Double-click the Application Servers folder to open it.

   If no Transformer servers appear, you will have to add one.

   For more information about adding application servers, see "Add a Transformer Server" (p. 66).
4. Select the Transformer server.
5. From the Action menu, click Add Transformer Signon.
6. Type a user ID in the User ID box.

   This is the user ID required to access the server.
7. Type the server password in the Password and Verify Password boxes.

8. If you want, type a description in the Description box.
9. Click OK.

### Tip

- If the password for the server has changed, you can change the password stored in Access Manager by typing the password in the Password box and then in the Verify Password box.
- To delete a reference to a Transformer server, select the Transformer server, and click Delete from the Action menu.

### Related Topics

- "Add a PowerPlay Server" (p. 67)
- "Add a Transformer Server" (p. 66)
- "Set Up a Server: Overview" (p. 65)

## Add a PowerPlay Server

### Description

When you add a PowerPlay server, you set up a reference to a server that users can access using a client application, such as PowerPlay, PowerPlay Web, or PowerPlay for Excel.

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. Double-click the namespace to list the contents.
3. Select the Application Servers folder.
4. From the Action menu, click Add PowerPlay Server.
5. Type the name of the server in the Host box.

   The name must be the name by which the server is identified on the network.
6. Type the port number to access the server in the Port box.
7. Type a value for the maximum length of time Access Manager will try to connect to the server in the Timeout box.
8. If you want, type a description of the server in the Description box.
9. Click OK.

   The server appears in the Application Servers folder.

### Related Topics

- "Add a Transformer Server" (p. 66)
- "Set Up a Server: Overview" (p. 65)
- "Set Up Auto-Access for a Transformer Server" (p. 66)

## Search for Authentication Data

### Description

You can search a namespace for any type of object that is contained in the namespace. For example, you can search for users, user classes, server hosts, databases, cubes, and signons. The search results return objects that meet the search criteria, the type of objects they are, and the location in the namespace where the objects can be found.

You can search only one namespace at a time.

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. From the Edit menu, click Find.
3. Type the name or partial name of the object you want to find in the Name box.
4. Choose the type of object you want to find from the Type box.
5. Click Find Now.

   Any objects found, along with their type and location in the namespace, appear in the dialog box. You can click the object to open its Properties dialog box.

### Related Topics

- "Sort Authentication Data" (p. 68)
- "Set Up Authentication Data" (p. 47)

## Sort Authentication Data

### Description

Authentication data (listed in a folder in the left pane of the Access Manager window) is listed alphabetically or numerically from A to Z or 0 to 9. However, you can sort data in the right pane of the Access Manager window by name or type. For example, you can sort application servers by type so that all Transformer servers are listed together and all PowerPlay servers are listed together.

### Steps

1. Log on to a namespace.

   For more information, see "Log On to a Namespace" (p. 28).
2. Double-click the namespace to list the contents.
3. Select the folder that contains the data you want to sort.
4. In the right pane of the Access Manager window, click the Name or Type title bar to sort the columns alphabetically.

   An arrow appears in the title bar indicating how the data is sorted: by which column and in which direction.

### Related Topics

- "Search for Authentication Data" (p. 67)
- "Set Up Authentication Data" (p. 47)

# Chapter 4: Set Up Security Across Applications

When you use Cognos applications to create reports and cubes from your organization's database information, you can secure them by applying user classes, created and managed in Access Manager Administration. The user classes restrict user access to specific information. For example, a cube may contain financial information that you do not want all your employees to see. By applying a user class to information, such as dimensions in a cube, you can ensure that only members of that user class view that information.

When users access a cube, or a report that has user class security applied to it, they must be identified by Access Manager before they can access the information. Depending on the user classes to which they belong and how those user classes are applied, Access Manager grants the user access only to the information that you want them to see. For example, in a PowerPlay cube, user classes can be applied to specific dimensions, and only members of that user class will be able to view those dimensions.

Setting up authentication data in Access Manager Administration is only one part of providing secure user access to information. You must also set up your user's access to the authentication data so they can use it.

### Configure Access to Authentication Data

As the administrator of authentication data, there may be times when you want to test how the user classes you defined in Access Manager Administration perform in a Cognos application. Before you can test your user classes, you must use Configuration Manager the same way a typical user does to configure your Cognos application to access the required authentication data.

For more information about Configuration Manager, see "Configure an Authentication Source" (p. 13).

After you define and test your authentication data, and apply the user classes in other applications, your users must configure their computers to access the required authentication data from the authentication source.

To configure access to authentication data, users must have

- Configuration Manager installed with their Cognos applications. Configuration Manager is installed by default.
- connections to the required data sources (for example, the directory server on which a namespace is located, or a local authentication export file (.lae) for a remote user).
- directory server connection information, such as the host, port, and base distinguished name (DN).
- ticket service information for Web-based access.

### Use Local Authentication Cache Files

When a user connects to a secure data source, such as a cube or a report, Access Manager can automatically create a local authentication cache file (.lac) and stores it on the user's computer. As a result, if the user tries to connect to the same data source while they are not connected to the network, Access Manager uses the.lac file, instead of the original authentication source.

Access Manager automatically creates .lac files for those Cognos applications that can use Access Manager, such as Transformer, PowerPlay, and PowerPlay Web. Upfront does not support .lac files, nor do Architect, Cognos Query, or Impromptu Web Reports.

### Notes

- Local authentication cache files (.lac) are intended for use with client tools, such as PowerPlay client, which only need read access to authentication data. Using .lac files on Cognos servers is not supported as they may cause performance and concurrency problems. Local authentication cache files (.lac) can be disabled with the Configuration Manager.

### Related Topics


- "Access Manager and Architect" (p. 70)
- "Access Manager and Cognos Query" (p. 76)
- "Access Manager and Impromptu" (p. 74)
- "Access Manager and Impromptu Web Reports" (p. 75)
- "Access Manager and PowerPlay" (p. 72)
- "Access Manager and PowerPlay Enterprise Server" (p. 73)
- "Access Manager and Transformer" (p. 71)
- "Access Manager and Upfront" (p. 76)
- "Access Manager and Cognos Visualizer" (p. 77)
- "Access Manager and NoticeCast" (p. 78)
- "Ticket Services" (p. 78)


## Access Manager and Architect

Architect is a metadata management tool that provides a single administration point for metadata that supports all your Cognos reporting and analytical tools. Architect modelers use Architect to build a common set of business-oriented metadata so that users can build queries, reports, and cubes.

Model security in Architect is based on user classes that you create and maintain in Access Manager Administration.

Architect modelers can control which parts of the model are accessible to the members of a user class, whether they are using the model in Architect, or as authors in Impromptu, Cognos Query or Transformer.

You can set permissions for each user class that

- define which objects are visible to the members of the user class, both within Architect and from other Cognos products
- identify allowable activities of report authors and query designers who work with the model in Impromptu and Cognos Query
- set runtime execution limits and restrict the query activities to help maximize system resources, and to minimize network and database performance issues

If you want to allow Architect modelers to create Architect models, import metadata sources, and change passwords, you must give them permission within Access Manager Administration. (User Class Properties dialog box, Permissions tab)

### Use the Windows Common Logon Server

When users install the Windows Common Logon server that comes with Architect, they can use the same authentication data to access multiple data sources.

For more information about installing the server, see the installation and configuration guide for your product.

### Notes

- If you import user classes from an Impromptu catalog and there is a conflict between the user classes in the Impromptu catalog and the user classes in the Architect model, only unique (new and non-conflicting) user classes are imported from the Impromptu catalog.
- Only users who are members of the root user class can import security information into an Architect model.
- Architect supports the union of user classes. Users who belong to more than one user class are logged on with all the privileges of all the user classes to which they belong.

For more information about using security in Architect, see the Architect online help.

### Related Topics

- "Access Manager and Cognos Query" (p. 76)
- "Access Manager and Impromptu" (p. 74)
- "Access Manager and Impromptu Web Reports" (p. 75)
- "Access Manager and PowerPlay" (p. 72)
- "Access Manager and PowerPlay Enterprise Server" (p. 73)
- "Access Manager and Transformer" (p. 71)
- "Access Manager and Upfront" (p. 76)
- "Access Manager and Cognos Visualizer" (p. 77)
- "Access Manager and NoticeCast" (p. 78)
- "Ticket Services" (p. 78)
- "Set Up Security Across Applications" (p. 69)

## Access Manager and Transformer

Transformer is used to create multidimensional cubes from database information. Users then access the cube in PowerPlay to view and analyze their corporate data. Transformer administrators can apply the user classes you create in Access Manager Administration to the cubes they create. The user classes identify which users have access to which portions of data in the cube.

For information about applying user classes to a cube, see the Transformer online help.

Users who access a secure cube must also be able to access the authentication source specified for that particular cube. The most common source for authentication data is in a namespace on an LDAP directory server. If there is no namespace specified in the Transformer model, the user class information is verified against the default namespace specified in Configuration Manager. If there is no default namespace specified in Configuration Manager, user class information is verified against the default namespace specified in the directory server.

If users of the secure cube cannot access the authentication data, for example, because they are not connected to the network, you must convert the data to a local authentication export file (.lae) and copy the file to the user's computer.

Transformer does not support the union of user classes. Users who belong to more than one user class must select a user class each time they access secure data.

### Access a Cube in a Database

Access Manager also stores information for auto-access to cubes that are contained within other databases. The database may have security and the cube may have user class security. You can use Access Manager Administration to manage and combine the user class and database connection information by specifying signon information for the database. As a result, the user doesn't have to provide a user ID and password for the database when they access the cube.

For more information, see "Set Up Auto-Access for a Database" (p. 62).

### Apply Auto-Access to Cubes

Instead of using Transformer to store signon information, such as database user IDs, passwords, and connection parameters in a cube (.mdc file), you can use Access Manager to store signon information in a namespace. Storing signon information in a namespace facilitates centralized administration of signon information.

If both a namespace and Transformer contain signon information for the same cube, the information in the namespace takes precedence. Also, if a user is configured to use a namespace on the directory server, Transformer automatically reads the auto-access information specified in the namespace.

For information about applying auto-access in Transformer, see the Transformer online help.

### Apply User Class Views in Transformer

You can further define what data a user has access to by creating user class views and assigning user classes to them. For example, the Great Outdoors Company distributes a cube that contains Order Date, Product Line, and Region dimensions. The cube contains user class views that permit members of the Europe, North America, and Far East user classes to view data that only applies to their region.

In Transformer you can apply a dimension view and user classes to a cube to create a cube with a custom view. This is similar to user class views because you create a cube that only a specific user class can access. However, it is more efficient to use user class views because you can apply multiple views to one cube and therefore greatly reduce the number of files that you distribute. Also, cubes with user class views are optimized for auto-partitioning.

For information about applying user class views in Transformer, see the Transformer online help.

### Related Topics


- "Access Manager and Architect" (p. 70)
- "Access Manager and Cognos Query" (p. 76)
- "Access Manager and Impromptu" (p. 74)
- "Access Manager and Impromptu Web Reports" (p. 75)
- "Access Manager and PowerPlay" (p. 72)
- "Access Manager and PowerPlay Enterprise Server" (p. 73)
- "Access Manager and Upfront" (p. 76)
- "Access Manager and Cognos Visualizer" (p. 77)
- "Access Manager and NoticeCast" (p. 78)
- "Ticket Services" (p. 78)
- "Set Up Security Across Applications" (p. 69)


## Access Manager and PowerPlay

PowerPlay is used to view and analyze data in a multidimensional cube that was created in Transformer. When a Transformer administrator creates a cube, the administrator can apply user classes that restrict user access to dimensions of the cube. When a user accesses the cube using PowerPlay, the user can only see the dimensions that the user class, of which the user is a member, has been given access.

PowerPlay supports the union of user classes. Users who belong to more than one user class are logged on with all the privileges of all the user classes to which they belong.

For more information about applying user class security to a cube, see "Access Manager and Transformer" (p. 71).

### Use the Windows Common Logon Server

When users install the Windows Common Logon server that comes with PowerPlay, they can use the same authentication data to access multiple data sources.

For more information about installing the server, see the installation and configuration guide for your product.

### Create Administrative Macros to Facilitate User Access

To facilitate user access to cubes, you can set up administrative macros that automatically provide PowerPlay with the authentication data the user needs to access the cube. By default, when a user tries to open a cube, PowerPlay determines if you have set up macros to automate the process. If it does not find any macros, it prompts the user for a user ID and password.

For more information about administrative macros, see the PowerPlay Macro help.

### Access Manager and PowerPlay Connect

The PowerPlay Connect utility is used by PowerPlay users or administrators to create or modify .mdc pointer files that store information about server and database connections. You can use PowerPlay Connect to define access to cubes stored in Oracle, Sybase, MS SQL Server, Informix, or DB2 databases. You can also use PowerPlay Connect to define access to Hyperion, DB 2, Oracle Express, and MS SQL Server OLAP servers.

Access Manager provides PowerPlay Connect with connection information that users need to create .mdc pointer files. If the currently configured namespace contains server and database connection information, PowerPlay Connect reads the information and shows it in a browse list. As a result, users can select, rather than enter the appropriate connection information.

For more information, see the PowerPlay Connect online help.

### Related Topics


- "Access Manager and Architect" (p. 70)
- "Access Manager and Cognos Query" (p. 76)
- "Access Manager and Impromptu" (p. 74)
- "Access Manager and Impromptu Web Reports" (p. 75)
- "Access Manager and PowerPlay Enterprise Server" (p. 73)
- "Access Manager and Transformer" (p. 71)
- "Access Manager and Upfront" (p. 76)
- "Access Manager and Cognos Visualizer" (p. 77)
- "Access Manager and NoticeCast" (p. 78)
- "Set Up Security Across Applications" (p. 69)


## Access Manager and PowerPlay Enterprise Server

You use PowerPlay Enterprise Server with a Web browser to view cubes that are stored on the PowerPlay Enterprise Server. Anyone can access the server or Web site simply by referencing a cube; however, Transformer administrators can apply user class security or user class views to the cubes they create. As a result, when a user accesses a cube, the user can only see the dimensions that the user class or user class view, of which the user is a member, has been given access. The Transformer administrator can also apply auto-access to password-protected cubes, servers, and databases.

To be able to deploy secure cubes on the server, the administrator must have access to a directory server namespace and must use a version of Transformer that can apply user class views to a cube.

PowerPlay Enterprise Server supports the union of user classes. Users who belong to more than one user class are logged on with all the privileges of all the user classes to which they belong.

For more information about applying user class security to cubes, see "Access Manager and Transformer" (p. 71). For more information about applying security to cubes, see the Transformer online help.

### Deploy Secure Cubes Using the PowerPlay Enterprise Server

When the administrator adds a secure cube to the PowerPlay Enterprise Server, they can specify to the server the authentication source that is associated with the cube and any logon information the user needs to provide, such as user ID and password, user class name, or database user ID and password. If they don't specify an authentication source, Access Manager reads the authentication source specified in the cube.

For more information, see the PowerPlay Enterprise Server Administration help.

### Publish to Upfront

To publish cubes and reports from the PowerPlay Enterprise Server Administration tool to Upfront, you must secure the tool using Access Manager. You cannot use the server password security method to publish to Upfront.

For more information, see the PowerPlay *Enterprise Server* Guide.

### Ticket Services

The ticket service of the Access Manager Server issues tickets to control user access to reports and cubes. Multiple Cognos applications can use the same authentication data during a single session.

For more information, see "Ticket Services" (p. 78).

### Related Topics


- "Access Manager and Architect" (p. 70)
- "Access Manager and Cognos Query" (p. 76)
- "Access Manager and Impromptu" (p. 74)
- "Access Manager and Impromptu Web Reports" (p. 75)
- "Access Manager and PowerPlay" (p. 72)
- "Access Manager and Transformer" (p. 71)
- "Access Manager and Upfront" (p. 76)
- "Access Manager and Cognos Visualizer" (p. 77)
- "Access Manager and NoticeCast" (p. 78)
- "Ticket Services" (p. 78)
- "Set Up Security Across Applications" (p. 69)


## Access Manager and Impromptu

Use Impromptu to create reports. Impromptu performs queries in structured query language (SQL) against a database to retrieve information for a report. An Impromptu administrator creates a catalog that contains the metadata (columns and tables) used to create reports. The catalog provides a business-oriented view of the database.

Impromptu administrators apply the user classes you create in Access Manager to the catalogs they create. The user classes identify which users have access to which portions of data in the catalog.

Impromptu administrators can specify a namespace for Access Manager to check every time an Impromptu user opens the catalog. If the user is not listed in the namespace, Impromptu denies access.

If the administrator did not specify a namespace, but the Impromptu user has Access Manager set up on their computer, Impromptu checks the default namespace instead. If the user is not listed in the default namespace, they can still log on using catalog security. Users can also use Access Manager to add their operating system user name and password to the namespace so that they can automatically log on to the catalog.

Impromptu does not support the union of user classes. Users who belong to more than one user class must select a user class each time they access secure data.

For information about applying user classes to a catalog, see the Impromptu online help.

### Use the Windows Common Logon Server

When users install the Windows Common Logon server that comes with Impromptu, they can use the same authentication data to access multiple data sources.

For more information about installing the server, see the installation and configuration guide for your product.

### Related Topics

- "Access Manager and Architect" (p. 70)
- "Access Manager and Cognos Query" (p. 76)
- "Access Manager and Impromptu Web Reports" (p. 75)
- "Access Manager and PowerPlay" (p. 72)
- "Access Manager and PowerPlay Enterprise Server" (p. 73)
- "Access Manager and Transformer" (p. 71)
- "Access Manager and Upfront" (p. 76)
- "Access Manager and Cognos Visualizer" (p. 77)
- "Access Manager and NoticeCast" (p. 78)
- "Ticket Services" (p. 78)
- "Set Up Security Across Applications" (p. 69)

## Access Manager and Impromptu Web Reports

Impromptu Web Reports is used with a Web browser to view Impromptu reports that are stored on a server. When a report author creates a report in Impromptu, they can apply security to the report by applying user profiles. The report administrator can add additional security to the report in Impromptu Web Reports by applying user classes. User classes identify which users have access to which reports and report folders, whereas user profiles identify which users have access to which portions of report data.

The report administrator creates user classes in Impromptu Web Reports by generating them from Impromptu user profiles.

Impromptu Web Reports does not support the union of user classes. Users who belong to more than one user class must select a user class each time they access secure data.

For more information, see the Report Administrator's Guide for Impromptu Web Reports.

### Ticket Services

The ticket service of the Access Manager Server issues tickets to control user access to reports and cubes. Multiple Cognos applications can use the same authentication data during a single session.

For more information, see "Ticket Services" (p. 78).

### Related Topics

- "Access Manager and Architect" (p. 70)
- "Access Manager and Cognos Query" (p. 76)

- "Access Manager and Impromptu" (p. 74)
- "Access Manager and PowerPlay" (p. 72)
- "Access Manager and PowerPlay Enterprise Server" (p. 73)
- "Access Manager and Transformer" (p. 71)
- "Access Manager and Upfront" (p. 76)
- "Access Manager and Cognos Visualizer" (p. 77)
- "Access Manager and NoticeCast" (p. 78)
- "Ticket Services" (p. 78)
- "Set Up Security Across Applications" (p. 69)


## Access Manager and Cognos Query

Use Cognos Query to create queries of business data. Users open foundation queries in Cognos Upfront.

You define security settings for Cognos Query in Access Manager Administration by setting up users and user classes.

Cognos Query supports the union of user classes. Users who belong to more than one user class are logged on with all the privileges of all the user classes to which they belong.

For information about using Cognos Query, see the Cognos Query online help.

### Related Topics


- "Access Manager and Architect" (p. 70)
- "Access Manager and Impromptu" (p. 74)
- "Access Manager and Impromptu Web Reports" (p. 75)
- "Access Manager and PowerPlay" (p. 72)
- "Access Manager and PowerPlay Enterprise Server" (p. 73)
- "Access Manager and Transformer" (p. 71)
- "Access Manager and Upfront" (p. 76)
- "Access Manager and Cognos Visualizer" (p. 77)
- "Access Manager and NoticeCast" (p. 78)
- "Ticket Services" (p. 78)
- "Set Up Security Across Applications" (p. 69)


## Access Manager and Upfront

Use Cognos Upfront with PowerPlay Web and Cognos Query to organize and share business information. PowerPlay Web, Cognos Query, and Architect users publish reports and queries to Upfront, as NewsIndex entries.

You define security settings for Upfront in Access Manager Administration by setting up users and user classes. Each Upfront user must belong to at least one user class. Upfront NewsIndex administrators then apply the user classes to NewsIndex entries to control access to NewsBoxes and NewsIndex entries.

Upfront users can view their user ID and the user classes they belong to, from within Upfront.

If you want Upfront users to be able to change their own passwords and personal settings within Upfront, you must give them permission to do so in Access Manager Administration. (User Class Properties dialog, Permissions tab) They can only change the settings that are stored in Access Manager.

Upfront supports the union of user classes. Users who belong to more than one user class are logged on with all the privileges of all the user classes to which they belong.

For information about using Upfront, see the Upfront online help.

### Related Topics


- "Access Manager and Architect" (p. 70)
- "Access Manager and Cognos Query" (p. 76)
- "Access Manager and Impromptu" (p. 74)
- "Access Manager and Impromptu Web Reports" (p. 75)
- "Access Manager and PowerPlay" (p. 72)
- "Access Manager and PowerPlay Enterprise Server" (p. 73)
- "Access Manager and Transformer" (p. 71)
- "Access Manager and Cognos Visualizer" (p. 77)
- "Access Manager and NoticeCast" (p. 78)
- "Ticket Services" (p. 78)
- "Set Up Security Across Applications" (p. 69)


## Access Manager and Cognos Visualizer

Cognos Visualizer creates visualizations that represent business data graphically in three dimensions. You can view several metrics in a visualization that originates from different data sources, and users can interact with this data.

Visualizations can reference secure data sources such as cubes or databases. When a user opens a visualization that refers to a secure data source, they are prompted for authentication data. Without proper authentication, the visualization will open, but the panel, axis, or filter that refers to the secure data source appears blank.

You do not secure Visualization files (.viz) directly. You secure the database or cube that the Visualization file references. You can secure the data source using Access Manager Administration. Because Visualization files (.viz) are designed to be widely distributed, users must also have access to the authentication source. If many users will access the secured files, we recommend that you use a directory server namespace.

Cognos Visualizer supports the union of user classes. Users who belong to more than one user class are logged on with all the privileges of all the user classes to which they belong.

To use Access Manager with Cognos Visualizer, you must upgrade your directory server.

For more information, see the installation and configuration guide for your product.

### Related Topics


- "Access Manager and Architect" (p. 70)
- "Access Manager and Cognos Query" (p. 76)
- "Access Manager and Impromptu" (p. 74)
- "Access Manager and Impromptu Web Reports" (p. 75)
- "Access Manager and PowerPlay" (p. 72)
- "Access Manager and PowerPlay Enterprise Server" (p. 73)
- "Access Manager and Transformer" (p. 71)
- "Access Manager and Upfront" (p. 76)
- "Access Manager and NoticeCast" (p. 78)
- "Ticket Services" (p. 78)
- "Set Up Security Across Applications" (p. 69)

## Access Manager and NoticeCast

NoticeCast enables users to detect and manage time-critical events in their business applications. Users apply rules and threshold values to their data to alert key individuals when those rules and thresholds are true. Notification may be by email to wired or wireless devices.

Access permission for each NoticeCast user is controlled by their membership in the user classes defined in Access Manager.

### Related Topics


- "Access Manager and Architect" (p. 70)
- "Access Manager and Cognos Query" (p. 76)
- "Access Manager and Impromptu" (p. 74)
- "Access Manager and Impromptu Web Reports" (p. 75)
- "Access Manager and PowerPlay" (p. 72)
- "Access Manager and PowerPlay Enterprise Server" (p. 73)
- "Access Manager and Transformer" (p. 71)
- "Access Manager and Upfront" (p. 76)
- "Access Manager and Cognos Visualizer" (p. 77)
- "Ticket Services" (p. 78)
- "Set Up Security Across Applications" (p. 69)


## Ticket Services

### Description

You have the option to increase the reliability of Access Manager by configuring multiple ticket services. If multiple ticket services are configured, a failover mechanism automatically switches to a secondary ticket service when no response is detected from the primary ticket service. You can also balance the load between the ticket services to improve performance.

The ticket service is part of Access Manager Server. The Access Manager Server ticket service issues tickets to control user access to reports and cubes. Multiple Cognos applications can use the same authentication data during a single session. As a result, users trying to access multiple cubes on a server only have to provide a single signon. They do not need to provide a user ID and password every time they try to access a secure data source. For example, a user provides a user ID and password to log on to a PowerPlay cube that is stored on the server. Then the user drills through to a report in Impromptu Web Reports. At this point, the authentication data passes from PowerPlay Enterprise Server to Impromptu Web Reports via a ticket.

The ticket service controls user access to a report or cube for one session.

You can store ticket service information in a local authentication export file (.lae).

For information about installing a ticket service, see the installation and configuration guide for your product.

### Steps

1. In the Authentication Information pane, click the Directory Servers folder.
2. From the Action menu, click Add Connection.

   The Directory Server Properties dialog box appears.
3. On the General tab, in the Host box, type the name or IP address of the server where the directory server is installed.

4. In the Port box, type the port the directory server uses.

   By default, the port is 389. The directory server assigns this port to LDAP servers. If you have more than one server on a computer, the port name distinguishes between the two servers.

5. In the Timeout box, type the maximum amount of time (in seconds) the user has to establish a connection to the directory server.

6. In the Base Distinguished Name (DN) box, type the DN for the root of the directory according to the LDAP standard.

   This DN is the name you typed in the Directory Suffix box when you installed the SunONE Directory Server (for example, o=Cognos, c=CA). If you did not install the directory server, contact the administrator for the required DN.

7. Click the Runtime Credentials tab.

   The Administrator Access dialog box appears.

8. In the Runtime Administrator Distinguished Name (DN) box, type the name that you use to log onto the directory server.

9. In the Runtime Administrator Password box, type the password.

10. Click Log On.

11. Click the Ticket Services tab.

    **Note**: If you used Configuration Manager to configure one or more ticket services, the entries in the Ticket Service connections list should appear as the ticket services configured using Configuration Manager.

    To connect to additional ticket services proceed to step 12. If you are satisfied with the ticket services configured, skip to step 13 to ensure ticket service connections have been set up properly.

12. Click Add. In the Prompt box, type the name or the IP address of the server where the ticket service is installed and the port.

    **Tip**: The host can be entered by name or IP address. The port you specify must be the same as the one specified in Configuration Manager. The default port number is 9010.

13. For each ticket service in the ticket service connections list, select the ticket service and click Test.

    If the connection is unsuccessful, an error message appears. Ensure that you have the correct connection information.

    **Tip**: Ticket service entries should be in the 'host:port' format.

14. Click OK.

### Notes

- Every computer that will access the ticket serviceticket service must be able to reach the ticket service computer. If you cannot ping the ticket service computer from each computer that needs to access it, you must register the ticket service computer name in a domain name system (DNS) server, or refer to it by IP address.
- If you configure the directory server to use the host name of a ticket service that resides on UNIX, ensure that the server can communicate using the selected host name. Otherwise, use the IP address of the UNIX server or edit the /etc/hosts file so that it contains the correct naming resolution.
- The entries in the ticket service connections list should not be rearranged at runtime. If you decide to change the order of your ticket service connections, you must restart your Upfront services or you may experience authentication problems.

### Related Topics


- "Access Manager and Architect" (p. 70)
- "Access Manager and Cognos Query" (p. 76)
- "Access Manager and Impromptu" (p. 74)
- "Access Manager and Impromptu Web Reports" (p. 75)
- "Access Manager and PowerPlay" (p. 72)
- "Access Manager and PowerPlay Enterprise Server" (p. 73)
- "Access Manager and Transformer" (p. 71)
- "Access Manager and Upfront" (p. 76)
- "Access Manager and Cognos Visualizer" (p. 77)
- "Access Manager and NoticeCast" (p. 78)
- "Set Up Security Across Applications" (p. 69)
- "Audit User Session Activity" (p. 80)


# Audit User Session Activity

### Description

You can optionally enable auditing of session information by using the ticket service of Access Manager Server. This provides a log file containing historic information about successful logins, logouts, and session (ticket) expiry. For information on enabling this feature, see the Configuration Manager *User Guide*.

## Convert Log Files

When event logging is enabled, session logs are created. The logs are in a non-readable format so that run-time performance is not significantly impacted when enabling ticket service event logging. You must use the conversion utility, TSLogProcessor, to convert the non-readable log files to text files.

### Steps

1. Start a command prompt session.
2. Change directory to *installation location*\bin.
3. Type **TSLogProcessor** and the required parameters.

   For example,
   TSLogProcessor -h myhost -p 1465 -r "o=cognos, c=ca" -D "cn=Directory Manager" -w admin1234 -f "X:\Program Files\Cognos\cern\bin\logs\ts-901020021016.log" -n mynamespace

   The parameters are listed in the following table.

| Parameter | Description |
|---|---|
| -? | Help information. |
| -h | Name of the directory server host. |
| -p | Port number of the directory server. |
| -r | Root distinguished name. |
| -D | Bind name for the directory server. |
| -w | Bind password for the bind name. |

| Parameter | Description |
|---|---|
| -f | Path to log file. |
| -n | Specify a namespace. Optional parameter.<br>If a namespace is specified, only the entries for that namespace are returned. If no namespace is specified, all entries in the log file are returned. |
| -x | Format the file in XML format. Optional parameter. |
| -S | SSL is enabled. |
| -C | The path of the SSL certificate database. |

### Analyze Converted Log Files

After the log files are converted to a readable format, you can analyze the data to assess ticket service usage. The log file contains header information regarding ticket service properties such as host, port, and base DN. All subsequent log entries contain information regarding events requested of the ticket service.

An entry in the log file may be as follows:

```
[Mon Nov 04 09:46:39 2002] from:142.88.98.219
ticket:10364211933Ngqb8QiOo515jSSchUA action:access details:ns=MyNamespace
user=John Doe status:success
```

| Parameter | Description |
|---|---|
| [Date/Time] | A timestamp of when a ticket service event occurred. |
| from: <IP_address> | The IP address of the server that requested an action. |
| action: [ logon \| check \| access \| logout \| expiry ] | The action requested by the ticket service. Five possible actions can be requested:<br>• **logon** indicates a request for the creation of a ticket.<br>• **check** indicates a request to check the contents of a ticket.<br>• **access** indicates a request to access the ticket.<br>• **logout** indicates a request to terminate the ticket.<br>• **expiry** indicates that the ticket duration has expired, and the ticket will be terminated. |
| details: <list of details> | Specifies namespace and user name. |
| status: [ success \| fail ] | Identifies the success or failure of a requested action. |

### Related Topics

- "Ticket Services" (p. 78)
- "Enable Audit Logging" (p. 42)

# Frequently Asked Questions and Troubleshooting

## Why can't I log on as a user?

Check that your user ID and password are correct, and ensure that you are assigned to at least one user class.

## Why can't I delete a user?

If a namespace is enabled for anonymous access, you cannot delete the anonymous user from the namespace.

If a namespace is enabled for guest access, you cannot delete the guest user from the namespace.

You cannot delete the user whose credentials you are using for the current session.

## Why can't I delete a user class?

If a namespace is enabled for a public user class, you cannot delete the public user class from the namespace.

You cannot delete the root user class.

You cannot delete the user classes to which you belong or modify the properties for those user classes.

## Why can't I open a secured resource after merging namespaces?

A secured resource such as a cube, report, or foundation query, stores unique key values about the users and user classes it is associated with.

If you merge namespaces and one namespace contains either a new secured resource or a new list of users, you must re-associate the resource with the list of users in the target namespace. You must also re-associate a target namespace that contains identical resource names or user names.

To re-associate the secure resource, you must regenerate it.

For more information about merging namespaces, see "Transfer Namespace Information Between Directory Servers" (p. 38).

## When does the cut command behave like copy command?

When you select all the objects in the right pane of Access Manager Administration for a user, and then click the Cut command in the Edit menu or from the toolbar, the Cut command behaves like the Copy command. For example, after you cut database cube objects for a user, then select another user and click the Paste command, the objects that you selected for the previous user are copied from the clipboard into the right pane of the current user.

# Appendix A: AM_NamespaceReport Utility

### Description

Run the AM_NamespaceReport command line utility to create an XML report that lists all users or user classes in a namespace.

### Discussion

You can use the AM_NamespaceReport command line utility with any version of a namespace. Any user with a basic signon can log on. However, only users and user classes for which you have show privileges appear in the report.

If the report is the users type with the filter of the all type, the following information is returned: name, first name, last name, description, email, phone number, basic signons, and OS signons. For the namespace version 17.0, external user DN is also returned.

If the report is userclasses type with the filter of the all type, the following information is returned: user class name, names of children user classes, names of member users, and access permissions.

The XML schema for both types of report output is located in the *Cognos_installation*/cer4/accman/AM_NamespaceReport_users|AM_NamespaceReport_userclasses.xsd directory.

### Parameters

| Parameter | Description |
|---|---|
| -h | Specifies the computer name of the directory server.<br>default: localhost |
| -p | Specifies the port number of the directory server.<br>default: 389 |
| -r | Specifies the base DN of the directory server.<br>default: o=cognos, c=ca |
| -s | Specifies that SSL is enabled.<br>This parameter is optional. |
| -C | Specifies the location of the cert7.db file.<br>This parameter is required only if SSL is enabled. |
| -n | Specifies the name of the namespace for reporting.<br>default: default namespace |
| -D | Specifies the basic signon to use for namespace authentication.<br>This parameter is mandatory. |
| -w | Specifies the basic signon password.<br>This parameter is mandatory. |
| -t | Specifies the type of report. The report types users and userclasses are supported.<br>default: users |

| | |
|---|---|
| -f | Specifies a filter type for a report.<br>For the users report type, the following filter types are supported:<br>• all<br>Returns all user information; this is the default filter.<br>• userclasses<br>Returns only information about the users' user class membership.<br>• brokenlinks<br>Returns only the names of users whose DNs are broken. This filter is used only with the namespace version 17.0.<br>• lockedout<br>Returns only the names of users whose accounts are locked.<br>• disabled<br>Returns only the names of users whose accounts are disabled.<br>For the userclasses report type, the following filter types are supported:<br>• all<br>Returns all user class information; this is the default filter.<br>• users<br>Returns only the names of the member users.<br>• userclasses<br>Returns only information about the children user classes. |
| -o | Indicates the file to which output is written.<br>This parameter is mandatory. |

### Example

To report all users in a namespace, type the following:

```
D:\Cognos\cer4\bin>AM_NamespaceReport –n default –D Administrator –w "" -t
users -f all –o all_users.xml
```

Here is a sample output of the users report type:

```
<?xml version="1.0" encoding="UTF-8"?>
<NamespaceReport xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="D:\Cognos\cer4\accman\AM_NamespaceReport.xsd"
host="localhost" port="389" baseDN="o=Cognos,c=ca" ns="Default"
user="Administrator" type="users" filter="all">
    <User name="Sam Carter" first_name="Sam" last_name="Carter"
email="sam.carter@cognos.com" phone="(123)456-7890"
externalUserDN="uid=scarter,ou=people,o=cognos,c=ca">
       <BasicSignon>scarter</BasicSignon>
       <OSSignon>domain/scarter</OSSignon>
       <Description>Employee id: 12345</Description>
    </User>
    <User name="Ted Morris" first_name="Ted" last_name="Morris"
email="ted.morris@cognos.com" phone="(123)456-7899"
externalUserDN="uid=tmorris,ou=people,o=cognos,c=ca">
       <BasicSignon>tmorris</BasicSignon>
       <OSSignon>domain/tmorris</OSSignon>
       <Description>Employee id: 56789</Description>
    </User>
</NamespaceReport>
```

# Glossary

**Access Manager Server**

A Cognos security component that manages a ticket service and an authentication service. An Access Manager Server can be configured as a ticket service or an authentication service, or both.

At least one Access Manager Server is needed for each Cognos application. Preferably, it should be installed on the same computer as the directory server. To implement failover and load balancing for the Access Manager Server, you can install additional Access Manager Servers and configure load balancing in Configuration Manager.

See also Ticket Service and Authentication Service.

**anonymous user**

An unnamed user who can access a data source without seeing a logon screen. Anonymous users are never asked for identification but you can restrict their access to data sources and their membership in user classes.

Anonymous users are usually granted minimal access privileges, such as access to Public folders in Upfront. They usually belong to user classes that cannot permanently change preferences or any IDs or passwords for secure resources.

The anonymous user

- must be a member of at least one user class
- can have auto-access
- can exist in the public user class

If you enable anonymous users in a namespace, then other Cognos products will not prompt users for a user ID or password .

**authenticate**

To identify a user with a signon (user ID and password), verify that the user has the required access privileges, and grant access accordingly.

**authentication data**

Data that is required to identify users (user IDs and passwords) and to provide access to application servers and data sources protected by means of user class privileges or user passwords.

**authentication service**

An Access Manager Server service used for authentication in Web-deployed Cognos applications. When an authentication service is configured, the logon process communicates with the authentication service, which then communicates with the ticket service and the directory server. When an authentication service is not configured, the logon process communicates directly with the ticket service and the directory server. By default, the authentication service is not enabled. To use this service, an Access Manager server must be configured as an authentication service.

See also Access Manager Server and Ticket Service.

**authentication source**

Source of authentication data. Most Cognos applications currently support directory server namespaces and local authentication export files (.lae).

**auto-access**

The ability to access a password-protected cube, database, or server without being prompted for logon information.

**base distinguished name (DN)**

The higher levels and directory names of the path (including the root) that you specify to access the hierarchical information in a namespace.

For example, the root level C (country) in the directory CA (Canada) together with the organizational level (O=Cognos) forms the base DN for the following distinguished name:

CN = Cognos Documentation, O = Cognos, C = CA

**basic signon**

A signon (user ID and password) that you create and maintain in Access Manager and that Cognos applications use to identify individual users.

Compare to operating system (OS) signon.

**bind**

To access a directory in a directory server by providing the appropriate distinguished name (DN) and password.

**collection**

A group of related OLE objects that you can reference as a unit. Any action performed on a collection affects all objects in that collection.

See also ownership collection and reference collection.

**common logon**

A set of user prompts that Access Manager uses to identify users and govern access to data sources. Users are prompted once for their logon information.

Windows-based Cognos products use the Windows Common Logon Server to record this information, and Web-based Cognos products provide for a single signon using tickets issued by the Access Manager Server ticket service.

**Cognos security administration file (.csa)**

A .csa file is used by Access Manager to store connection information. It maintains directory server and .lae file connection information, the directory server currently configured to be active, and the expansion state of the nodes on the directory tree.

**cube**

Multidimensional information structured hierarchically, to support efficient online analytical processing (OLAP). Cognos business intelligence tools can generate reports based on cubes that were created in PowerPlay Transformer (PowerCubes), and in various third party OLAP sources. You can store cubes in one of several supported relational databases, in a LAN folder, or on a local computer (standard cubes).

**data object**

An object that identifies individual data locations and that enables access to them.

**default namespace**

The directory server namespace used by Access Manager at run time when no namespace is specified in the configuration.

### delegated administrator

An administrator who can create and update lower-level permissions. For example, directory administrators (also known as a directory managers in SunONE directory server) can administer directories on a directory server; regional managers can administer the authentication data associated with users in their regional office.

### directory server

A general term for an LDAP-compliant server that contains authentication data. Cognos applications can use the SunONE directory server or Active Directory Server to associate users with data access permissions.

### distinguished name (DN)

The path that you specify to access the hierarchical information in a namespace. The hierarchy has a name for each level, called CommonName (CN), OrganizationName (O), and an optional CountryCode (C). There can be many directories on the same level.

Unlike a DOS path, where the root directory precedes the target, in a distinguished name the lowest (target) level and directory name appear first, followed by each higher level and directory name, terminating in the root. For example, a DN used to access a namespace of the security directory server is as follows:

CN = Cognos Documentation, O = Cognos, C = CA

The root level is C (Country) and the root directory is Canada. The target level is CN (Common Name) and the target directory is Cognos Documentation.

### distributed administration

A method of updating local data from a centrally-maintained master source. In the case of authentication data, a Cognos security administration file (.csa) can be used to provide updated local authentication export files (.lae) or directory server namespaces to remote or networked systems.

### drill through

To view detailed information behind a value in a report. For example, you can drill through from a summary to view the detailed sales transactions for a particular customer. You may also be able to drill through to information provided in another Cognos application, such as Impromptu.

### guest user

An unnamed user who can access a data source without providing signon information. Enabling guest users allows you to set different security access for named and for unnamed (guest) users.

Guest users are usually granted minimal access privileges, such as access to Public folders in Upfront. They usually belong to user classes that cannot permanently change preferences or any IDs or passwords for secure resources.

The guest user

- must be a member of at least one user class
- can have auto-access
- can exist in the public user class

If you enable guest users in a namespace, then Cognos products that support guest access will offer users the option of logging in as guests.

### LDAP data interchange format file (.ldif) (definition)

An ASCII file in standard LDAP data interchange format.

### Lightweight Directory Access Protocol (LDAP)

A product-independent protocol that is used to locate organizations, individuals, files, and other resources on the Internet or a corporate Intranet.

To use Access Manager with Cognos BI servers in production, you must use an LDAP directory server as your authentication source.

### local authentication

The process of verifying access to protected data sources using local authentication export files (.lae) or local authentication cache files (.lac) Usually used for mobile or standalone users.

### local authentication cache file (.lac)

A source of personal authentication data in Access Manager that can automatically be created on each user's computer when those users access the central directory server. The .lac file enables mobile users to access their authentication data even when they aren't connected to the network. Local authentication cache files are read-only.

### local authentication export file (.lae)

A source of authentication data in Access Manager that is independent of a directory server and that may be used to

- authenticate standalone users who cannot be authenticated over a network (Access Manager configuration)
- transfer authentication data between namespaces (Access Manager Administration)

You can only use .lae files locally on a single computer, not on a network or with multiple users.

### locked namespace

A namespace that has become inaccessible, due to a power failure, for example, or some other unexpected interruption during the directory server update process.

### lockout

A condition whereby a user is prevented from logging on for a set period of time because they made a number of unsuccessful logon attempts. Administrators define the number of permitted attempts and the lockout duration.

### logon

The process of authentication (for example, entering a user ID and password for basic signon) to gain access to protected data sources. An administrator can limit the number of unsuccessful logon attempts, after which access is restricted for a prescribed lockout duration.

### method

An action defined in a Basic-like language that is performed by OLE automation objects. You use an object method to cause the application to perform an operation on an object, such as open or save.

### multidimensional cube file (.mdc)

The Cognos file that the PowerCube designer creates in PowerPlay Transformer, and that contains multidimensional data. It can also be a pointer file that connects to a database cube or a third-party OLAP source.

### namespace

A source of authentication data used by Access Manager that exists as a directory on a directory server, or as an entry in a local authentication export file (.lae), depending on the default security server configured in the system registry.

The security data stored in each namespace, such as signon information for users, user classes, application servers and data sources, distinguishes each entry from all other namespaces in the repository.

### Netscape Certificate Database file

A file that stores the digital certificates used to create digital signatures and private keys required for a Secure Sockets Layer (SSL) connection.

### object

The OLE automation element that you manipulate to create and modify such things as files and reports. You manipulate an object by changing its associated properties and methods.

### OLE automation

A process whereby the features of an application are made available as a collection or group of objects. OLE automation objects have properties and methods that you can use to control object attributes and operating characteristics. For example, the objects, properties, and methods exposed by an application correspond to the dialog box options and menu commands provided by the Application object.

### operating system (OS) signon

An operating system (OS) signon consists of a user ID and password that authorizes a user to log on to their computer network or operating system. The OS signon is used by Access Manager but created and maintained outside of Access Manager. If a user has both an OS signon and a basic signon, the OS signon is verified first, then the basic signon.

To find an OS signon, Access Manager first checks for a network ID. If the user is not connected to a network, Access Manager then checks for an operating system ID.

### ownership collection

Contains a group of objects that are dependent on the collection.

See also reference collection.

### password-protected data

Sensitive or confidential data that may only be accessed by users who enter the correct password.

### permission

In Access Manager, an information access privilege set up by an administrator and granted at runtime, such as the ability to create and update data.

### privilege

See permission.

### property

In OLE automation terms, a set of values or characteristics that remains with an OLE object, and which is retained in memory. You use an object property to set or access the value of some property that the object has. A property defines one of the characteristics of an object, such as its size or color, or an aspect of its behavior, such as whether it is visible or not (that is, appears on the screen or performs its commands without displaying anything on the screen). To change the characteristics of an object, you change the value of its properties.

### public user class

The user class to which all users in a namespace automatically belong. This user class is carried forward into other Cognos products. You do not have to name the public user class "public".

You can associate users with other user classes, but they always remain members of the public user class. You can assign properties and access to the public user class, as you would for any other user class.

By default, a namespace does not have a public user class associated with it.

### reference collection

References an object that has been previously created, and contains a group of objects that are independent of the collection.

See also ownership collection.

### restricted administrator

See delegated administrator.

### root administrators

Administrators who have access to an entire namespace and all permissions associated with it. The root administrator is created by default, and can be renamed but not removed from the namespace.

### root user class

The user class with all administration privileges to the namespace. The Administrator user is a member of the root user class. The root user class is created by default, and can be renamed but not removed from the namespace.

### schema

A description of the object classes (the various types of objects) and the attributes for those object classes in an LDAP database.

When you configure a directory server, you extend the directory server schema to include Access Manager functionality.

### signon

A User ID and password that is used to identify individual users and govern their access to resources.

### single signon

A process whereby a user logs on once but can access multiple data sources, without multiple prompts. The term generally applies to Web-based products only; for Windows products, an equivalent term is common logon.

### ticket

A record of a user's authorization that allows use of a Web-based product for an amount of time specified by the administrator. A ticket is created each time that the user logs on.

### ticket service

An Access Manager Server service that issues tickets used to maintain single signons for users of Web-deployed Cognos applications. The tickets are issued for a specified period of time so that users can access multiple applications without having to re-enter authentication data. To use this service, an Access Manager server must be configured as a ticket service.

See also Access Manager Server and Authentication Service.

### user object

A software object that represents the users of a product. For authentication purposes, user objects are used to specify the user's ID and password, basic signon or operating system (OS) signon, user class memberships, and auto-access assignments.

### user class object

A software object that administrators define for their organizations to control access based on membership in specific user groups or communities. A user class object specifies the user class name, the times that members of the user class can access data, and the administrative privileges the user class has in Access Manager.

The data a user class can access is defined in a client application.

### user class-protected data

Sensitive or confidential data that may only be accessed by authorized users, on the basis of membership in a specified user class.

### user class union

A combination of user class permissions for users who belong to more than one user class. Applications that support a union of user classes do not require a user to choose a user class when they log on. Instead, users are granted all the combined permissions of the user classes that they belong to.

### user class view

In Transformer, the categories and measures that members of a specified user class are permitted to see, typically a subset of the information contained in the entire PowerCube. The cube designer can specify whether the values associated with omitted categories are rolled-up (summarized) or removed from reports based on the cube.

In other Cognos applications, the term is used more generally to signify access to a data source or an authorized subset of the information in that source, based on user class membership.

**Note:** Not to be confused with the User Classes and Users View in the Administration tool of Impromptu Web Reports, which is a hierarchical view of the User Classes folder and the Users folder.

### user reference

Information that associates a user with a user class. See also user and user class objects.

### Windows Common Logon Server

A server that records information about the users of a Windows-based application so that they can log on once and access multiple data sources.

# Index

## Symbols



## A

## B



## C



## D

## E



## F



## G



## H



## I



## L

## M



## N



## O



## P

## R



## S



## T

## U



## V



## W



## X