CA SiteMinder®

Directory Configuration - OpenLDAP

r6.0 SP6

CA Product References

This document references the following CA products: CA SiteMinder®.

Contact CA

Contact CA Support

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

- 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

Provide Feedback

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

If you would like to provide feedback about CA product documentation, complete our short customer survey, which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Configuring an OpenLDAP Directory Server

This section contains the following topics:

How to Configure the Slapd Configuration File

An OpenLDAP directory server requires additional configuration before you can use it as a policy store. The following process lists the configuration steps:

1. Specify the SiteMinder schema files.
2. Enable user authentication.
3. Specify database directives.
4. Test the configuration file.
5. Restart the OpenLDAP server.

Specify the SiteMinder Schema Files

Specifying the schema files in the include section of the slapd configuration file (slapd.conf) ensures that the slapd process (the LDAP Directory Server daemon) reads the additional configuration information. The included files must follow the correct slapd configuration file format.

To specify the schema files

1. Copy the following schema files to the schema folder in the OpenLDAP installation directory:
   - *path*/openldap/openldap_attribute.schema
   - *path*/openldap/openldap_object.schema
   - *path*/xps/openldap/openldap_attribute_XPS.schema
   - *path*/xps/openldap/openldap_object_XPS.schema

   path

   Specifies the path to the schema files extracted from the tier 2 directory zip.

2. Type the following in the include section of the slapd configuration file:

```
....
.....
include /usr/local/etc/openldap/schema/openldap_attribute.schema
include /usr/local/etc/openldap/schema/openldap_object.schema
include /usr/local/etc/openldap/schema/openldap_attribute_XPS.schema
include /usr/local/etc/openldap/schema/openldap_object_XPS.schema
```

Note: This procedure assumes that the OpenLDAP server is located at /usr/local/etc/openldap and that the schema files are located in the schema subdirectory.

The policy store schema is created for r6.0 SP6.

Enable User Authentication

Enabling user authentication ensures that you can protect resources with a supported authentication scheme.

To enable user authentication, add the following to the slapd configuration file:

```
access to attr=userpassword
by self write
by anonymous auth
by * none
```

Specify Database Directives

The slapd configuration file requires values for additional database directives.

To specify the directives, edit the following:

database

Specify any supported backend type.

Example: bdb

suffix

Specify the database suffix.

Example: dc=example,dc=com

rootdn

Specify the DN of root.

Example: cn=Manager,dc=example,dc=com

rootpw

Specify the password to root.

directory

Specify the path of the database directory.

Example: /usr/local/var/openldap-data

Note: The database directory must exist prior to running slapd and should only be accessible to the slapd process.

Test the Configuration File

Testing the configuration file ensures that it is correctly formatted.

To test the configuration file

1. Change the directory to the OpenLDAP server directory.
2. Run the following command:

   ```
   ./slapd
   ```

   Note: Unless you specified a debugging level, including level 0, slapd automatically forks, detaches itself from its controlling terminal, and runs in the background.
3. Run the following command:

   ```
   ./slapd -Tt
   ```

   The slapd configuration file is tested.

Restart the OpenLDAP Server

Restarting the OpenLDAP directory server loads the SiteMinder schema. The Policy Server requires that the SiteMinder schema is loaded before you can use the directory server as a policy store.

To restart the directory server

1. Stop the directory server using the following command:

   ```
   kill ?INT 'cat path_of_var/run_directory/slapd.pid'
   ```

   path_of_var/run_directory

   Specifies the path of the database directory.

   Example: kill ?INT 'cat /usr/local/var/run/slapd.pid'
2. Start the directory server using the following command:

   ```
   ./slapd
   ```

How to Create the Database

The following process lists the steps for creating the directory server database for the policy store:

1. Create the base tree structure.
2. Add entries.

Create the Base Tree Structure

You create the base tree structure to hold the policy store data.

To create the base tree structure, enter the following under the root DN:

```
ou=PolicySvr4,ou=SiteMinder,ou=Netegrity
```

Add Entries

Add entries to the directory server so that SiteMinder has the necessary organization and organizational role information.

To add database entries

1. Create an LDIF file.

   Example: The following example contains an organization entry and an organizational role entry for the entries.ldif.

   ```
   # Organization for example.com
   dn: root_DN (example.com)
   objectClass: dcObject
   objectClass: organization
   dc: example
   o: Example Corporation

   # Organizational Role for Directory Manager
   dn: cn=Manager,root_DN
   objectClass: organizationalRole
   objectClass: top
   cn: Manager
   description: Directory Manager
   ```

2. Use the following command to add the entries.

   ```
   ldapadd -<file_name.ldif>
   -D "cn=Manager,dc=example,dc=com" -w<password>
   ```

How to Configure the Directory Server as a Policy Store

You can use the Policy Server Management Console and the Policy Server User Interface to configure the directory server as a policy store. The following process lists the steps for using the directory server as a policy store:

1. Create the Policy Store
2. Connect to the Policy Store

Create the Policy Store

Using the directory server as a policy store requires that you point SiteMinder to the root DN under which the base tree structure was created.

Important! Before running a SiteMinder utility or executable on Windows Server 2008, open the command line window with Administrator permissions. Open the command line window this way, even if your account has Administrator privileges. For more information, see the release notes for your SiteMinder component.

To create the policy store

1. Start the Policy Server Management Console.
2. Click the Data tab.

   The Data tab opens.
3. Type the *root_DN* in the Root DN field, and click OK.

   SiteMinder saves the root DN.
4. Run the following from <*siteminder_installation_path*>/bin:

   `smreg -su <password>`

   Note: You can run smreg from any location if the path was previously set.

   SiteMinder sets the administrator password.
5. Run the following:

   `smobjimport -ismpolicy.smdif -dSiteminder -w<password> -v`

   SiteMinder imports the base policy store data into OpenLDAP.

Connect to the Policy Store

To connect an OpenLDAP directory server to the policy store, see Configuring Policy Servers to Use an LDAP Policy Store or Key Store in the *Policy Server Installation Guide*.

How to Configure the Directory Sever as a User Store

You can use the OpenLDAP directory server as a user store. The following process lists the steps for using the directory server as a user store:

1. Create a User Store
2. Connect to the User Store

Create a User Store

You can use an OpenLDAP directory server as a user store

To create a user store

1. Use an LDIF file to create ou=People under the root DN.
2. Create users under the organizational unit.

Connect to the User Store

You must configure the Policy Server to use an OpenLDAP user directory.

Note: The following procedure assumes you are logged into the Policy Server User Interface.

To connect the user store

1. Click Edit, System Configuration, Create User Directory.

   The User Directories Properties dialog appears with the Directory Setup tab open.

2. Complete the following:
   - Type the *server IP address and port number* in the Server field.
   - Type the *root DN* in the Root field.
   - Type the *search criteria* in the Start field.
3. Click the Credentials and Connection tab.

   The Credentials and Connection tab opens.

4. Complete the following:
   a. Select Require Credentials
   b. Type the *full dn of the administrator* in the Username field.

      Example: cn=Manager, dc=example, dc=com

   c. Type the *administrator password* in the Password and Confirm Password fields.

5. Click the User Attributes tab.

   The User Attributes tab opens.

6. Type the names of the *user profile attributes* that SiteMinder is to use, and click OK.

   SiteMinder saves the user directory settings, and the user directory appears in the User Directory List.

Chapter 2: Troubleshooting

This section contains the following topics:

Cyrus SASL Installation

Symptom:

When I install Cyrus SASL, I am experiencing compiling problems.

Solution:

More information on troubleshooting Cyrus SASL installation problems can be found at:

http://marc.theaimsgroup.com/?l=cyrus-sasl&m=111835942621184&w=2

Berkeley Database Version Mismatch Errors

Symptom:

I am receiving Berkeley database version mismatch errors.

Solution:

More information on troubleshooting Berkeley database version mismatch errors can be found at:

http://www.openldap.org/faq/data/cache/1113.html

Building and Installing openSSL

Symptom:

I am having problems building and installing openSSL.

Solution:

More information on building and installing openSSL can be found at:

http://www.proscrutiny.com/howtos/OpenLDAP.html#confssl-co

Appendix A: Configuring SiteMinder Connections over SSL

This section contains the following topics:

How to Configure an LDAP User Directory Connection over SSL

Configuring an LDAP user directory connection over SSL requires that you configure SiteMinder to use your certificate database files.

Complete the following steps to configure the connection over SSL:

1. Before you configure a connection over SSL.
2. Install the NSS utility.
3. Create the certificate database files.
4. Add the root Certificate Authority (CA) to the certificate database.
5. Add the server certificate to the certificate database.
6. List the certifications in the certificate database.
7. Configure the user directory connection for SSL.
8. Point the Policy Server to the certificate database.
9. Verify the SSL connection.

Before You Configure a Connection over SSL

Review the following before configuring an LDAP user directory connection over SSL:

- Ensure your directory server is SSL-enabled.

  Note: For more information on configuring your directory server to communicate over SSL, refer to the vendor-specific documentation.

- SiteMinder uses a Netscape LDAP SDK to communicate with LDAP directories. As a result, SiteMinder requires that the database files be in a Netscape version file format (cert7.db).

  Important! Do not use Microsoft Internet Explorer to install certificates into your cert7.db database file.

- A third-party certificate utility, which is compatible with Netscape, is required to manage your SSL certificates. We recommend the Mozilla® Network Security Services (NSS) utility, version 3.2.2.

  Note: Version 3.2.2 is required to support the cert7.db format. Do not use later versions.

- (Active Directory) Considering the following:
  - If the SiteMinder user directory connection was configured with the AD namespace, the following process does not apply. The AD namespace uses the native Windows certificate repository when establishing an SSL connection. When configuring the AD namespace to communicate over SSL:
    - Ensure that the SiteMinder user directory connection is configured for a secure connection. For more information, refer to Configure the User Directory Connection for SSL (see page 24).
    - On the machine hosting the Active Directory instance, ensure that the root CA certificate and the server certificate are added to the services' certificate store.

    Note: For more information on configuring Active Directory to communicate over SSL, refer to the Microsoft documentation.
  - If the SiteMinder user directory connection was configured with the LDAP namespace, complete the following process to configure the connection over SSL.

Install the NSS Utility

You install the NSS utility to manage your certificate database files.

Note: Install the utility on a system to which the Netscape Portable Runtime (NSPR) or the Policy Server is installed. Installing the utility to a system with either component ensures that the necessary DLLs or shared objects are available.

To install the NSS utility

1. Access the Mozilla NSS 3.2.2 FTP site.
2. Download the respective zip or tar for your operating system.

   Note: A zip is not available for Windows Server 2003. Download the zip for Windows NT.
3. Extract the NSS utility to a temporary location on the system to which you are managing your certificate database files.

Create the Certificate Database Files

The Policy Server requires that the certificate database files be in the Netscape version file format (cert7.db). You may use the NSS utility to create the certificate database files.

Note: The following procedure details the specific options and arguments to complete the task. For a complete list of the NSS utility options and arguments, refer to the Mozilla documentation on the NSS project page.

To create the certificate database files

1. From a command prompt, navigate to the bin directory in the location to which you extracted the NSS utility.

   Example: C:\nss\bin

   Note: Windows has a native certutil utility. Ensure you are working from the bin directory of the NSS utility or you may inadvertently run the Windows certutil utility.

2. Enter the following command:

   `certutil -N -d certificate_database_directory`

   -N

   Creates the cert7.db, key3.db, and secmod.db certificate database files.

   -d *certificate_database_directory*

   Specifies the directory to which the NSS utility is to create the certificate database files.

   Note: If the file path contains spaces, bracket the path in quotes.

   The utility prompts for a password to encrypt the database key.

3. Enter and confirm the password.

   NSS creates the required certificate database files:

   - cert7.db
   - key3.db
   - secmod.db

Example: Create the Certificate Database Files

```
certutil -N -d C:\certdatabase
```

Add the Root Certificate Authority to the Certificate Database

You add the root Certificate Authority (CA) to make it available for communication over SSL.

Note: The following procedure details the specific options and arguments to complete the task. For a complete list of the NSS utility options and arguments, refer to the Mozilla documentation on the NSS project page.

Important! Before running a SiteMinder utility or executable on Windows Server 2008, open the command line window with Administrator permissions. Open the command line window this way, even if your account has Administrator privileges. For more information, see the release notes for your SiteMinder component.

To add the root CA certificate to the certificate database

1. From a command prompt, navigate to the bin directory in the location to which you extracted the NSS utility.

   Example: C:\nss\bin

   Note: Windows has a native certutil utility. Ensure you are working from the bin directory of the NSS utility or you may inadvertently run the Windows certutil utility.

2. Run the following command to add the root CA to the database file:

   `certutil -A -n alias -t trust_arguments -i root_CA_path -d certificate_database_directory`

   -A

   Adds a certificate to the certificate database.

   -n *alias*

   Specifies an alias for the certificate.

   Note: If the alias contains spaces, bracket the alias with quotes.

   -t *trust_arguments*

   Specify the trust attributes to apply to the certificate when adding it to the certificate database. There are three available trust categories for each certificate, which are expressed in this order: "SSL, email, object signing". Specify the appropriate trust arguments so that the root CA is trusted to issue SSL certificates. In each category position, you may use zero or more of the following attribute arguments.

   p

   Valid peer.

   P

   Trusted peer. This argument implies p.

c

Valid CA.

T

Trusted CA to issue client certificates. This argument implies c.

C

Trusted CA to issue server certificates (SSL only). This argument implies c.

Important! This is a required argument for the SSL trust category.

u

Certificate can be used for authentication or signing.

-i *root_CA_path*

Specifies the path to the root CA file. Consider the following:

- The path must include the certificate name.
- Valid extensions for a certificate include .cert, .cer, and .pem.

Note: If the file path contains spaces, bracket the path in quotes.

-d *certificate_database_directory*

Specifies the path to the directory that contains the certificate database.

Note: If the file path contains spaces, bracket the path in quotes.

NSS adds the root CA to the certificate database.

Example: Adding a Root CA to the Certificate Database

```
certutil -A -n "My Root CA"  -t "C,," -i C:\certificates\cacert.cer -d C:\certdatabase
```

Add the Server Certificate to the Certificate Database

You add the server certificate to the certificate database to make it available for communication over SSL.

Note: The following procedure details the specific options and arguments to complete the task. For a complete list of the NSS utility options and arguments, refer to the Mozilla documentation on the NSS project page.

Important! Before running a SiteMinder utility or executable on Windows Server 2008, open the command line window with Administrator permissions. Open the command line window this way, even if your account has Administrator privileges. For more information, see the release notes for your SiteMinder component.

To add the server certificate to the certificate database

1. From a command prompt, navigate to the bin directory in the location to which you extracted the NSS utility.

   Example: C:\nss\bin

   Note: Windows has a native certutil utility. Ensure you are working from the bin directory of the NSS utility or you may inadvertently run the Windows certutil utility.

2. Run the following command to add the root certificate to the database file:

   `certutil -A -n alias -t trust_arguments -i server_certificate_path -d certificate_database_directory`

   -A

   Adds a certificate to the certificate database.

   -n *alias*

   Specifies an alias for the certificate.

   Note: If the alias contains spaces, bracket the alias with quotes.

   -t *trust_arguments*

   Specify the trust attributes to apply to the certificate when adding it to the certificate database. There are three available trust categories for each certificate, which are expressed in this order: "SSL, email, object signing". Specify the appropriate trust arguments so that the certificate is trusted. In each category position, you may use zero or more of the following attribute arguments:

   p

   Valid peer.

   P

   Trusted peer. This argument implies p.

   Important! This is a required argument for the SSL trust category.

   -i *server_certificate_path*

   Specifies the path to the server certificate. Consider the following:

   - The path must include the certificate name.
   - Valid extensions for a certificate include .cert, .cer, and .pem.

   Note: If the file path contains spaces, bracket the path in quotes.

-d *certificate_database_directory*

Specifies the path to the directory that contains the certificate database.

Note: If the file path contains spaces, bracket the path in quotes.

NSS adds the server certificate to the certificate database.

Example: Adding a Server Certificate to the Certificate Database

```
certutil -A -n "My Server Certificate" -t "P,," -i C:\certificates\servercert.cer -d
C:\certdatabase
```

List the Certificates in the Certificate Database

You list the certifications to verify that they were added to the certificate database.

Note: The following procedure details the specific options and arguments to complete the task. For a complete list of the NSS utility options and arguments, refer to the Mozilla documentation on the NSS project page.

Important! Before running a SiteMinder utility or executable on Windows Server 2008, open the command line window with Administrator permissions. Open the command line window this way, even if your account has Administrator privileges. For more information, see the release notes for your SiteMinder component.

To list the certifications in the certificate database

1. From a command prompt, navigate to the bin directory in the location to which you extracted the NSS utility.

   Example: C:\nss\bin

   Note: Windows has a native certutil utility. Ensure you are working from the bin directory of the NSS utility or you may inadvertently run the Windows certutil utility.

2. Run the following command:

   ```
   certutil -L -d certificate_database_directory
   ```

   -L

   Lists all of the certificates in the certificate database.

   -d *certificate_database_directory*

   Specifies the path to the directory that contains the certificate database.

   Note: If the file path contains spaces, bracket the path in quotes.

NSS displays the root CA alias, the server certificate alias, and the trust attributes you specified when adding the certificates to the certificate database.

Example: List the Certificates in the Certificate Database

```
certutil -L -d C:\certdatabase
```

Configure the User Directory Connection for SSL

You configure the user store connection to ensure that an SSL connection is used when the Policy Server and user store communicate.

Note: When you create or modify a Policy Server object in the Policy Server User Interface, use ASCII characters. Object creation or modification with non-ASCII characters is not supported.

To configure the user store connection for SSL

1. Log in to the Policy Server User Interface.
2. Click Infrastructure, Directory.
3. Click User Directory, Modify User Directory.

   The Modify User Directory pane appears with a list of existing user directory connections.
4. Select the user directory connection you want, and click Select.

   User directory settings appear.
5. Select the Secure Connection check-box, and click Submit.

   The user directory connection is configured to communicate over SSL.

Point the Policy Server to the Certificate Database

You point the Policy Server to the certificate database to configure the Policy Server to communicate with the user directory over SSL.

Note: When you create or modify a Policy Server object in the Policy Server User Interface, use ASCII characters. Object creation or modification with non-ASCII characters is not supported.

To point the Policy Server to the certificate database

1. Start the Policy Server Management Console.

   Important! If you are accessing this graphical user interface on Windows Server 2008, open the shortcut with Administrator permissions, even if you are logged into the system as an Administrator. For more information, see the release notes for your SiteMinder component.

2. Click the Data tab.
3. Enter the path to the Netscape certificate database file in the Netscape Certificate Database File field.

   Example: C:\certdatabase\cert7.db

   Note: The key3.db file must also be in the same directory as the cert7.db file.

4. Restart the Policy Server.

The Policy Server is configured to communicate with the user directory over SSL.

Verify the SSL Connection

You verify the SSL connection to ensure the user directory and the Policy Server are communicating over SSL.

Note: When you create or modify a Policy Server object in the Policy Server User Interface, use ASCII characters. Object creation or modification with non-ASCII characters is not supported.

To verify the SSL connection

1. Log in to the Policy Server User Interface.
2. Click Infrastructure, Directory.
3. Click User Directory, View User Directory.

   The View User Directory pane appears with a list of existing user directory connections.

4. Select the connection you want, and click Select.

   User directory settings appear.

5. Click View contents.

   If SSL is properly configured, the Directory Content pane appears and lists the contents of the user directory.

Index