CA Performance Center

Single Sign-On User Guide

2.4.1

CA Technologies Product References

This document references the following CA Technologies products:

- CA Performance Center
- CA Infrastructure Management Data Aggregator
- CA Network Flow Analysis
- CA Application Delivery Analysis
- CA Unified Communications Monitor

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Customizing Authentication in CA Performance Center

This section contains the following topics:

CA Single Sign-On

Single Sign-On is the authentication scheme for CA Performance Center and all supported data sources. Once they are authenticated to CA Performance Center, users can navigate among the console and registered data sources without signing in a second time.

By enabling navigation among separate product interfaces, Single Sign-On helps ensure a seamless drilldown experience for operators who are analyzing performance and status data. For example, if a user logs in to CA Performance Center and then follows a drilldown path to the data source interface, that user does not log in again.

CA Performance Center uses a distributed architecture. An instance of the Single Sign-On website is automatically installed on every server where a supported data source or CA Performance Center is installed. The distributed architecture lets users log in to individual CA data source products by logging in to the servers where these products are running.

CA Performance Center Authentication and Security

Single Sign-On provides authentication services to CA Performance Center and supported data sources. It also supports external authentication schemes, such as LDAP and SAML 2.0. This support lets you integrate CA Performance Center and other CA data source products into the same authentication scheme, enterprise-wide.

The Single Sign-On security auditing feature logs information about who is logging in, and at what time of day. On Linux servers, the log is saved in the following location:
`[InstallationDirectory]/PerformanceCenter/sso/logs`

And on Windows servers where the data sources are installed, the log is saved in the following directory:
`[InstallationDirectory]\Portal\SSO\logs`

Authentication Methods

The Single Sign-On component provides the login page that supports user authentication in CA Performance Center and in the data source products. Single Sign-On supports the following authentication methods:

- Product authentication, which is based on user accounts
- LDAP
- Security Assertion Markup Language (SAML) 2.0

The CA Performance Center administrator can modify settings for an individual instance of Single Sign-On. For example, you can set up LDAP authentication in Single Sign-On. You can also configure optional encryption with Secure Sockets Layer (SSL) or change the default virtual directory.

Note: As a result of the distributed architecture, any updates to the Single Sign-On website only affect those data source products that are running on the same server.

Data Source Support

CA Single Sign-On supports all of the following data sources:

- CA Infrastructure Management Data Aggregator
- CA Network Flow Analysis
- CA Application Delivery Analysis
- CA Unified Communications Monitor

The Single Sign-On Configuration Tool was designed to run on Linux systems. However, you can also deploy it on the Windows servers where data sources are installed. If you launch the Configuration Tool from a Windows server, log in as an Administrator on that server.

You can also run the Configuration Tool on Linux and send configuration instructions to data sources running on Windows by using the Remote Value option.

The Configuration Tool is installed in the following directory location on Linux:
`[InstallationDirectory]/CA/PerformanceCenter`

On Windows servers where the data sources are installed, the Configuration Tool is installed in the following directory:
`[InstallationDirectory]\Portal\SSO\bin\SsoConfig.exe`

Single Sign-On Configuration Tool

The Single Sign-On Configuration Tool is a command-line application that lets administrators adjust the settings for the Single Sign-On website and the associated CA data source products.

Note: The 'Remote Value' option in the Configuration Tool propagates the settings to each registered data source. Use the 'Local Override' option to override the propagated settings on a selected server.

The Single Sign-On Configuration Tool was designed to run on Linux systems. However, you can also deploy it on the Windows servers where data sources are installed. If you launch the Configuration Tool from a Windows server, log in as an Administrator on that server.

Use the Single Sign-On Configuration Tool to perform the following tasks:

- Configure data source products to use LDAP authentication.

  All of the LDAP settings for each product are updated using this tool. You can also test the current LDAP configuration to verify settings.

- Configure data source products to use SAML 2.0 authentication.

  In addition to using the Configuration Tool, the administrator must also take some steps on the Identity Provider to set up SAML 2.0 authentication.

- Update the Single Sign-On virtual directory that each product references.

  If you added an encryption scheme or changed the Single Sign-On virtual directory, use this tool to synchronize the data source products. For example, data sources on the modified server need instructions on where to redirect users who do not successfully authenticate.

- Enable communications among servers running CA software products using HTTPS.

  This change affects the Single Sign-On URL scheme and port. The Single Sign-On Configuration Tool lets administrators easily update these values in all of the necessary data source products.

Back Up Single Sign-On Configuration Files

When you change settings using the Configuration Tool, your settings are saved in configuration files. Create backup copies of these files on a regular basis to avoid losing Single Sign-On settings. Use rsync or another preferred method, such as a script, to back these files up automatically or before an upgrade.

Add the following files to your backup procedures:

InstallationDirectory/CA/PerformanceCenter/sso/start.ini
InstallationDirectory/CA/PerformanceCenter/PC/start.ini

Also back up the following directories:

InstallationDirectory/CA/PerformanceCenter/sso/webapps/sso/configuration
InstallationDirectory/CA/PerformanceCenter/sso/etc
InstallationDirectory/CA/PerformanceCenter/sso/conf
InstallationDirectory/CA/PerformanceCenter/PC/etc
InstallationDirectory/CA/PerformanceCenter/PC/conf

Note: The default installation directory is /opt/CA.

Update Single Sign-On Website Settings

The Single Sign-On Configuration Tool lets you change default settings for the Single Sign-On website. For example, you can change the virtual directory for the Single Sign-On website. The virtual directory is required to use an encryption scheme for communications among CA servers.

You can change other settings that affect Single Sign-On behavior when users attempt to log in. Some parameters also affect user interface behavior, such as the timeout period that logs the user out automatically in response to inactivity.

Important! Updates to the Single Sign-On website only affect CA data source products that are running on the same server because of the distributed architecture of the software.

Follow these steps:

1. Log in to the server where CA Performance Center or a CA data source product is installed.

   Log in as root or with the 'sudo' command.

2. Launch the Single Sign-On Configuration Tool by running the './SsoConfig' command in the following directory:

   `[InstallationDirectory]/CA/PerformanceCenter`

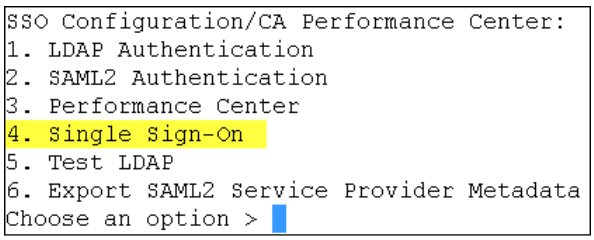
   You are prompted to select an option. The available options correspond to CA applications running on the local server.

3. Use the following commands as needed while you are selecting settings:

   - q (quit)
   - b (go back to the previous menu)
   - u (update)
   - r (reset)

4. Enter 1 to configure CA Performance Center.

   You are prompted to select an option.

5. Enter 4 for Single Sign-On.

   You are prompted to specify the priority.

   The Priority parameter only applies to CA Performance Center.

6. Enter one of the following options:

   1. Remote Value

   Refers to settings that only administrators can change. Such settings are propagated to all other CA products registered to this instance of CA Performance Center. Remote Value settings are only used if a corresponding Local Override value is not present.

   2. Local Override

   Refers to settings that can be changed for all products. If a Local Override value is present, it takes precedence over both the Remote Value and default settings.

   You are prompted to select a property to configure.

7. Enter one or more of the following properties. When prompted, enter u to update the value and supply a new value:

   1. Anonymous User Enabled

   Specifies whether the Sign-In page appears when users attempt to log in to a data source interface. A value for the Anonymous User ID parameter is required if this parameter is enabled. Users do not see the Sign-In page when they attempt to log in. They are logged in as the user associated with the Anonymous User ID parameter.

   The Localhost User Enabled parameter takes precedence when the following conditions are met:

   - The user is logging in from the Single Sign-On server.
   - The 'Localhost User Enabled' parameter and the 'Anonymous User Enabled' parameter are both enabled.

   Default: Disabled.

   Note: The Anonymous User login takes precedence over Windows Authentication.

   2. Anonymous User ID

   Specifies the username that is used to authenticate the user automatically, bypassing the Sign-In page. This parameter is only used if the Anonymous User Enabled parameter is enabled. Select one of the following values:

   - **1** - The username for the default administrator account (admin).
   - **2** - The username for the default user account (user).
   - Another username that exists in the CA Performance Center database.

3. Localhost User Sign-In Page Enabled

Specifies whether the Sign-In page appears when the user is logging in from the server where Single Sign-On is installed.

If this parameter is enabled, the Sign-In page appears, even if the user is logging in from the Single Sign-On server.

If this parameter is disabled, the following rules apply:

- The Localhost User Enabled parameter must be enabled.
- The value for the Localhost User ID parameter must contain a valid product username. This value is used to log the user in to the software interface, bypassing the Sign-In page.

Default: Disabled.

4. Localhost User Enabled

Specifies whether users are automatically signed in—bypassing the Sign-In page—when they are logging in from the Single Sign-On server. A value for the 'Localhost User ID' parameter is required if this parameter is enabled.

- If the 'Localhost User Sign-In Page Enabled' parameter is enabled, this parameter is used in cases where the user clicks Sign In without entering a username or password. The user is then logged in to the software as the user associated with the 'Localhost User ID' parameter.
- If the user does supply a username and password, those credentials are used for authentication.
- If this parameter is enabled but the 'Localhost User Sign-In Page Enabled' parameter is disabled, the user bypasses the Sign-In page. The user is instead logged in to the interface using the value of the 'Localhost User ID' parameter.
- If the user is logging in from the Single Sign-On server and both the 'Localhost User Enabled' and 'Anonymous User Enabled' parameters are enabled, the 'Localhost User Enabled' parameter takes precedence.

Default: Disabled.

5. Localhost User ID

Specifies the user ID that is used to authenticate users automatically—bypassing the Sign-In page—when they log in to the Single Sign-On server. This parameter is used only if the 'Localhost User Enabled' parameter is enabled. Enter one of the following values:

1 - The username for the default administrator account (admin).

2 - The username for the default user account (user).

6. Cookie Timeout Minutes

Specifies the number of minutes that pass before a Single Sign-On cookie expires. Each time a user performs an action in a data source interface, the cookie timeout resets. If the timeout expires, the user is logged out and must reauthenticate.

Default: 20 minutes

7. Encryption Decryption Key

Specifies the key that is used to encrypt and decrypt the Single Sign-On cookie.

8. Encryption Algorithm

Specifies the encryption algorithm that is used to encrypt and decrypt the Single Sign-On cookie. Supply either DES or AES for the value.

9. Failed Sleep Seconds

Specifies the number of seconds the Single Sign-On application waits after a failed sign-in attempt.

10. Remember Me Enabled

Specifies whether the Remember Me check box is displayed on the Sign-In page. The Remember Me setting determines whether a user is automatically logged out when the Cookie Timeout expires.

Default: Enabled.

11. Remember Me Timeout Days

Specifies the number of days that pass before a user who selected 'Remember Me' on the Sign-In page must reauthenticate. This parameter is only used if the 'Remember Me Enabled' parameter is enabled. A value of 0 indicates that the Remember Me setting does not expire; the user must click the Sign Out link in a data source product interface.

12. Scheme

Specifies the URL scheme that data source products can use to access the Single Sign-On application. If you are using SSL, supply 'https:' for the value.

13. Port

Specifies the URL port that data source products can use to access the Single Sign-On application.

14. Virtual Directory

Specifies the name of the virtual directory for Single Sign-On.

Default: SingleSignOn.

Note: If you change the value for any of the previous parameters, the default value is not replaced, but the new value now takes precedence. The new value is actually a Local Override.

8. Enter b when you have finished changing the default settings.
9. You return to the previous set of options.
10. Enter b again to go back to the first set of options.
11. Enter q to close the Single Sign-On Configuration Tool.

    The Single Sign-On Configuration Tool closes.

    CA Performance Center directs all unauthenticated users to the Single Sign-On website using the new values that you supplied.

Update CA Performance Center Website Settings

The Single Sign-On Configuration Tool lets you change the default settings for the CA Performance Center website and web service. For example, you can specify a different host or port number for the CA Performance Center web service. These settings instruct the Single Sign-On application how to connect to CA Performance Center.

Follow these steps:

1. Log in to the server where CA Performance Center or a CA data source product is installed.

   Log in as root or with the 'sudo' command.

2. Launch the Single Sign-On Configuration Tool by running the './SsoConfig' command in the following directory:

   `[InstallationDirectory]/CA/PerformanceCenter`

   You are prompted to select an option. The available options correspond to CA applications running on the local server.

3. Use the following commands as needed while you are selecting settings:
   - q (quit)
   - b (go back to the previous menu)
   - u (update)
   - r (reset)
4. Enter 1 to configure CA Performance Center.

   You are prompted to select a configuration option.

```
SSO Configuration/CA Performance Center:
1. LDAP Authentication
2. SAML2 Authentication
3. Performance Center
4. Single Sign-On
5. Test LDAP
6. Export SAML2 Service Provider Metadata
Choose an option >
```

5. Enter 3 for Performance Center.

   You are prompted to specify the priority.

   The Priority parameter only applies to CA Performance Center.
6. Enter one of the following options:

   1. Remote Value

   Refers to settings that only administrators can change. Such settings are propagated to all other CA products registered to this instance of CA Performance Center. Remote Value settings are only used if a corresponding Local Override value is not present.

   2. Local Override

   Refers to settings that can be changed for all products. If a Local Override value is present, it takes precedence over both the Remote Value and default settings.

   You are prompted to select a property to configure.
7. Enter one or more of the following properties. When prompted, enter u to update the value and supply a new value:

   1. Web Service Scheme

   Specifies the URL scheme that the Single Sign-On application can use to access the CA Performance Center web service. Change this value to ‘https’ if you are using SSL for encryption.

2. Web Service Host

Specifies the URL of the host where the Single Sign-On application can access the CA Performance Center web service.

3. Web Service Port

Specifies the URL port that the Single Sign-On application can use to access the CA Performance Center web service.

4. Web Service Inventory

Specifies the URL path that the Single Sign-On application can use to access the CA Performance Center Inventory web service.

5. Web Service Product Request

Specifies the URL path that the Single Sign-On application can use to access the CA Performance Center Product Request web service.

6. Web Site Scheme

Specifies the URL scheme that the Single Sign-On application can use to access CA Performance Center. If you have set up SSL, use https://.

7. Web Site Host

Specifies the URL host that the Single Sign-On application can use to access CA Performance Center.

8. Web Site Port

Specifies the URL port that the Single Sign-On application can use to access CA Performance Center.

9. Web Site Path

Specifies the URL path that the Single Sign-On application can use to access CA Performance Center.

10. SMTP Enabled

Specifies whether the Simple Mail Transfer Protocol (SMTP) is enabled to allow CA Performance Center operators to email reports and event notifications.

Default: Disabled.

11. SMTP Server Address

Is the IP address of the SMTP server.

Default: Disabled.

12. SMTP Ports:

Specifies the port to use for SMTP requests.

Default: Port 25.

13. SMTP SSL

Specifies whether to use SSL encryption when sending email from CA Performance Center or other CA data source products. Verify that SSL has been properly set up on your system before you enable this option.

Default: Disabled.

14. Email Reply Address

Specifies the return address to use for email messages that are generated by CA Performance Center. Enter u to update the value, and supply an email address. Use the format username@mydomain.com.

15. Email Format

Specifies the format to use for email messages that are sent by CA Performance Center. Enter u to update the value, and supply either HTML or text.

16. SMTP Username

Specifies a username to use when the email server challenges an SMTP request. Supply a username, or supply an empty string to disable client-side authentication.

17. SMTP Password

Specifies a username to use when the email server challenges an SMTP request. Supply any valid password. The SMTP Username parameter is required.

8. Enter b when you have finished changing the default settings.

   You return to the previous set of options.

9. Enter b again to go back to the first set of options.

10. Enter q to quit.

    The Single Sign-On Configuration Tool closes.

    CA Performance Center directs all users to the Single Sign-On website using the new values that you supplied.

Chapter 2: Setting Up LDAP Authentication

This section contains the following topics:

LDAP Support

Single Sign-On provides LDAP integration, allowing operators to authenticate to a Lightweight Directory Access Protocol (LDAP) server running in your environment. Once authenticated, they are mapped to a user account that the administrator can specify: either to a predefined user account, or to a custom account.

The Single Sign-On Configuration Tool lets you precisely specify how the Single Sign-On server connects to the LDAP server. You can also map individual CA Performance Center users to the user accounts that support their workflow while protecting sensitive data.

Note: Changes made in the Single Sign-On Configuration Tool only affect newly created LDAP users. They do not apply to existing LDAP users registered within CA Performance Center.

The LDAP parameters available in the Single Sign-On Configuration Tool let you integrate CA Infrastructure Management and all registered data sources into an existing authentication scheme. For example, the LDAP server can authorize groups of users who are mapped to a single custom user account in CA Performance Center. The actual account names and LDAP groups can be extensively customized. Search scope parameters let you determine how the directory search is conducted. And you can select the user account properties that are considered when validating users.

Enable LDAP Authentication with No Authentication Mechanism

Use the Single Sign-On Configuration Tool to instruct registered data sources to use the same LDAP scheme to authenticate users. The Single Sign-On Configuration Tool lets you supply parameters that enable the CA server to connect securely to the LDAP server. Using the Configuration Tool, you can also associate users in the LDAP catalog with either predefined or custom user accounts in CA Performance Center.

The steps to take to enable LDAP authentication are slightly different if you are using an authentication mechanism (see page 24) such as GSSAPI. Without an authentication mechanism, you must use a service account to bind to the LDAP server. This account requires read and search access to the LDAP server. You must supply the full DN (distinguished name) of the connection user, and you must also enable the User Bind parameter.

Single Sign-On binds to the LDAP server using the credentials that you supply for the Connection User and Connection Password parameters. Then Single Sign-On performs a directory search that is based on the string that you supply for the Search String parameter. The search results include the DN of the user. Single Sign-On performs a second bind to the LDAP server using this DN and password.

Important! In cases where no authentication mechanism is used, we strongly recommend establishing an SSL connection to the LDAP server. Otherwise, the passwords are transmitted to the LDAP server in cleartext.

Follow these steps:

1. Log in to the server where CA Performance Center or a CA data source product is installed.

   Log in as root or with the 'sudo' command.

2. Launch the Single Sign-On Configuration Tool by running the './SsoConfig' command in the following directory:

   InstallationDirectory/CA/PerformanceCenter

   You are prompted to select an option. The available options correspond to CA applications running on the local server.

3. Use the following commands as needed while you are selecting settings:
   - q (quit)
   - b (go back to the previous menu)
   - u (update)
   - r (reset)
4. Enter 1 to configure CA Performance Center.

   You are prompted to select an option.
5. Enter 1 for LDAP Authentication.

   You are prompted to specify the priority.

   The Priority parameter only applies to CA Performance Center.
6. Enter one of the following options:

   1. Remote Value

   Refers to settings that only administrators can change. Such settings are propagated to all other CA products registered to this instance of CA Performance Center. Remote Value settings are only used if a corresponding Local Override value is not present.

   2. Local Override

   Refers to settings that can be changed for all products. If a Local Override value is present, it takes precedence over both the Remote Value and default settings.

   You are prompted to select a property to configure.
7. Enter one or more of the following properties. When prompted, enter u to update the value and supply a new value:

   1. Connection User

   Defines the user ID (in this case, the user ID of the service account) that the login server uses to connect to the LDAP server. This LDAP username is used to bind to the server.

   Important! A service account with read and search access to the LDAP server is required for this parameter if you are not using an authentication mechanism, such as GSSAPI.

   2. Connection Password

   Defines the password for the login server to use to connect to the LDAP server.

   Example: If the login server uses a fixed account, enter text like the following example:

   `SomePassword`

3. Search Domain

Identifies the LDAP server and port to which CA Single Sign-On connects. Also identifies the location in the directory tree where the search looks for users when verifying user account credentials. If you do not also supply a port number after the server in the string, Port 389 is used.

Use the following format for the search domain:

LDAP`://ldap_server:port/path_to_search`

Note: The search path is *required*.

4. Search String

Specifies the criteria that are used to locate the correct record for the user. Works with the Search Scope parameter. If only a subset of LDAP users is allowed to log in, the search string can be used to search the record for multiple properties. The value for this parameter can include any valid LDAP search criterion.

Example:

```
(saMAccountName={0})
```

5. Search Scope

Specifies the criteria that are used to locate the correct record for the user. Used with the Search String parameter. Determines the scope of the search that the LDAP server performs for the user account. Type one of the following values:

onelevel

Includes the current directory in the search. Matches objects in the current directory and prevents unexpected matches deeper in the directory.

subtree

Includes all subdirectories in the search. Recommended for most installations.

base

Limits the search to the base object.

6. User Bind

Specifies whether to do an additional authentication step (bind) using the distinguished name (DN) and password of the user to validate the supplied credentials.

Important! This parameter must be set to Enabled if you entered a service account in Steps 1 and 2.

Default: Disabled.

7. Encryption

Specifies the authentication mechanism to use when binding a second time to the LDAP server.

Default: Simple.

Accepted Values: Simple, GSSAPI, DIGEST-MD5.

8. Account User

Specifies the CA Performance Center default account to which to map validated LDAP users who lack a group membership. Works with the Account Password parameter. If a valid user does not match any group definitions, the user is logged in with the default user ID specified for this parameter.

To allow all users to log in with their own username, enter:

- {saMAccountName}
- {saMAccountName} or {CN}

Note: The Account User parameter corresponds to a field from the directory entry for this user. Typically, the value matches your search filter.

9. Account User Default Clone

Specifies a user account to clone if validated LDAP users are members of a group that is not specified for the Group parameter.

Example: Enter 'user' if you want such users to have minimal privileges.

Note: An existing user account is required.

10. Group

Lets you determine the default account handling for selected user accounts or groups of accounts.

Example: To enable all members of a group to log in using an administrator account, enter:

```
<LDAPGroups><Group searchTag="memberOf" searchString="CN=SEC_All
Employees,CN=Users,DC=company,DC=local" user="{saMAccountName}" passwd=""
userClone="admin"/></LDAPGroups>
```

11. Timeout

Specifies the amount of time that CA Performance Center waits while making authorization checks to the LDAP server. When the authorization check times out, users who try to log in are denied access. To view the errors, open the SSOService.log file. The default timeout is 10000.

8. Verify that the LDAP Status is set to Enabled. If the LDAP status is set to Disabled, then authentication uses the internal Performance Center user database.
9. Enter q to quit.

   The Configuration Tool closes.

Example Configuration

1. Connection User: CN=********,OU=Role-Based,OU=North America,DC=ca,DC=com [the full DN of the service account]
2. Connection Password: ******* [the password of the service account]
3. Search Domain: LDAP://******.ca.com/DC=ca,DC=com
4. Search String: (sAMAccountName={0})
5. Search Scope: Subtree
6. User Bind: Enabled
7. Encryption: false
8. Account User: {sAMAccountName}
9. Account User Default Clone: user
10. Group: 'All Employees'
11. Krb5ConfigFile: krb5.conf

Encrypt the Connection to the LDAP Server Using GSSAPI

CA Single Sign-On supports encrypted connections using DIGEST-MD5 or GSSAPI. When you use an encrypted connection to the directory server, you do not have to use a service account to bind to the LDAP server (the UserBind parameter that you set in the Single Sign-On Configuration Tool).

To use GSSAPI for encryption, you must change some settings in a configuration file.

Follow these steps:

1. Log in to the server where CA Performance Center or a CA data source product is installed.

   Log in as root or with the 'sudo' command.

2. Change to the following directory:
   Installation Dir/webapps/sso/Configuration/

3. Open the krb5.conf file in that directory for editing.
4. Set the following required parameters:

```
[libdefaults]
        default_realm = CA.COM
[realms]
        CA.COM  = {
                kdc = EXAMPLE.CA.COM
                default_domain = CA.COM
}

[domain_realm]
       .CA.COM = CA.COM
}
```

   where:

   [libdefaults]

   Contains default values for the Kerberos V5 library.

   default_realm

   Maps subdomains and domain names to Kerberos realm names. Lets programs determine the realm for a host, based on its fully qualified domain name. In this example, the default realm is CA.COM.

   realms

   Contains information about Kerberos realm names, which describe the location of Kerberos servers and include other realm-specific information.

   kdc

   Is the Kerberos key distribution center to support authentication services. For example, EXAMPLE.CA.COM.

   default_domain

   Is the default IP domain. For example, CA.COM.

   Note: Your Active Directory or LDAP Administrator can probably provide you with a krb5.conf file or help you to create one.

5. Save your changes.
6. Now follow the steps in Enable LDAP Authentication Using an Encryption Mechanism (see page 26) to configure LDAP authentication with CA Single Sign-On.

Enable LDAP Authentication Using an Encryption Mechanism

Use the Single Sign-On Configuration Tool to instruct registered data sources to use the same LDAP scheme to authenticate users. The Single Sign-On Configuration Tool lets you supply parameters that enable the CA server to connect securely to the LDAP server. When you use Digest-MD5 or GSSAPI to encrypt the connection to the LDAP server, a single bind operation—as the user you specify—occurs.

Using the Configuration Tool, you can also associate users in the LDAP catalog with either predefined or custom user accounts in CA Performance Center.

Follow these steps:

1. Log in to the server where CA Performance Center or a CA data source product is installed.

   Log in as root or with the 'sudo' command.

2. Launch the Single Sign-On Configuration Tool by running the './SsoConfig' command in the following directory:

   InstallationDirectory/CA/PerformanceCenter

   You are prompted to select an option. The available options correspond to CA applications running on the local server.

3. Use the following commands as needed while you are selecting settings:

   - q (quit)
   - b (go back to the previous menu)
   - u (update)
   - r (reset)

4. Enter 1 to configure CA Performance Center.

   You are prompted to select an option.

5. Enter 1 for LDAP Authentication.

   You are prompted to specify the priority.

   The Priority parameter only applies to CA Performance Center.

6. Enter one of the following options:

   1. Remote Value

   Refers to settings that only administrators can change. Such settings are propagated to all other CA products registered to this instance of CA Performance Center. Remote Value settings are only used if a corresponding Local Override value is not present.

   2. Local Override

   Refers to settings that can be changed for all products. If a Local Override value is present, it takes precedence over both the Remote Value and default settings.

   You are prompted to select a property to configure.

7. Enter one or more of the following properties. When prompted, enter u to update the value and supply a new value:

   1. Connection User

   Defines the user ID that the login server uses to connect to the LDAP server. This LDAP user name is used to bind to the server. A service account is not typically required for a connection that uses an authentication mechanism, such as GSSAPI.

   Example: If the login server uses a fixed account, enter text with the following syntax:

   ```
   CN=The User,cn=Users,dc=domain,dc=com
   ```

   Or you can enter the following value because the connection is using an authentication mechanism:

   ```
   {0}
   ```

   Complex configurations need the user principal name to identify the user. Supply '{0}' and use their email address as the domain name. For example:

   ```
   {0}@domain.com
   ```

   The LDAP server typically does not require a full DN for an encrypted connection.

   Note: For security reasons, do not make the connection user a static account. The LDAP authentication only checks the password when binding to the server. If you use a static account, any user that exists in the LDAP tree is able to log in with any password.

2. Connection Password

Defines the password for the login server to use to connect to the LDAP server.

Example: If the login server uses a fixed account, enter text like the following example:

```
SomePassword
```

Or you can enter the following value because the connection is using an authentication mechanism:

```
{1}
```

3. Search Domain

Identifies the LDAP server and port to which CA Single Sign-On connects. Also identifies the location in the directory tree where the search looks for users when verifying user account credentials. If you do not also supply a port number after the server in the string, Port 389 is used.

Use the following format for the search domain:

LDAP://*ldap_server*:*port*/*path_to_search*

Note: The search path is *required*.

4. Search String

Specifies the criteria that are used to locate the correct user in the directory. Works with the Search Scope parameter. If only a subset of LDAP users is allowed to log in, the search string can be used to search a record for multiple properties. The value for this parameter can include any valid LDAP search criterion.

Example:

```
(saMAccountName={0})
```

5. Search Scope

Specifies the criteria that are used to locate the correct record for the user. Used with the Search String parameter. Determines the scope of the search that the LDAP server performs for the user account. Type one of the following values:

onelevel

Includes the current directory in the search. Matches objects in the current directory and prevents unexpected matches deeper in the directory.

subtree

Includes all subdirectories in the search. Recommended for most installations.

base

Limits the search to the base object.

6. User Bind

Specifies whether to do an additional authentication step (bind) using the distinguished name (DN) and password of the user to validate the supplied credentials.

Default: Disabled. This value is acceptable with an encrypted connection.

7. Encryption

Specifies the authentication mechanism to use when binding again to the LDAP server.

In this case (that is, using an authentication mechanism), enter 'GSSAPI' or 'DIGEST-MD5', based on the mechanisms of your LDAP server.

Default: Simple.

Accepted Values: Simple, GSSAPI, DIGEST-MD5.

8. Account User

Specifies the CA Performance Center default account to which to map validated LDAP users who lack a group membership. Works with the Account Password parameter. If a valid user does not match any group definitions, the user is logged in with the default user ID specified for this parameter.

To allow all users to log in with their own username, enter:

- {saMAccountName}
- {saMAccountName} or {CN}

Note: The Account User parameter corresponds to a field from the directory entry for this user. Typically, the value matches your search filter.

9. Account User Default Clone

Specifies a user account to clone if validated LDAP users are members of a group that is not specified for the Groups parameter.

Example: Enter 'user' if you want such users to have minimal privileges.

Note: An existing user account is required.

10. Group

Lets you determine the default account handling for selected user accounts or groups of accounts.

Example: To enable all members of a group to log in using an administrator account, enter:

```
<LDAPGroups><Group searchTag="memberOf" searchString="CN=SEC_All
Employees,CN=Users,DC=company,DC=local" user="{saMAccountName}" passwd=""
userClone="admin"/></LDAPGroups>
```

11. Timeout

Specifies the amount of time that CA Performance Center waits while making authorization checks to the LDAP server. When the authorization check times out, users who try to log in are denied access. To view the errors, open the SSOService.log file. The default timeout is 10000.

8. Verify that the LDAP Status is set to Enabled. If the LDAP status is set to Disabled, then authentication uses the internal Performance Center user database.
9. Enter q to quit.

   The Configuration Tool closes.

Example Configuration

1. SSO Configuration/CA Performance Center/LDAP Authentication/Remote Value:
2. Connection User: {0}
3. Connection Password: {1}
4. Search Domain: LDAP://******.ca.com/DC=ca,DC=com
5. Search String: (sAMAccountName={0})
6. Search Scope: Subtree
7. User Bind: Disabled
8. Encryption: DIGEST-MD5
9. Account User: {sAMAccountName}
10. Account User Default Clone: user
11. Group: 'All Employees'
12. Krb5ConfigFile: krb5.conf

More information:

Encrypt the Connection to the LDAP Server Using GSSAPI (see page 24)

Enable LDAPS Authentication

Use the Single Sign-On Configuration Tool to instruct registered data sources to use LDAP over SSL (LDAPS) for secure user authentication. By default, LDAP traffic is transmitted unsecured. Enable LDAPS by installing a certificate from a certification authority (CA). With CA Single Sign-On, you must import your certificate into the Java trusted keystore.

The Single Sign-On Configuration Tool lets you supply parameters that enable the CA server to connect securely to the LDAP server. Using the Configuration Tool, you can also associate users in the LDAP catalog with either predefined or custom user accounts in CA Performance Center.

Follow these steps:

1. Log in to the server where CA Performance Center or a CA data source product is installed.

   Log in as root or with the 'sudo' command.

2. Follow the instructions in the topic titled Import the LDAP Certificate (see page 35) to obtain your certificate and import it into the Java keystore.

3. Launch the Single Sign-On Configuration Tool by running the './SsoConfig' command in the following directory:

   InstallationDirectory/CA/PerformanceCenter

   You are prompted to select an option. The available options correspond to CA applications running on the local server.

4. Use the following commands as needed while you are selecting settings:

   - q (quit)
   - b (go back to the previous menu)
   - u (update)
   - r (reset)

5. Enter 1 to configure CA Performance Center.

   You are prompted to select an option.

6. Enter 1 for LDAP Authentication.

   You are prompted to specify the priority.

   The Priority parameter only applies to CA Performance Center.

7. Enter one of the following options:

   1. Remote Value

   Refers to settings that only administrators can change. Such settings are propagated to all other CA products registered to this instance of CA Performance Center. Remote Value settings are only used if a corresponding Local Override value is not present.

   2. Local Override

   Refers to settings that can be changed for all products. If a Local Override value is present, it takes precedence over both the Remote Value and default settings.

   You are prompted to select a property to configure.

8. Enter one or more of the following properties. When prompted, enter u to update the value and supply a new value:

   1. Connection User

   Defines the user ID that the login server uses to connect to the LDAP server. This LDAP user name is used to bind to the server. A service account is not typically required for a connection that uses an authentication mechanism, such as GSSAPI.

   Example: If the login server uses a fixed account, enter text with the following syntax:

   ```
   CN=The User,cn=Users,dc=domain,dc=com
   ```

   Or you can enter the following value because the connection is using an authentication mechanism:

   ```
   {0}
   ```

   Complex configurations need the user principal name to identify the user. Supply '{0}' and use their email address as the domain name. For example:

   ```
   {0}@domain.com
   ```

   The LDAP server typically does not require a full DN for an encrypted connection.

   Note: For security reasons, do not make the connection user a static account. The LDAP authentication only checks the password when binding to the server. If you use a static account, any user that exists in the LDAP tree is able to log in with any password.

2. Connection Password

Defines the password for the login server to use to connect to the LDAP server.

Example: If the login server uses a fixed account, enter text like the following example:

```
SomePassword
```

Or you can enter the following value because the connection is using an authentication mechanism:

```
{1}
```

3. Search Domain

Identifies the LDAP server and port to which CA Single Sign-On connects. Also identifies the location in the directory tree where the search looks for users when verifying user account credentials. If you do not also supply a port number after the server in the string, Port 389 is used.

Use the following format for the search domain:
LDAPS://*ldap_server*:*port*/*path_to_search*

Note: The search path is *required*.

To establish an SSL connection to the LDAP server, use 636 or another SSL connection port for your LDAP server:

```
LDAPS://LDAP Server:636/OU=Users,OU=North
America,DC=ca,DC=com
```

4. Search String

Specifies the criteria that are used to locate the correct user in the directory. Works with the Search Scope parameter. If only a subset of LDAP users is allowed to log in, the search string can be used to search a record for multiple properties. The value for this parameter can include any valid LDAP search criterion.

Example:

```
(saMAccountName={0})
```

5. Search Scope

Specifies the criteria that are used to locate the correct record for the user. Used with the Search String parameter. Determines the scope of the search that the LDAP server performs for the user account. Type one of the following values:

onelevel

Includes the current directory in the search. Matches objects in the current directory and prevents unexpected matches deeper in the directory.

subtree

Includes all subdirectories in the search. Recommended for most installations.

base

Limits the search to the base object.

6. User Bind

Specifies whether to do an additional authentication step (bind) using the distinguished name (DN) and password of the user to validate the supplied credentials.

Default: Disabled. This value is acceptable with an encrypted connection.

7. Encryption

(Optional) Specifies the authentication mechanism to use when binding again to the LDAP server.

The default (Simple authentication) is acceptable with LDAPS.

8. Account User

Specifies the CA Performance Center default account to which to map validated LDAP users who lack a group membership. Works with the Account Password parameter. If a valid user does not match any group definitions, the user is logged in with the default user ID specified for this parameter.

To allow all users to log in with their own username, enter:

- {saMAccountName}
- {saMAccountName} or {CN}

Note: The Account User parameter corresponds to a field from the directory entry for this user. Typically, the value matches your search filter.

9. Account User Default Clone

Specifies a user account to clone if validated LDAP users are members of a group that is not specified for the Groups parameter.

Example: Enter 'user' if you want such users to have minimal privileges.

Note: An existing user account is required.

10. Group

Lets you determine the default account handling for selected user accounts or groups of accounts.

Example: To enable all members of a group to log in using an administrator account, enter:

```
<LDAPGroups><Group searchTag="memberOf" searchString="CN=SEC_All
Employees,CN=Users,DC=company,DC=local" user="{saMAccountName}" passwd=""
userClone="admin"/></LDAPGroups>
```

9. Enter q to quit.

   The Configuration Tool closes.

Example Configuration

1. SSO Configuration/CA Performance Center/LDAP Authentication/Remote Value
2. Connection User: {0}
3. Connection Password: {1}
4. Search Domain: LDAPS://******.ca.com:636/OU=Users,OU=North America,DC=ca,DC=com
5. Search String: (sAMAccountName={0})
6. Search Scope: Subtree
7. User Bind: Disabled
8. Encryption: Simple
9. Account User: {sAMAccountName}
10. Account User Default Clone: user
11. Group: 'All Employees'
12. Krb5ConfigFile: krb5.conf

Import the LDAP Certificate

To run with LDAPS, you must import an LDAP certificate into the Java keystore.

If you do not already have an SSL certificate, you can generate one using the keytool command. This procedure explains how to import a certificate from a CA and install it in the keystore.

Follow these steps:

1. Obtain the certificate from the LDAP server administrator.

2. Import the certificate into the Java Trusted Certificates keystore using the following command:

   `keytool -importcert -keystore installDirectory/jre/lib/security/cacerts -storepass cacertspasswd -alias alias -file filename.cer`

   keystore

   The location of the keystore file (.ks).

   cacertspasswd

   Specifies the password for the cacerts keystore.

   Default: changeit

   filename.cer

   The filename of the certificate.

3. Create a backup of the cacerts file.
4. (Optional) For more security, change the password of the java trusted certificates keystore using the following command:

   `keytool -storepasswd -keystore installDirectory/jre/lib/security/cacerts`

   You are prompted to provide the existing password and the new password.

5. Verify that your imported certificate is available. Use the following command:

   `keytool -list -keystore installDirectory/jre/lib/security/cacerts`

   Important! To enable the web services, the certificate must be in the cacerts keystore. Otherwise, you see an error in the log that reports that PKIX did not find a certificate.

Validate LDAP Settings

The Single Sign-On Configuration Tool lets you test the LDAP settings that you have supplied. You can verify that LDAP authentication is set up correctly. An LDAP test script prompts you to specify a username and password combination to test, using the current settings for LDAP authentication. If you have not already used the Configuration Tool to change LDAP authentication settings, the defaults are used.

Follow these steps:

1. Log in to the server where CA Performance Center or a supported data source product is installed.

   Log in as root or with the 'sudo' command.

2. Launch the Single Sign-On Configuration Tool by running the './SsoConfig' command in the following directory:

   InstallationDirectory/CA/PerformanceCenter

   You are prompted to select an option. The available options correspond to CA applications running on the local server.

3. Use the following commands as needed while you are selecting settings:

   - q (quit)
   - b (go back to the previous menu)
   - u (update)
   - r (reset)

4. Enter 1 to configure CA Performance Center.

   You are prompted to select an option.

5. Enter 5 for the Test LDAP option.

   The prompt asks you to enter a username.

6. Enter a username and a password that you know can authenticate using LDAP.

   Single Sign-On attempts to use the parameters you supplied when you set up LDAP authentication to connect to the LDAP server and validate the user account. If the test succeeds, numerous steps are logged.

   A message reports whether the authentication succeeded or failed.

7. Enter q to quit.

Chapter 3: Setting Up SAML 2.0 Support

This section contains the following topics:

About SAML 2.0

The Security Assertion Markup Language (*SAML*) is a security protocol that is based on XML. The basic concept involves the exchange of security assertions about a subject—a person or a computer—that is requesting access to a secure domain. Assertions include whether the subject can access certain resources, and whether an external data source, such as a policy store, is used.

A typical use of SAML-based authentication is in a federated environment, such as cloud-based services that require an extra layer of security in the corporate network. But any SAML implementation involves at least three component roles:

Relying Party

Uses identity information that is stored on another server to let authorized users gain access to a system. Also referred to as the 'service provider.' CA Performance Center has this role when Single Sign-On is configured to use SAML for authentication.

Asserting Party

Stores identity or security information and provides it when requested for authentication purposes. The SAML term for this component is the *Identity Provider* or *IdP*. The CA SiteMinder server has this role, for example.

Subject

Is the user (or computer) associated with the identity information that is stored by the IdP.

SAML 2.0 Support in Single Sign-On

CA Single Sign-On supports authentication with Security Assertion Markup Language (SAML), version 2.0. A Single Sign-On service can accept and decode SAML 2.0 tokens and can present them to authentication agents that conform to the SAML standard.

Single Sign-On support for SAML 2.0 includes support for single logout. With this support, a user who is logged in to multiple user interfaces can log out of all of them simultaneously. For example, a user who logs in to CA Performance Center and later drills down into flow data in CA Network Flow Analysis can log out of one interface and be logged out of the other interface automatically.

Single Sign-On uses a standards-based SAML 2.0 library. As a result, it potentially supports many more products that rely on the SAML 2.0 standards. However, the following CA products are the only Identity Providers that we have tested with CA Single Sign-On:

- CA SiteMinder Federation Manager
- CA Arcot A-OK™ On-Demand

In a SAML environment, you can select from multiple authentication methods. CA Performance Center users can log in using the typical ('Product') authentication method in Single Sign-On, or they can use a SAML token. The Product method is enabled by default for all active user accounts. Users access the CA Performance Center user interface using the standard URL for CA Single Sign-On.

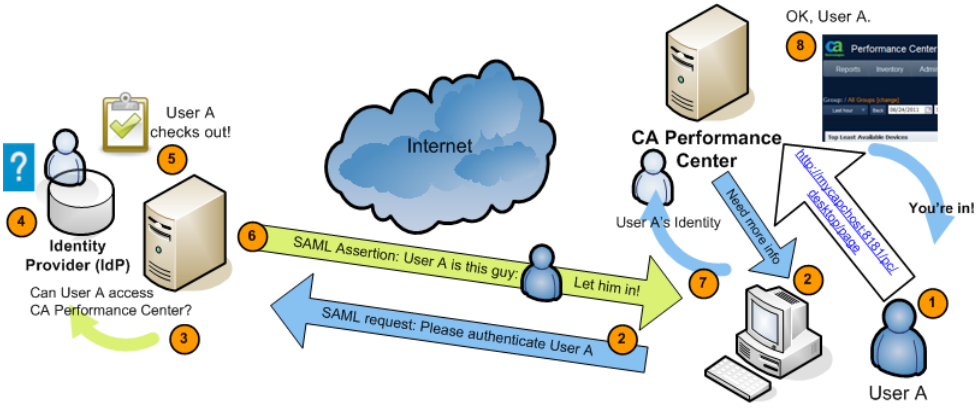
To let users authenticate using SAML 2.0, the administrator must change some Single Sign-On settings using the Configuration Tool. The administrator must also enable External Authentication for all user accounts, and for all registered data sources that support SAML 2.0.

Not all CA data source products support SAML 2.0. If you configure SAML 2.0 for external authentication in Single Sign-On and register a data source that lacks SAML support, CA Performance Center users must reauthenticate when they drill down into that data source.

How Single Sign-On Support for SAML 2.0 Works

The typical CA Performance Center authentication process using Single Sign-On differs from authentication that takes advantage of SAML 2.0 support. With SAML 2.0 authentication, users do not see the CA Performance Center Login page. They are instead redirected to an interface that the IdP provides. For all other supported authentication methods, Single Sign-On provides the login page.

The following diagram illustrates the SAML 2.0 authentication process with Single Sign-On, CA Performance Center, and an IdP that supports the SAML 2.0 standard, such as CA SiteMinder:



The following generic process describes how CA Performance Center supports SAML 2.0 authentication. Implementation-specific options, such as digitally signed certificates and transport binding, have been omitted:

1. A user attempts to access CA Performance Center, by navigating to http://mycapchost:8181/pc/desktop/page, for example.
2. CA Performance Center responds with a SAML request for authentication from the Identity Provider (IdP).
3. The browser processes the request and contacts the authentication software running on the IdP server.
4. The IdP determines whether the user has an existing logon security context—whether the user is already logged on.
5. If the user is not logged on, the IdP authenticates the user with an implementation-specific method.

   For example, the IdP might interact with the browser to challenge the user to provide credentials. This stage of the authentication is irrelevant to CA Single Sign-On.

6. The IdP builds and sends a SAML assertion representing the user's logon security context to the browser.

   The assertion includes a required attribute, subjectNameId, and an optional attribute, ClonedUser.

   The value of subjectNameId corresponds to the authorized user.

   You can include the name of the cloned user account in the assertion. This attribute defines the user account to which authorized SAML users are mapped.

7. The browser sends the SAML assertion to CA Performance Center.

8. CA Performance Center obtains the assertion and processes it.

9. If the assertion is valid, CA Performance Center establishes a session for the user. The browser redirects to the target page, the Home dashboard page for the user.

How to Set Up SAML Authentication

To enable SAML 2.0 authentication in Single Sign-On, the administrator must perform the following procedures:

1. Following the guidelines specific to the Identity Provider (IdP), create a metadata file that establishes the agreement between the IdP and Single Sign-On.

   For more information, see Prepare the IdP Agreement (see page 43).

2. (Optional) Create a properties file to enable digital signatures and encryption for communications between the IdP and servers running CA software.

   For more information, see Preparing the Security Properties File (see page 43).

3. Use the Single Sign-On Configuration Tool to set parameters for SAML Authentication.

   For more information, see Configure SAML Support in Single Sign-On (see page 44).

4. Set parameters on the IdP server. For example, add all data source product websites that support SAML to the list of trusted sites.

   For more information, see Configure the IdP (see page 48).

5. Update user accounts in CA Performance Center Administration to add an instruction to use external authentication.

   For more information, see Complete SAML Setup (see page 50).

Preparing the IdP Agreement

A metadata file in XML format is required to establish the agreement between the IdP and the Service Provider. In this case, CA Performance Center and all registered data sources that support SAML 2.0 require this agreement. The metadata file describes the IdP and contains information about the profiles it supports. This file also contains data about the services that it requires from the Service Provider.

Single Sign-On can import this file to set up the relationship with the IdP.

Some types of IdP, such as CA SiteMinder, provide utilities to help you create these files and export them. Or they create the agreement automatically, based on the parameters you set.

Consult the documentation for your IdP to perform this task.

Preparing the Security Properties File

If you plan to use encryption and digital certificates for communications between CA Performance Center and the IdP, a properties file is required. In this file, you specify the certificate to use for signing and encryption and other parameters to enable the encryption.

The SAML properties file is saved in the Single Sign-On home directory:
`/opt/CA/PerformanceCenter/sso/webapps/sso`

For example, a file like this is required:
`/opt/CA/PerformanceCenter/sso/webapps/sso/configuration/saml.properties`

The properties file must include the following parameters:

- Directory location and filename of the signing certificate.
- Verification certificate alias and password to access the certificate.
- Hostname of the CA Performance Center server.
- Directory location and filename of the agreement that you exported from the IdP.
- The length of the timeout period that is set on the IdP. The value must match the 'SAML2 IdP Session Timeout' parameter in Single Sign-On.

Here is an example of the syntax:

```
# Location of the certificate used for signing SAML documents
saml.sp.certificate.location=/opt/CA/saml2configuration/[Certificate filename]
saml.sp.certificate.password=[password]
saml.sp.certificate.alias=[alias]

saml.sp.metadata.hostname=[Full Hostname of CA Performance Center server]
saml.sp.metadata.entityID=[Name of the CA Performance Center server without IP
domain]
saml.sp.metadata.organizationName=[Name of your organization]
saml.sp.metadata.contactPerson=[First and last name of administrator]
saml.sp.metadata.email=[Email address of contact person]

# Location of the metadata file for the Login Site
saml.idp.metadata.file=/opt/CA/saml2configuration/[Filename].xml
# Session timeout with the IdP in minutes. Use this value for auto-reauthentication
and logout requests
saml.idp.sessionTimeout=[Length of timeout period in minutes]
```

Whenever you modify the saml.properties file, export the metadata file (which establishes the agreement with the IdP) again. For more information, see Configure SAML 2.0 Support in Single Sign-On (see page 44). You must also restart Single Sign-On.

Configure SAML 2.0 Support in Single Sign-On

The CA Performance Center administrator must set parameters for SAML authentication using the Single Sign-On Configuration Tool. Take these steps on all servers where a data source is installed whose users will authenticate using SAML 2.0.

Note: Multiple authentication schemes can be in use simultaneously. For example, users of a CA Network Flow Analysis data source can use LDAP to log in, while users of CA Infrastructure Management are using SAML 2.0.

Follow these steps:

1. Log in to the server where CA Performance Center or a CA data source product is installed.

   Log in as root or with the 'sudo' command.

2. Launch the Single Sign-On Configuration Tool by running the './SsoConfig' command in the following directory:

   InstallationDirectory/CA/PerformanceCenter

   You are prompted to select an option. The available options correspond to CA applications running on the local server.

3. Use the following commands as needed while you are selecting settings:
   - q (quit)
   - b (go back to the previous menu)
   - u (update)
   - r (reset)
4. Enter the value that corresponds to the data source that you want to configure. For example, enter 1 to configure CA Performance Center.

   You are prompted to select an option.
5. Enter 2 for SAML Authentication.

   You are prompted to specify the priority.

   The Priority parameter only applies to CA Performance Center.
6. Enter one of the following options:

   1. Remote Value

   Refers to settings that only administrators can change. Such settings are propagated to all other CA products registered to this instance of CA Performance Center. Remote Value settings are only used if a corresponding Local Override value is not present.

   2. Local Override

   Refers to settings that can be changed for all products. If a Local Override value is present, it takes precedence over both the Remote Value and default settings.

   You are prompted to select a property to configure.

   To supply values for the SAML2 properties, enter u to update the value and then enter a new value.
7. Enter 1 to select the 'Enable SAML2 Authentication' parameter.

   You are prompted to select an option.

8. Enter u to change the value, and enter 1 to enable SAML 2.0 authentication.
9. Enter 2 to set the 'Clone Default User Accounts' parameter.

   2. Clone Default User Accounts

   Defines the user account to which authorized SAML users are mapped. The role and product privileges that are associated with the user account you specify are applied to all users who successfully authenticate.

   Default: Blank.

   Example: Enter 'user' if you want all users to log in with user-level privileges.

   Note: An existing user account is required.

   The user accounts configured on the IdP are sent to CA Performance Center when the agreement is established. They appear in the User List on the Manage Users Admin page, where they can be edited.
10. Enter 3 to enable security parameters.

    3. SAML2 Signature and Encryption Enabled

    Enables security and encryption for communications between CA Performance Center and the IdP.

    Default: Disabled

    You are prompted to choose an option.
11. Enter u to change the value, and enter 1 to enable it.

    Note: This setting must match the setting on the IdP.
12. Enter 4 to enable automatic reauthentication.

    4. SAML2 Auto-Reauthentication

    Specifies whether users are required to reauthenticate after a timeout period expires. Enable this parameter to allow the IdP to perform a passive reauthentication ('auto-reauthentication'), with no user interaction.

    The next parameter lets you set the duration of the timeout period.

    Default: Disabled.
13. Enter u to change the value, and enter 1 to enable it.
14. Enter 5 to set the reauthentication timeout period.

    5. Auto-Reauthentication Time Period

    Sets the length of time that passes before a passive reauthentication is performed. If the 'SAML2 Auto-Reauthentication' parameter is disabled, this parameter is ignored.

    Value: Must be less than the value for the 'IdP Session Timeout' parameter.

    Default: None.

15. Enter u to change the value, and enter a new value.
16. Enter 6 to set a timeout period for the session to the Identity Provider.

    6. IdP Session Timeout

    Sets the length of time that passes before the session established between CA Performance Center and the Identity Provider is closed automatically. For example, enter '10' to set a 10-minute timeout.

    The value must be greater than the value specified for the 'Auto-Reauthentication Duration' parameter. Otherwise, no session exists to perform the reauthentication. And the value must match the value set in the security properties file for the 'saml.idp.sessionTimeout' parameter. For more information, see Preparing the Security Properties File (see page 43).

    Default: None.
17. Enter u to change the value, and enter a new value.
18. Enter b twice to go back to the initial prompt.
19. Enter 6 to export the metadata file that establishes the agreement with the IdP.

    The metadata file supplies the identity provider with the parameters to use when authenticating users.

    You are asked to supply a directory path and filename.
20. Enter the filename. For example, enter the following:

    ```
    /tmp/CAPCMetadata.xml
    ```

    The file is generated automatically, based on the settings you selected in the Configuration Tool.

    You see a printout of the XML if the export operation succeeds. If the operation fails, you see an error message.
21. Enter q to quit.

    The Configuration Tool closes.

Configure the IdP

To begin using SAML 2.0 for user authentication in CA Performance Center, set some parameters on the identity provider (IdP). Any IdP that supports the SAML 2.0 standard should work, but CA has only tested with CA SiteMinder.

You can manually configure the IdP, or you can import the IdP agreement from the Single Sign-on server.

Manually Configure the IdP

Follow these steps:

1. Enable the SAML2 authentication mode on the IdP.
2. Provide a URL for the assertion consumer service, which is running on the servers where Single Sign-On is installed. For example:

   `http://MyServerName:8381/sso/saml2/UserAssertionService`

   where 8381 is the port that Single Sign-On uses.
3. Set the binding method to 'HTTP-Redirect'.

   Note: HTTP Redirect is the only binding method that Single Sign-On supports.
4. Provide URLs for the single logout service.

   The logout service and the response location are both required. These services are running on the server where Single Sign-On is installed.

   Use the following examples:

   `http://MyServerName:8381/sso/saml2/LogoutService`
   `http://MyServerName:8381/sso/saml2/LogoutServiceResponse`
5. Add all data source product websites that support SAML 2.0 to the list of trusted sites.

   This step can involve adding these websites to a list of federation partnership entities.
6. (*Optional*) Verify digital signature and encryption settings. You must also configure these settings in Single Sign-On.

Import the IdP Agreement File

Follow these steps:

1. Import the IdP agreement file from its location on the Single Sign-On server.

   You exported this file after you completed other setup steps using the Single Sign-On Configuration Tool. For more information, see Configure SAML Support in Single Sign-On (see page 44).

2. Add all data source product websites that support SAML 2.0 to the list of trusted sites.

   This step can involve adding these websites to a list of federation partnership entities.

3. (*Optional*) Verify digital signature and encryption settings. You must also configure these settings in Single Sign-On.

Troubleshooting

Problem:

You see the following error message after configuring SAML:

```
RelayState is either null or a blank string. RelayState must be set
for SSO to work correctly.

Invalid syntax, RelayState=<value>

RelayState does not have parameter SsoRedirectUrl,
RelayState=<value>
```

Reason:

Some IdPs do not return the RelayState= value that CA Performance Center sends to the IdP during authentication verification.

Resolution:

Manually configure RelayState for your IdP. Use the following syntax:

```
SsoProductCode=pc&SsoRedirectUrl=http://[assign the value for
CAPC in your book]:8181/pc/desktop/page
```

Note: For secure communications, replace http: with https:, and replace the port number.

Completing SAML 2.0 Setup

To enable SAML 2.0 authentication, edit user accounts to use External Authentication. New user accounts in CA Performance Center are set to use Performance Center Authentication by default. The administrator must update the accounts of all operators who authenticate using SAML 2.0.

During SAML2.0 configuration, you specify an existing CA Performance Center user account to be 'cloned' in the IdP. Any users who are already defined on the IdP receive the same level of product privilege as the user account you designate. These accounts are also propagated to CA Performance Center, where they appear as new users in the User List. In many cases, you must edit these accounts to make sure that these users can access only the data they require to do their jobs.

Follow these steps:

1. Log in to CA Performance Center as a user with administrative privileges.
2. Select Admin, User Settings, and click Users.

   The Manage Users page opens.
3. Select a user account to edit.
4. Click Edit.

   The Edit User wizard opens.
5. Select 'External' as the Authentication Type.
6. Use the wizard to make any other desired changes to the user account. For example, advance to the third wizard dialog to select a different Product Privilege for this user.
7. Click Save.

   The changes to the user account are saved.

Chapter 4: Using HTTPS with Single Sign-On

This section contains the following topics:

Secure Sockets Layer (SSL) Encryption: HTTPS

By default, Single Sign-On uses HTTP (Hyper Text Transfer Protocol) for communications between the user's browser and CA Performance Center. TLS (Transport Layer Security) and its predecessor, SSL (Secure Sockets Layer), are widely supported encryption protocols that secure data transmissions over the Internet. TLS and SSL can be used with HTTP to form HTTPS (HTTP-Secure). This guide uses *SSL* as a blanket term to mean "TLS and SSL."

You can enhance the security in your monitoring system by configuring Single Sign-On to use HTTPS instead of HTTP.

Configuring CA Single Sign-On to use HTTPS is optional. Before you can configure the Single Sign-On website to use HTTPS, you must obtain a server certificate. The team that creates and enforces security policies for your organization can probably assist you with these steps.

How to Set Up HTTPS for CA Single Sign-On

To enable SSL, several steps are required. First, install the certificates that validate the identity of the server. Second, change the database so that CA Performance Center properly redirects to the correct port and scheme for Single Sign-On, and the reverse. Finally, change the services for both CA Performance Center and Single Sign-On to reflect the new ports and schemes.

Two ports are important for these steps: the CA Performance Center port (which defaults to 8181) and the Single Sign-On port (which defaults to 8381). Port 8181 is the CA Performance Center connection port. If users require authentication, the server redirects them to Single Sign-On on port 8381, where they see the Login page. Once a user has successfully logged in, the server redirects that user back to the original URL at port 8181.

Therefore, you cannot use the same port in each configuration step. Otherwise, a conflict occurs between CA Performance Center and Single Sign-On.

To enable HTTPS for CA Performance Center and Single Sign-On, complete the following steps:

1. Obtain a server certificate and install it in the web server keystore (see page 52).
2. Use the Single Sign-On Configuration Tool to update the necessary properties (see page 57).
3. Set up HTTPS on the CA Performance Center console (see page 59).
4. Set up HTTPS in Single Sign-On (see page 61).
5. Stop and restart the services.

Set Up SSL Certificates

Before you can configure the Single Sign-On website to use HTTPS, you must obtain and install a private key and an associated public certificate. SSL can be used with either a self-signed certificate or a certificate that a trusted Certificate Authority has signed. The procedures are typically specific to an organization and the policies of its security team. However, these procedures provide some information to guide you.

Select the appropriate procedure for your situation:

- Generate and import a new certificate (see page 53).
- Import an existing certificate (see page 56).

Note: For more information about the keytool command that is used in these procedures, see the Java documentation on the Oracle website.

Generate and Import a Certificate

If you do not already have an SSL certificate, you can generate one using the keytool command. This procedure explains how to generate a self-signed certificate and install it in the keystore.

Follow these steps:

1. Run the following command:

   `cd installDirectory/PerformanceCenter/jetty/etc`

2. Create a backup of the existing jetty keystore file by renaming it using the following commands:

   `mv installDirectory/PerformanceCenter/jetty/etc/keystore installDirectory/PerformanceCenter/jetty/etc/keystore.bak`

   Important! You must remove the old keystore. If you do not, an error appears in later steps: "Keystore was tampered with, or password was incorrect."

3. Generate a private key and a public, self-signed certificate using the following command:

   `keytool -genkeypair -keystore keystore_file.ks -storepass storepasswd -keyalg RSA -keysize 2048 -keypass keypasswd -alias alias_name`

   storepasswd

   Specifies the password for the keystore.

   keypasswd

   Specifies the password for the private key within the keystore.

   Important! Remember these passwords—they cannot be recovered.

4. Export the self-signed certificate from the keystore using the following command:

   `keytool -exportcert -keystore keystore_file.ks -storepass storepasswd -alias alias_name -file filename.cer`

   alias

   Specifies an alias that can be used to refer to the keystore entry that will be created to contain the keys.

   filename.cer

   Determines the file to which the certificate is exported. We recommend using a full pathname that does not place the file in the current directory.

   Example: /tmp/capcCert.cer.

   Note: We recommend backing up the cacerts file before continuing.

5. Import the self-signed certificate into the java trusted certificates keystore using the following command:

   `keytool -importcert -keystore installDirectory/jre/lib/security/cacerts -storepass cacertspasswd -alias capcSelfSigned -file filename.cer`

   Note: The default password for the cacerts keystore is "changeit."

   cacertspasswd

   Specifies the password for the cacerts keystore.

   Default: changeit

   filename.cer

   The file to which the certificate was exported in a previous step.

6. Back up the cacerts file.

7. (Optional) For more security, change the password of the java trusted certificates keystore using the following command:

   `keytool -storepasswd -keystore installDirectory/jre/lib/security/cacerts`

   You are prompted to provide the existing password and the new password.

8. Verify that your imported keystore is available. Use the following command:

   `keytool -list -keystore installDirectory/jre/lib/security/cacerts`

   Important! To enable the web services, the self-signed certificate must be in the cacerts keystore. Otherwise, you see an error in the log that reports that PKIX did not find a certificate.

9. Restart each CA Performance Center service using these commands:

   `/sbin/service caperfcenter_sso restart`

   `/sbin/service caperfcenter_devicemanager restart`

   `/sbin/service caperfcenter_console restart`

   Your self-signed SSL certificate is generated and installed in the keystore.

Next steps:

- (Optional) Convert a Self-Signed Certificate to a Certification Authority SSL Certificate (see page 55)
- Configure the port and website to support HTTPS (see page 57)

Convert a Self-Signed Certificate to a Certification Authority SSL Certificate

A self-signed certificate prompts a browser warning when users open CA Performance Center. Users can manually dismiss the warning to continue. However, a certificate that a trusted Certification Authority has signed avoids the browser warning. The following procedure explains how to convert the self-signed certificate to a certificate that a trusted Certification Authority has signed.

Follow these steps:

1. Run the following command:

   `cd installDirectory/PerformanceCenter/jetty/etc`

2. Export a certificate signature request using the following command:

   `keytool -certreq -keystore keystore_file.ks -storepass storepasswd -alias alias_name -keypass keypasswd -file requestFileName.csr`

   r*equestFileName*.csr

   Determines the path and file name of the exported signature request.

3. Send the resulting file (*requestFileName*.csr) to a qualified signing authority, along with any other requested information.

   The Certificate Authority sends you a signed certificate (*signedCert*.cer). They might also provide a root Certificate Authority certificate (*rootCA*.cer) to authenticate the signed certificate.

4. (*Optional*) Determine whether the root Certificate Authority certificate is part of the default java trusted authorities using the following command:

   `keytool -list -v -keystore installDirectory/jre/lib/security/cacerts -storepass cacertspasswd`

5. (*Optional*) Search the output for the Certificate Authority that signed your certificate. If the Certificate Authority is not listed, add it to the list of trusted authorities using the following command:

   `keytool -importcert -keystore installDirectory/jre/lib/security/cacerts -storepass cacertspasswd -alias myRootCa -file rootCA.cer`

6. Import the signed certificate using the following command:

   `keytool -importcert -trustcacerts -keystore keystore -storepass storepasswd -alias alias_name -keypass keypasswd -file signedCert.cer`

7. Validate the contents of the jetty keystore using the following command:

   `keytool -list -keystore installDirectory/PerformanceCenter/jetty/etc/keystore`

   The single certificate that you imported appears in the list.

8. Restart each CA Performance Center service using these commands:

   `/sbin/service caperfcenter_sso restart`

   `/sbin/service caperfcenter_devicemanager restart`

   `/sbin/service caperfcenter_console restart`

   The Certificate Authority SSL certificate replaces your self-signed certificate in the keystore.

Next step: Configure the port and website to support HTTPS (see page 57).

Import a Key and an Existing Certificate

You can use a private key and public certificate (either a self-signed or a Certificate Authority certificate) from a different source. For example, your security team provides an SSL certificate that is customized for your organization. To use this SSL certificate, import the private key and the signed certificate.

Follow these steps:

1. Run the following command:

   `cd /opt/CA/PerformanceCenter/jetty-version/etc`

2. Remove the old keystore using the command:

   `rm keystore`

3. Create a PKCS#12 keystore from the private key and certificate using the following command:

   `openssl pkcs12 -export -in certificate.pem -inkey privatekey.pem -name MyAlias -out keystore.pkcs12`

   certificate.pem

   Specifies the certificate provided to you.

   privatekey.pem

   Specifies the private key provided to you.

   Note: This command works on Linux only.

4. Import the key and certificate into the CA Performance Center keystore using the following command:

   `keytool -importkeystore -destkeystore keystore_file -deststorepass storepasswd -srckeystore keystore.pkcs12 -srcstoretype pkcs12 -srcalias src_alias_name -destalias dest_alias_name -destkeypass keypasswd`

5. Restart each CA Performance Center service using these commands:

   ```
   /sbin/service caperfcenter_sso restart
   ```

   ```
   /sbin/service caperfcenter_devicemanager restart
   ```

   ```
   /sbin/service caperfcenter_console restart
   ```

   Your existing SSL certificate is imported into the keystore.

Next step: Configure the port and website to support HTTPS (see page 57).

Note: Import the certificate into the Java cacerts keystore if the certificate does not include a chain that terminates at a certificate in the keystore. Run the following command to determine whether the certificate includes the chain:

```
keytool -printcert -file filename
```

filename

Specifies the name of the certificate.

See Generate and Import a Certificate (see page 53) for instructions on importing a certificate into the Java cacerts keystore.

Configure the Port and Website for SSL

By default, Single Sign-On uses Port 8381. To set up HTTPS, use the Single Sign-On Configuration Tool to update the default website scheme and port to match the encryption settings.

Perform the tasks in this procedure on every server where a data source is installed.

Follow these steps:

1. Launch the Single Sign-On Configuration Tool by running the './SsoConfig' command in the following directory:

   InstallationDirectory/CA/PerformanceCenter

   You are prompted to select an option.

2. Use the following commands as needed while you are changing settings:
   - q (quit)
   - b (go back to the previous menu)
   - u (update)
   - r (reset)

3. Enter 1 to select CA Performance Center.

4. Enter 4 to configure Single Sign-On.

   You are prompted to specify the priority.

5. Enter one of the following options:

   1. Remote Value

   Refers to settings that only administrators can change. Such settings are propagated to all other CA products registered to this instance of CA Performance Center. Remote Value settings are only used if a corresponding Local Override value is not present.

   2. Local Override

   Refers to settings that can be changed for all products. If a Local Override value is present, it takes precedence over both the Remote Value and default settings.

   You are prompted to select a property to configure.

6. Enter 12 for the Scheme property.
7. Enter 'u' to update the value.
8. Supply 'https' for the value.
9. Enter 13 for the Port property.
10. Update the value to '8382'.
11. Enter 'b' twice to go back to the SSO Configuration/CA Performance Center menu.
12. Enter '3' to configure the Performance Center.

    You are prompted to specify the priority.

13. Enter either '1' for Remote Value or '2' for Local Override.
14. Enter '6' to select Web Site Scheme.
15. Update the value to 'https'.
16. Enter '8' to select Web Site Port.
17. Update the value to '8182'.
18. Enter q to quit.

Now you must configure CA Performance Center files to use HTTPS.

Configure CA Performance Center to Use HTTPS

You must edit some configuration files to reflect the new website and port settings. Edit the configuration files to replace the HTTP connector with an HTTPS connector. You must also restart the CA Performance Center services so that the changes take effect.

Follow these steps:

1. Change to the following directory:

   cd/*InstallationDirectory*/CA/PerformanceCenter/PC

2. Open the start.ini file for editing.

3. Find the following line and remove the '#' so that it is active:

   #/opt/CA/PerformanceCenter/PC/etc/jetty-ssl.xml

   where '/opt/CA' is the default installation directory.

4. Save start.ini.

5. Change to the following directory:

   cd/*InstallationDirectory*/CA/PerformanceCenter/PC/etc

6. Create a file named 'jetty-ssl.xml' in that directory with the following contents:

```
<?xml version="1.0"?>
<!DOCTYPE Configure PUBLIC "-//Jetty//Configure//EN"
"http://www.eclipse.org/jetty/configure.dtd">
<Configure id="Server" class="org.eclipse.jetty.server.Server">
  <Call name="addConnector">
    <Arg>
      <New class="org.eclipse.jetty.server.ssl.SslSelectChannelConnector">
         <Set name="Port">8182</Set>
         <Set name="maxIdleTime">30000</Set>
        <Set name="Keystore"><Property name="jetty.home" default="."
/>/etc/keystore</Set>
        <Set name="Password">***PASSWORD***</Set>
         <Set name="KeyPassword">***PASSWORD***</Set>
        <Set name="truststore"><Property name="jetty.home" default="."
/>/etc/keystore</Set>
        <Set name="trustPassword">***PASSWORD***</Set>
        <Set name="allowRenegotiate">true</Set>
      </New>
    </Arg>
  </Call>
</Configure>
```

7. Replace all instances of the “***PASSWORD***” value with the passwords in use in your system.

8. Save the file.

9. Open the file jetty.xml for editing.
10. Remove the following lines for the default HTTP connector:

```
<Call name="addConnector">
  <Arg>
      <New class="org.eclipse.jetty.server.nio.SelectChannelConnector">
          <Set name="host"><Property name="jetty.host" /></Set>
            <!-- Changed: Used to be Property -->
           <Set name="port"><SystemProperty name="jetty.port"
default="8181"/></Set>
           <Set name="maxIdleTime">300000</Set>
           <Set name="Acceptors">2</Set>
           <Set name="statsOn">false</Set>
           <Set name="confidentialPort">8443</Set>
           <Set name="lowResourcesConnections">20000</Set>
           <Set name="lowResourcesMaxIdleTime">5000</Set>
      </New>
  </Arg>
 </Call>
```

11. Save jetty.xml.
12. Change to the following directory:

    cd/*InstallationDirectory*/CA/PerformanceCenter/PC/conf

13. Edit the file wrapper.conf. In the following line, replace '8181' with '8182' so that it matches the port defined in jetty-ssl.xml, described previously:

    wrapper.java.additional.2=-Djetty.port=8181

14. Save wrapper.conf.
15. Change to the following directory:

    cd */InstallationDirectory*/CA/PerformanceCenter/sso/webapps/
    sso/configuration

16. Edit the file 'CAPerformanceCenter.xml'.
17. Replace the <Scheme> and <Port> values with settings appropriate for SSL:

```
<?xml version="1.0" encoding="utf-8" ?>
<Configuration>
     <SingleSignOnEnabled>True</SingleSignOnEnabled>
     <SingleSignOnProductCode>pc</SingleSignOnProductCode>
     <SignInPageProductDefaultUrl>
```

```
            <Scheme>https</Scheme>
            <Port>8182</Port>
            <PathAndQuery>/pc/desktop/page</PathAndQuery>
        </SignInPageProductDefaultUrl>
        <SingleSignOnWebServiceUrl>
            <Scheme>https</Scheme>
            <Port>8182</Port>
            <PathAndQuery>/pc/center/webservice/sso</PathAndQuery>
        </SingleSignOnWebServiceUrl>
</Configuration>
```

Update Single Sign-On Configuration and Restart the Services

Edit some startup files to support SSL encryption in Single Sign-On. You must also restart all CA Performance Center and Single Sign-On services to update the settings.

Follow these steps:

1. Change to the following directory:

   InstallationDirectory/CA/PerformanceCenter/sso

2. Open the start.ini file for editing.

3. Find the following line and remove the '#' so that it is active:

   ```
   #/opt/CA/PerformanceCenter/sso/etc/jetty-ssl.xml
   ```

   where '/opt/CA' is the default installation directory.

4. Save start.ini.

5. Change to the following directory:

   InstallationDirectory/CA/PerformanceCenter/sso/etc

6. Create a file named jetty-ssl.xml in that directory with the following contents:

   ```
   <?xml version="1.0"?>
   <!DOCTYPE Configure PUBLIC "-//Jetty//Configure//EN"
   "http://www.eclipse.org/jetty/configure.dtd">
   <Configure id="Server" class="org.eclipse.jetty.server.Server">
     <Call name="addConnector">
       <Arg>
         <New class="org.eclipse.jetty.server.ssl.SslSelectChannelConnector">
            <Set name="Port">8382</Set>
            <Set name="maxIdleTime">30000</Set>
   ```

```
        <Set name="Keystore"><Property name="jetty.home" default="."
/>/etc/keystore</Set>
        <Set name="Password">***PASSWORD***</Set>
        <Set name="KeyPassword">***PASSWORD***</Set>
       <Set name="truststore"><Property name="jetty.home" default="."
/>/etc/keystore</Set>
        <Set name="trustPassword">***PASSWORD***</Set>
        <Set name="allowRenegotiate">true</Set>
      </New>
    </Arg>
  </Call>
</Configure>
```

7. Replace all instances of the “***PASSWORD***” value with the passwords in use in your system.
8. Save jetty-ssl.xml.
9. Open the file jetty.xml.
10. Remove the following lines for the default HTTP connector:

```
<Call name="addConnector">
  <Arg>
      <New class="org.eclipse.jetty.server.nio.SelectChannelConnector">
          <Set name="host"><Property name="jetty.host" /></Set>
            <!-- Changed: Used to be Property -->
           <Set name="port"><SystemProperty name="jetty.port"
default="8181"/></Set>
           <Set name="maxIdleTime">300000</Set>
           <Set name="Acceptors">2</Set>
           <Set name="statsOn">false</Set>
           <Set name="confidentialPort">8443</Set>
           <Set name="lowResourcesConnections">20000</Set>
           <Set name="lowResourcesMaxIdleTime">5000</Set>
      </New>
  </Arg>
 </Call>
```

11. Save jetty.xml.
12. Change to the following directory:

    InstallationDirectory/CA/PerformanceCenter/sso/conf
13. Edit the file wrapper.conf. In the following line, replace '8381' with '8382' so that it matches the port defined in jetty-ssl.xml, described previously:

```
wrapper.java.additional.2=-Djetty.port=8381
```

14. Save wrapper.conf.

15. Stop the console, device manager, and SSO services by entering the following commands:

    ```
    service caperfcenter_console stop

    service caperfcenter_devicemanager stop

    service caperfcenter_sso stop
    ```

16. Restart the services by entering the following commands

    ```
    service caperfcenter_sso start

    service caperfcenter_devicemanager start

    service caperfcenter_console start
    ```

Chapter 5: Troubleshooting

This section contains the following topics:

Browser Shows Error

Symptom:

When I entered my password on the Login page, I was redirected to an error page in the web browser. Did I type the wrong password?

Solution:

This symptom does not indicate that you entered the wrong SAML credentials. Instead, the browser error (such as 401 or 500) indicates that Single Sign-On redirected the browser to the login URL, but the Identity Provider (IdP) server is down.

Take the following steps:

- Verify that the IdP server is running.
- Test the network connection between the CA Performance Center server and the IdP server.

Logs

By checking your log files daily or weekly, you can resolve problems before they affect normal operations. All logs are stored in subfolders that correspond to a service (or daemon). Find log files in the following path:

`CA/PerformanceCenter/`*`servicename`*`/logs`

Replace the *servicename* parameter with one of the following service names:

DM

The Device Manager.

- DMService.log – Output from the Device Manager, primarily related to synchronization.
- wrapper.log – caperfcenter_devicemanager process logging.

EM

The Event Manager.

- EMService.log – Output from the Event Manager; includes details of events and alarms.
- wrapper.log – caperfcenter_eventmanager process logging.

PC

The main console program.

- PCService.log – CA Performance Center-related logging; comprises user interface and view components.
- wrapper.log – caperfcenter_console process logging.

SSO

The Single Sign-On authentication software.

- SSOService.log – Single Sign-On logging, including HTTPS (Secure Sockets Layer) information where HTTPS has been configured.
- wrapper.log – caperfcenter_sso process logging.

For problems with the Single Sign-On Configuration Tool, check the application log in the following location:

`/opt/CA/PerformanceCenter/sso/logs/application.log`

Log filenames include the relevant date and time.

New log files are generated automatically each day. Older log files are removed automatically after 14 days to avoid consuming excessive disk space.

Access the most recent log file to find errors associated with the database or data source synchronization. You can start by opening the Events dashboard from the Dashboards tab and sorting by Status. If you want to look at the related log file, note the event type and failure date and time. In the log directory, open the log file with the corresponding date in the filename.

Check the Audit Log

Single Sign-On supports security auditing by logging daily details about user login activity to a file. Check the log to verify user activity.

Follow these steps:

1. Log in to the server where a CA data source product is installed.
2. Open a command prompt, and cd to the following directory:

   `[InstallationDirectory]/PerformanceCenter/sso/logs`

   Note: The audit log is saved in the following location on Windows servers: `[InstallationDirectory]\Portal\SSO\logs.`
3. Enter dir to see the contents of the directory.

   The filename of the log file is SingleSignOnAuditLogyyyy-mm-dd.log.
4. Enter the name of the audit file you want to view.

   The file opens in the local text editor application.

Glossary

Configuration Tool

The *Configuration Tool* is a command-line application that lets administrators adjust the settings used by the Single Sign-On website and the associated CA data source products.

Identity Provider (IdP)

The *Identity Provider*, or IdP, stores identity or security information and provides it when requested for authentication purposes. Also called the "asserting party," one of the three component roles required for SAML authentication.

LDAP

LDAP (Lightweight Directory Access Protocol) is a protocol that specifies methods for searching and editing directories and storing directory information in IP networks. In addition, LDAP is often used to secure network access because it includes an authentication component. LDAP directories are typically organized into logical groups of units. Microsoft Active Directory is a prominent example of a directory application that uses LDAP.

SAML

The Security Assertion Markup Language (*SAML*) is a security protocol that is based on XML. The basic concept involves the exchange of security assertions about a subject—a person or a computer—that is requesting access to a secure domain. Assertions include whether the subject can access certain resources, and whether an external data source, such as a policy store, is used.

Single Sign-On

Single Sign-On is the authentication scheme for CA Performance Center and all supported data sources. Once they are authenticated to CA Performance Center, users can navigate among the console and registered data sources without signing in a second time.

SSL

SSL (Secure Sockets Layer) is an encryption protocol that many web browsers support for data security over the Internet. Servers exchange SSL certificates that contain a public key to encrypt the data that is exchanged and a private key to decipher it. SSL lets a web browser specify the level of encryption to use based on browser, client computer, and server capabilities. The maximum level is 256-bit encryption, the most difficult to decipher.

TLS

TLS (Transport Layer Security), and its predecessor, SSL (Secure Sockets Layer), are widely supported encryption protocols that secure data transmissions over the Internet. SSL/TLS can be used in conjunction with HTTP to form HTTPS (HTTP-Secure).

Index