CA SiteMinder®

Policy Server Administration Guide

12.52 SP1

CA Technologies Product References

This document references the following CA Technologies products:

- CA SiteMinder®
- CA SiteMinder® Web Services Security (formerly CA SOA Security Manager)
- CA IdentityMinder® (formerly CA Identity Manager)
- CA Security Compliance Manager

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.

Documentation Changes

No updates have been made to the 12.52 SP1 documentation, as a result of issues found in previous releases.

The following updates have been made to the 12.52 documentation, as a result of issues found in previous releases.

- Configure the CA SiteMinder Event Manager (see page 190)—Added information about configuring an Event library file (178452).
- Resolve LDAP search timeout issues (see page 273)—Added another use case for setting the SearchTimeout registry setting. Resolves CQ169864 and STAR Issue # 20130617
- Reset the r12.x Policy Store Encryption Key (see page 112)—Added step to stop the Policy Server before resetting the encryption key to resolve CQ171497, CQ171365.
- Resolve MySQL Session Store Timeout Errors (see page 277)—Added topic to describe how to troubleshoot session store timeout errors for MySQL database. Resolves CQ 177929.
- VLV Indexing on Some LDAP User Directories Causes SiteMinder Agent Group Lookups to Fail (see page 292)—Added topic to describe how to troubleshoot agent group lookup failures caused by VLV indexing. Resolves CQ 176247 and STAR issue 20397633-1.
- SM--Administrative UI Becomes Unresponsive (see page 273)—Added topic describing how to troubleshoot situations where the Administrative UI becomes unresponsive on a stand–alone Administrative UI installation (with an embedded JBoss application server). Resolves CQ 175819 and STAR issue 21529036-1.
- Reset the r12.x Policy Store Encryption Key (see page 112)—Updated instructions, Resolves CQs 171365/178999.
- Import Audit Data into an ODBC Database (see page 48)—Added note to not to set the Enable bulk load option in the ODBC Oracle Wire Protocol Driver Setup dialog when using the smauditimport tool to import audit data into an Oracle database using the -b option. Resolves CQ 159529 and STAR issue 21045785-2.

Contents

Chapter 1: Policy Server Management

This section contains the following topics:

Policy Server Management Overview

The Policy Server provides a platform for access control that operates in conjunction with other CA products, including:

- CA SiteMinder®—Combines the Policy Server with CA SiteMinder® Agents to provide access control for web servers.
- CA SiteMinder® Web Services Security—Combines the Policy Server with [set AGENT value for your book]s to provide access control for XML-based web services. If you have purchased this product, see the *CA SiteMinder® Web Services Security Policy Configuration Guide* for more information.
- CA Identity Manager—Provides identity management services, see the *CA Identity Manager Administration Guide* for more information.

Note: For information about SiteMinder and policy-based resource management, see the *Policy Server Configuration Guide.*

Policy Server Components

A Policy Server environment consists of two core components:

- **Policy Server**—Provides policy management, authentication, authorization, and accounting services.
- **Policy Store**—Contains all Policy Server data.

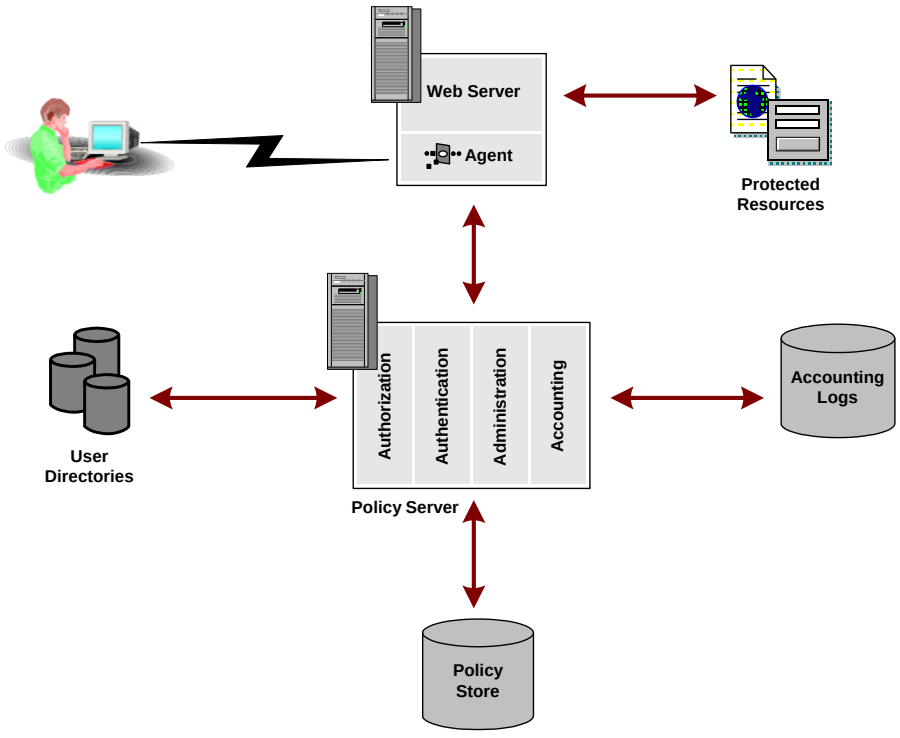
Additional components are included with various CA products, for example, CA SiteMinder® Agents. CA SiteMinder® Agents are integrated with a standard Web server or application server. They enable CA SiteMinder® to manage access to Web applications and content according to predefined security policies. Other types of CA SiteMinder® Agents allow CA SiteMinder® to control access to non-Web entities. For example, a CA SiteMinder® RADIUS Agent manages access to RADIUS devices, while a CA SiteMinder® Affiliate Agent manages information passed to an affiliate's Web site from a portal site.

Policy Server Operations

The Policy Server provide access control and single sign-on. It typically runs on a separate Windows or UNIX system, and performs the following key security operations:

- **Authentication**—The Policy Server supports a range of authentication methods. It can authenticate users based on user names and passwords, using tokens, using forms based authentication, and through public-key certificates.
- **Authorization**—The Policy Server is responsible for managing and enforcing access control rules established by Policy Server administrators. These rules define the operations that are allowed for each protected resource.
- **Administration**—The Policy Server can be configured using the Administrative UI. The Administration service of the Policy Server is what enables the UI to record configuration information in the Policy Store. The Policy Store is the database that contains entitlement information.
- **Accounting**—The Policy Server generates log files that contain auditing information about the events that occur within the system. These logs can be printed in the form of predefined reports, so that security events or anomalies can be analyzed.
- **Health Monitoring**—Policy Server provides health monitoring components.

The following diagram illustrates a simple implementation of a Policy Server in a SiteMinder environment that includes a single SiteMinder Web Agent.

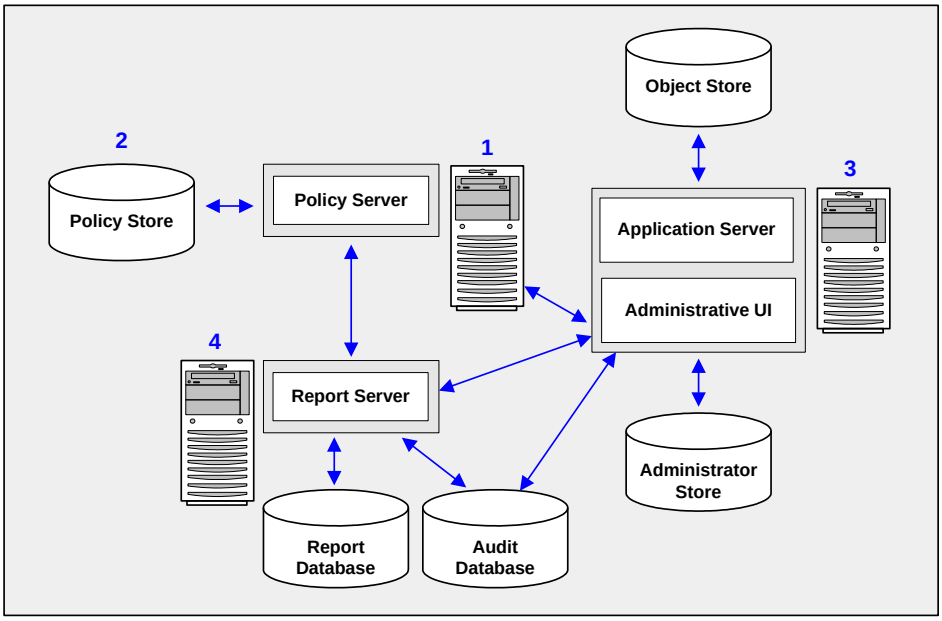


In a Web implementation, a user requests a resource through a browser. That request is received by the Web Server and intercepted by the SiteMinder Web Agent. The Web Agent determines whether or not the resource is protected, and if so, gathers the user's credentials and passes them to the Policy Server. The Policy Server authenticates the user against native user directories, then verifies if the authenticated user is authorized for the requested resource based on rules and policies contained in the Policy Store. When a user is authenticated and authorized, the Policy Server grants access to protected resources and delivers privilege and entitlement information.

Note: Custom Agents can be created using the SiteMinder Agent API. For more information, see the *Programming Guide for C*.

Policy Server Administration

The following diagram illustrates the Policy Server administrative model:



1. **Policy Server**—The Policy Server provides policy management, authentication, authorization, and accounting services.
2. **Policy store** - The policy store contains all of the Policy Server data. You can configure a policy store in a supported LDAP or relational database.

3. **Administrative UI**—You use the Administrative UI to manage CA SiteMinder® administrator accounts, objects, and policy data through the Policy Server. You configure a directory XML file, an administrator user store, and an object store when installing the Administrative UI:
   - **Object store**—The Administrative UI is an asynchronous application that is event and task-based. The object store stores this information. You configure an object store in either a Microsoft SQL Server or Oracle database.
   - **Administrator user store**—The Administrative UI authenticates CA SiteMinder® administrator accounts using the administrator user store. All of your administrator accounts must be stored in a single administrator user store. You configure an administrator user store in a supported LDAP directory server or ODBC database when installing the Administrative UI.
4. **Report server and databases**—You can create and manage a collection of CA SiteMinder® policy analysis and audit reports from the Administrative UI. A report server and report database are required to use the reporting feature. The report server and report database are required to run policy analysis reports. The report server and audit database are required to run audit-based reports.

Policy Server Management Tasks

As a Policy Server administrator, you are responsible for system-level configuration and tuning of the SiteMinder environment, monitoring and ensuring its performance, as well as management of users and user sessions as necessary.

You perform most fundamental system configuration and management tasks using the Policy Server Management Console. Others tasks are performed using the Administrative UI.

Policy Server management tasks include:

- Starting and Stopping the Policy Server
- Configuring the Policy Server Executives
- Cache Management
- Configuring and Managing Encryption Keys
- User Session and Account Management
- Monitoring the Health of Your SiteMinder Environment
- Running Reporting

Policy Server Management Console

The Policy Server Management Console (or Management Console) provides a range of Policy Server configuration and system management options. The Management Console has a tab-based user interface in which information and controls are grouped together by function and presented together on tabs in a single window.

Important! The Policy Server Management Console should only be run by users who are members of the administrator group in Microsoft Windows.

Start the Management Console

Follow these steps:

- **Windows**

  Select the Policy Server Management Console icon in the CA SiteMinder® program group.

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

- **UNIX**

  Run *installation_directory*/siteminder/bin/smconsole.

Note: To run the Policy Server Management Console on UNIX:

- The X display server must be running.
- Enable the display with:

  `export DISPLAY=`*`n.n.n.n`*`:0.0`

  n.n.n.n

  Specifies the IP address of the Policy Server host system.

Save Changes to Management Console Settings

On any tab in the Management Console, click:

- Apply to save the settings and keep the Management Console open
- OK to save the settings and close the Management Console.

Note: You must stop and restart the Authentication and Authorization processes to put Management Console settings changes into effect. The Policy Server cannot use the new settings until these services restart.

Policy Server User Interface

The browser–based CA CA SiteMinder® Administrative UI primarily enables management of Policy Server objects, but also provides some system management functionality.

To access the Administrative UI

1. Do one of the following:
   - From the computer hosting the Administrative UI, click Start, Programs, CA, CA SiteMinder®, CA SiteMinder® Administrative UI.
   - Open the following URL in your browser:

     `http://fqdn:port/iam/siteminder/adminui`

     fqdn

     Specifies the fully qualified domain name of the Administrative UI host system.

     port

     Specifies the port on which the application server, which is hosting the Administrative UI, is listening. If you installed the Administrative UI using the stand–alone option, enter 8080.

     Example: http://somehost@example.com:8080/iam/siteminder/adminui

     The login page for the Administrative UI appears.
2. Enter a valid user name and password.

   If you are accessing the Policy Server for the first–time, use the default superuser administrator account, which you created during Policy Server installation.
3. Click Log In.

   The Administrative UI opens.

   The contents of the window depend on the privileges of the administrator account you used to log in. You only see the items to which your account has access.

Grant Access to XPS Tools

Access to the XPS tools included with CA SiteMinder® must be granted to individual users by an Administrator using the Administrative UI.

Follow these steps:

1. Log in to the Administrative UI.
2. Click the Administration, Administrator, Administrators.

3. Do one of the following:
   - To add a new administrator, click Create Administrator
   - To change the access of an existing administrator, search for the user and click the name of the user to access the record.
4. Enter a name and an optional description in the respective fields.
5. Enter a user path or click Lookup to select an existing user path.

   Note: The user path (specified in the Administrative UI or with the XPSSecurity tool by an Administrator) is required for write access to any of the settings controlled by the XPS Tools. A user path has the following format:
   namespace://*directory_server*/*DN* or *Login_for_OS*
6. (Optional) Select the Super User option to grant super user rights.
7. Select any of the following command line tools in the Access Methods section:

   XPSEvaluate Allowed

   Grants access to the XPS expression evaluation tool.

   XPSExplorer Allowed

   Grants access to the tool that edits the XPS database.

   XPSRegClient Allowed

   Grants access to the XPS tool that registers Web Access Managers or Reports servers as privileged clients.

   XPSConfig Allowed

   Grants access to the tool that examines and configures XPS settings in XPS-aware products.XPSSecurity Allowed

   Grants access to the security tool which creates XPS users and specifies their XPS-related privileges.
8. Click Submit.

   The administrator has permission to use the selected XPS tools.

More information:

Add Event Handler Libraries (see page 130)

Chapter 2: Starting and Stopping the Policy Server

This section contains the following topics:

Services and Processes Overview

The Policy Server runs two services under Windows and two processes on UNIX. The Policy Server installation process starts the Policy Server and Monitor processes and configures executive applications to run the processes automatically at system startup in the future.

The main Policy Server processes for Windows are:

Policy Server

Serves Agent requests for authentication, authorization, accounting and logging, and (if enabled) administration.

SiteMinder Health Monitor Service

The OneView Monitor, which monitors the health and performance of the authentication server, authorization server, and Web Agent.

The main Policy Server processes for UNIX are:

smpolicysrv

Serves Agent requests for authentication, authorization, accounting and logging, and (if enabled) administration.

smmon

The OneView Monitor, which monitors the health and performance of the authentication server, authorization server, and Web Agent.

Start and Stop Policy Server Services on Windows Systems

To start or stop Policy Server services on Windows systems:

- On the Management Console Status tab, click the Start or Stop button.
- Use the Windows Services dialog, which you can access from the Windows Start Menu using Settings, Control Panel, Services. When you start or stop a Policy Server process, the associated executive starts or stops.
- You can stop the policy server from the command line using smpolicysrv:

  ```
  installation_path\siteminder\bin\smpolicysrv -stop
  ```

Note: On Windows systems, do *not* run the smpolicysrv command from a remote desktop or Terminal Services window. The smpolicysrv command depends on inter-process communications that do not work if you run the smpolicysrv process from a remote desktop or Terminal Services window.

Important! Before running a CA 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.

Start and Stop Policy Server Processes on UNIX Systems

To start or stop Policy Server processes on UNIX systems, take either of these actions:

- On the Management Console Status tab, click the corresponding Start and Stop button.
- Use the supplied scripts. Two scripts are provided to start and stop the Policy Server processes. These scripts also stop the UNIX executive so that the processes do not restart automatically.

  ```
  installation_path/siteminder/start-all
  installation_path/siteminder/stop-all
  ```

In addition, the following script can be used to start and stop the Policy Server process. If the UNIX executive is not running when you execute the script, the executive starts along with the process. The script can be invoked with the same command line options, as follows:

```
installation_path/siteminder/smpolsrv
```

Command line options:

-stop

Stops a process.

-start

Starts a process.

-status

Indicates whether or not a process is running.

The Policy Server logs all UNIX executive activity in the *installation_directory*/log/smexec.log file. Log entries are always appended to the existing log file.

More Information:

Command Line Troubleshooting of the Policy Server (see page 278)

Thread Exit Window during Policy Server Shutdown

By default, the Policy Server waits 3 minutes for all threads to exit before shutting down. If any of the threads do not exit, the Policy Server exits.

You can change the maximum amount of time the Policy Server waits for threads to exit by creating a registry key.

To create the registry key

1. Access the Policy Server host system and do one of the following:
   - (Windows) Open the Registry Editor and navigate to HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\\Netegrity\SiteMinder\CurrentVersion\PolicyServer.
   - (UNIX) Open the sm.registry file. The default location of this file is *siteminder_home*/registry.

     siteminder_home

     Specifies the Policy Server installation path.
2. Create MaxShutDownTime with a registry value type of REG_DWORD.

   Unit of measurement: seconds

   Default value: 180

   Minimum value: 30

   Maximum value: 1800

3. Do one of the following:
   - (Windows) Exit the Registry Editor.
   - (UNIX) Save the sm.registry file.
4. Restart the Policy Server.

Important! If the Policy Server threads do not exit properly during shutdown, contact CA SiteMinder® Support.

Configure the Policy Server Executives

In both UNIX and Windows installations of the Policy Server, one or more executive applications monitor the status of Policy Server processes and automatically restart any processes that fail. The following sections describe how to start and stop Policy Server processes based on your platform and how to configure, disable, and enable the UNIX and Windows executives.

Configure Windows Executives

For Windows, each Policy Server process is monitored by a separate executive. Each of these executives reads the following threshold values from the *Policy_Server_installation_ path*\config\siteminder.conf configuration file:

SMEXEC_UPTIME_THRESHOLD

Indicates the minimum amount of time (in seconds) a Policy Server service must run after startup before the associated executive stops monitoring for frequent crashes. The default value for this parameter is 60 seconds.

SMEXEC_RESTART_THRESHOLD

Indicates the maximum number of times the executive attempts to restart a service in the time specified by the SMEXEC_UPTIME_THRESHOLD parameter. If a service crashes more than the number of attempts specified by this parameter, the executive stops attempting to restart the service. The default value for this parameter is five attempts.

To change the threshold parameters, edit the siteminder.conf file and restart the Policy Server processes.

Configure the UNIX Executive

For UNIX, the Policy Server and Health Monitor processes are monitored by a single executive. The executive reads its settings from the following configuration file:

installation_path/config/siteminder.conf

You can edit this file to change the following settings:

POLICYSERVER_ENABLED

Indicates the state of the Policy Server process when the executive starts running. Set this parameter to YES to enable the process at executive startup.

MONITOR_ENABLED

Indicates the state of the health monitor process when the executive starts running. Set this parameter to YES to enable the process at executive startup.

SMEXEC_UPTIME_THRESHOLD

Indicates the minimum amount of time (in seconds) a Policy Server service must run after startup before the associated executive stops monitoring for frequent crashes. The default value for this parameter is 60.

SMEXEC_RESTART_THRESHOLD

Indicates the maximum number of times the executive attempts to restart a service in the time specified by the SMEXEC_UPTIME_THRESHOLD parameter. If a service crashes more than the number of attempts specified by this parameter, the executive stops attempting to restart the service. The default value for this parameter is five attempts.

To change any of the UNIX Executive parameters

1. Edit the *installation_path*/config/siteminder.conf file.
2. From a command line, run the following script:

   `installation_path/siteminder/bin/stop-all`

   The Policy Server processes stop.
3. From a command line, run the following script:

   `installation_path/siteminder/bin/start-all`

   The UNIX executive restarts using the new settings in the siteminder.conf file.

Chapter 3: Configuring Policy Server Data Storage Options

This section contains the following topics:

Configure Data Storage Options Overview

You configure storage locations for CA SiteMinder® data stores from the Policy Server Management Console Data tab.

Follow these steps:

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. Use Administrator permissions even if you are logged in to the system as an Administrator. For more information, see the release notes for your CA SiteMinder® component.

2. Click the Data tab.

   Note: For more information about the settings and controls on this tab, click Help, Management Console Help.

3. Select the data store that you want to configure from Database. The data store you select determines the storage possibilities that are available.

   Note: The following table lists the data stores that you can configure and the respective storage options. The combination of these settings determines the settings displayed in the context–sensitive controls that become available.

4. Select a storage type for the selected data store from Storage.

5. Configure the required information.

6. Click OK to save the settings.

The following table lists CA SiteMinder® data stores and the available storage options. For more information about these stores, see the *CA SiteMinder® Implementation Guide*.

Database	Available Storage
Policy Store	LDAP ODBC
Key Store	LDAP ODBC
Audit Logs	ODBC Text file
Session Store	ODBC CA Directory

Configure the Policy Store Database

The Policy Store is the database in which all Policy Server objects are stored.

To configure the policy store database

1. Select Policy Store from the Database drop-down list.
2. Select an available storage type (LDAP or ODBC) from the Storage drop-down list.
3. Specify Storage Options appropriate for the chosen storage type.
4. Click Apply to save your settings, or click OK to save the settings and exit the Console.
5. (Optional) If you changed the Policy Store database storage type to LDAP, and want the Policy Store to be used as the key store, complete the steps described Configure the Key Store or Audit Logs to Use the Policy Store Database (see page 31).

   Note: If you have one or more Policy Servers communicating with an LDAP-enabled policy store, configure the same setting in the Management Console on each of those Policy Server systems.

Configure the Key Store or Audit Logs to Use the Policy Store Database

After you configure the Policy Store, you can optionally configure databases. If the Policy Store is of a compatible storage type (that is, if the Policy Store is configured to be stored in a database that is also a valid storage option for the other database), you can configure the Policy Server to use the policy store database as one or more of the following:

- Key store
- Audit logs

Important! If you are using an LDAP database as your Policy Store, do *not* use the Policy Store database for audit logs. Audit logs cannot be written to an LDAP database. If you are using the CA SiteMinder® sample data source (SmSampleUsers) as your Policy Store, do *not* use the Policy Store database for audit logs. Audit logs are not supported by the sample policy store.

To configure another database to be stored in the Policy Store database, set the Use Policy Store Database option that appears between the Database drop-down list and the Storage Options area whenever a database other than Policy Store is chosen from the Database drop-down list.

When the Use Policy Store Database option is selected, the Storage drop-down list and the context-sensitive Storage Options are grayed-out.

Configure a Separate Database for the Key Store

The Key store is where the Policy Server stores keys used to encrypt cookies created by CA SiteMinder® Agents.

To configure a separate database for the key store

1. Choose Key Store from the Database drop-down list.
2. Choose an available storage type (LDAP or ODBC) from the Storage drop-down list.

   Note: The Policy Server supports mixed LDAP/ODBC policy and key stores. The policy store can exist in an ODBC database and the key store can reside in an LDAP Directory Server or vice versa. For a list of supported databases, refer to the CA SiteMinder® Platform Matrix on the Technical Support site.
3. Specify Storage Options appropriate for the chosen storage type.
4. Click Apply to save your settings, or click OK to save the settings and exit the Console.

Configure a Separate Database for the Audit Logs

The audit log database is where the Policy Server stores audit logs containing event information.

Storing audit logs in a database has the potential add to latency to your environment. This latency occurs because of the additional traffic between the Policy Server and the database. As the amount of transactions increase, this database latency can affect the performance of the Policy Server. When the database slows down, the Policy Server also slows down.

Consider logging to a text file and exporting those logs to a database as an alternative if the performance of your database is unacceptable.

Follow these steps:

1. Choose Audit Log from the Database drop-down list.
2. Choose an available storage type from the Storage drop-down list.
3. Specify Storage Options appropriate for the chosen storage type.
4. Click Apply to save your settings, or click OK to save the settings and exit the Console.

When deciding whether to store the Policy Server audit logs in an ODBC database or text file, consider the following factors:

- CA SiteMinder® Reporting requires that the audit logs are written to an ODBC database. Reporting does *not* support the text file logs.
- CA SiteMinder® audit logging to an ODBC database and to a text file supports internationalization (I18N).
- By default, CA SiteMinder® administrator changes to policy store objects are not written to the audit database. These object changes are written to text files that are located in the *siteminder_home*\audit directory. You can configure CA SiteMinder® to include these events in reports.
- Synchronous logging affects the performance of the Policy Server more than asynchronous logging does.
- When logging to an ODBC database, set the following registry key values in the HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Database\ registry location. These settings helps prevent losing auditing data under heavy load:

  ConnectionHangwaitTime

  We recommend 60 seconds for heavy loads. The default is 30 seconds.

  QueryTimeout

  We recommend 30 seconds for heavy loads. The default is 15 seconds.

LoginTimeout

We recommend 30 seconds for heavy loads. The default is 15 seconds.

Note: The value of ConnectionHangwaitTime must always be at least double the value of QueryTimeout and LoginTimeout.

More information:

Record Administrator Changes to Policy Store Objects (see page 76)
How to Include CA SiteMinder® Administrative Audit Events in Reports (see page 79)

Configure the Session Store

The session store is where the Policy Server stores persistent session data.

Follow these steps:

1. Select Session Server from Database.
2. Select an available storage type from Storage.
3. Set the Session Server Enabled option.

   If you are going to use persistent sessions in one or more realms, enable the session store. Enabling the session store affects Policy Server performance.

   Note: The following option is disabled:

   `Use Policy Store database`

   For performance reasons, the session store cannot be run on the same database as the policy store.
4. Specify the required storage options.
5. Click OK to save the settings and exit the console.

Configure the Session Store Timeout for Heavy Load Conditions

Under heavy load conditions, long-running queries necessary for session store maintenance tasks, such as removing idled–out or expired sessions, can timeout. Adjust the timeout for session store maintenance tasks (60 seconds by default), by increasing the value of the MaintenanceQueryTimeout registry setting. Increase the value so that the maintenance thread can complete its tasks successfully.

The MaintenanceQueryTimeout registry setting can be found at the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\
SessionServer
```

Configure LDAP Storage Options

Use the LDAP context–sensitive storage controls to point CA SiteMinder® to an LDAP directory server that is configured as:

- A policy store
- A session store

Consider the following items:

- CA Directory is the only LDAP directory server that CA SiteMinder® supports as a session store. For more information, see the 12.52 SP1 CA SiteMinder® Platform Support Matrix.
- Restart the Policy Server after updating LDAP settings in the Policy Server Management Console. The parameters do not take effect until the Policy Server is restarted.

Configure an LDAP Database

To configure an LDAP database

1. Specify the Server name or IP address of the LDAP server in the LDAP IP Address field. For performance reasons, the IP address is preferred.

   Note: You can specify multiple servers in this field to allow for LDAP server failover.

2. Specify the LDAP branch under which the CA SiteMinder® schema is located in the Root DN field (for example, o=myorg.org).

3. If your Policy Server communicates with the LDAP directory over SSL, select the Use SSL check box.

   Note: If you select this option, you must specify a certificate database in the Netscape Certificate Database File field.

4. Specify the DN of the LDAP directory administrator (for example, cn=Directory Manager) in the Admin Username field.
5. Enter the administrative password for the LDAP directory in the Admin Password field.
6. Confirm the administrative password for the LDAP directory in the Confirm Password field.
7. Click Test LDAP Connection to verify that the parameters you entered are correct and that the connection can be made.

Configure LDAP Failover

If you have multiple LDAP directories, you can configure directories for failover. To enable failover, enter LDAP server IP addresses and port numbers in the LDAP Server field as a space-delimited list of LDAP server addresses. You can specify a unique port for each server. If your LDAP servers are running on a non-standard port (389 for non SSL/ 636 for SSL), append the port number to the last server IP address using a ':' as a delimiter. For example, if your servers are running on ports 511 and 512, you can enter the following:

```
123.123.12.11:511 123.123.12.22:512
```

If the LDAP server 123.123.12.11 on port 511 did not respond to a request, the request is automatically passed to 123.123.12.22 on port 512.

If all of your LDAP servers are running on the same port, you can append the port number to the last server in the sequence. For example, if all of your servers are running on port 511, you can enter the following:

```
123.123.12.11 123.123.12.22:511
```

Configure Enhanced LDAP Referral Handling

Enhancements have been made to CA SiteMinder®'s LDAP referral handling to improve performance and redundancy. Previous versions of CA SiteMinder® supported automatic LDAP referral handling through the LDAP SDK layer. When an LDAP referral occurred, the LDAP SDK layer handled the execution of the request on the referred server without any interaction with the Policy Server.

CA SiteMinder® now includes support for non-automatic (enhanced) LDAP referral handling. With non-automatic referral handling, an LDAP referral is returned to the Policy Server rather than the LDAP SDK layer. The referral contains all of the information necessary to process the referral. The Policy Server can detect whether the LDAP directory specified in the referral is operational, and can terminate a request if the appropriate LDAP directory is not functioning. This feature addresses performance issues that arise when an LDAP referral to an offline system causes a constant increase in request latency. Such an increase can cause CA SiteMinder® to become saturated with requests.

To configure LDAP referral handling

1. Open the Policy Server Management Console.

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

2. Select the Data tab.

   Enable Enhanced Referrals

   Mark this check box to allow the Policy Server to use enhanced handling LDAP referrals at the Policy Server, rather than allowing LDAP referral handling by the LDAP SDK layer.

   Max Referral Hops

   Indicates the maximum number of consecutive referrals that will be allowed while attempting to resolve the original request. Since a referral can point to a location that requires additional referrals, this limit is helpful when replication is misconfigured, causing referral loops.

3. Modify the values as required.
4. Restart the Policy Server.

Configure Support for Large LDAP Policy Stores

Large LDAP policy stores can cause Administrative UI performance issues.

To prevent these problems, you can modify the values of the following registry settings:

Max AdmComm Buffer Size

Specifies the Administrative UI buffer size (the maximum amount of data [bytes] that is passed from the Policy Server to the Administrative UI in one packet).

Configure this setting at the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion
\PolicyServ\
```

We recommend using caution when setting this value. Allocation of a larger buffer decreases overall performance.

Range: 256 KB to 2,097,000 KB

Default: 256 KB (also applies when this registry setting does not exist).

SearchTimeout

Specifies the search timeout, in seconds, for LDAP policy stores.

Configure this setting at the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion
\LdapPolicyStore\SearchTimeout
```

Examples of factors which influence the appropriate value for this setting include (but are not limited to) the following items:

- The network speed
- The size of the LDAP search query response
- The LDAP connection state
- The load on the LDAP server

A large enough value prevents any LDAP timeouts when fetching large amounts of policy store data.

Limit: Use hexadecimal numbers.

Default: 0x14 (20 seconds). This value is also used when the registry setting does not exist.

Example: 0x78 (120 seconds)

More information:

Configure the Policy Store Database (see page 30)
Configure a Separate Database for the Key Store (see page 31)

How to Configure SSL Support

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

Complete the following steps to configure a connection over SSL:

1. Review the SSL connection prerequisites.
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. If the server certificate was signed by a certificate authority, add the root certificate from the respective certificate authority to the certificate database as well.
6. List the certifications in the certificate database.
7. Point the Policy Server to the certificate database.

SSL Prerequisites

Consider the following SSL prerequisites:

- Verify that the directory server is SSL–enabled.

  Note: For more information, see vendor–specific documentation.

- CA SiteMinder® uses a Mozilla LDAP SDK to communicate with LDAP directories and requires that the database files be in a Netscape version file format (cert8.db).

  Important! Do not use Microsoft Internet Explorer to install certificates into your cert8.db database file.

Create the Certificate Database Files

To create the certificate database files, use the Mozilla Network Security Services (NSS) certutil application that is included with the Policy Server

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 CA 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.

Follow these steps:

1. From a command prompt, navigate to the installation bin directory.

   Example: C:\Program Files\CA\SiteMinder\bin

   Note: Windows has a native certutil utility. Verify that you are working from the Policy Server bin directory, or you can inadvertently run the Windows certutil utility.

2. Enter the following command:

   `certutil -N -d certificate_database_directory`

   -N

   Creates the cert8.db, key3.db, and secmod.db certificate database files.

   -d *certificate_database_directory*

   Specifies the directory in which the certutil tool 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:

   - cert8.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

To add the root Certificate Authority (CA), use the Mozilla Network Security Services (NSS) certutil application, which is in the Policy Server.

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 CA 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.

Follow these steps:

1. From a command prompt, navigate to the Policy Server installation bin directory.

   Example: C:\Program Files\CA\SiteMinder\bin

   Note: Windows has a native certutil utility. Verify that you are working from the bin directory of the NSS utility, or you can inadvertently run the Windows certutil utility.

2. Run the following command:

   `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*

   Specifies the trust attributes to apply to the certificate. The three available trust categories are expressed in this order: "SSL, email, object signing". In each category position, you can 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 argument is required 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. The path includes the certificate name. The 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.

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

To enable communication over SSL, add the server certificate to the certificate. Use the Mozilla Network Security Services (NSS) certutil application, which is available with the Policy Server.

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 CA 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.

Follow these steps:

1. From a command prompt, navigate to the Policy Server installation bin directory.

   Example: C:\Program Files\CA\SiteMinder\bin

   Note: Windows has a native certutil utility. Verify that you are working from the bin directory of the NSS utility, or you can inadvertently run the Windows certutil utility.

2. Run the following command:

   ```
   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*

Specifies the trust argument. The three available trust categories for each certificate are expressed in this order: "SSL, email, object signing". In each category position, you can use zero or more of the following attribute arguments:

p

Valid peer.

P

Trusted peer. This argument implies p.

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

-i *server_certificate_path*

Specifies the path to the server certificate. The path includes the certificate name. The 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

To verify that the certificates are in the certificate database, use the Mozilla Network Security Services (NSS) certutil application. Policy Server includes this tool.

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 CA 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.

Follow these steps:

1. From a command prompt, navigate to the Policy Server installation bin directory.

   Example: C:\Program Files\CA\SiteMinder\bin

   Note: Windows has a native certutil utility. Verify that you are working from the bin directory of the NSS utility, or you can 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.

   This command 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
```

Point the Policy Server to the Certificate Database

To communicate with the user directory over SSL, point the Policy Server to the certificate database.

Follow these steps:

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. Use Administrator permissions even if you are logged in to the system as an Administrator. For more information, see the release notes for your CA SiteMinder® component.

2. Click the Data tab.

3. Enter the path to the certificate database file in the Netscape Certificate Database File field.

   Example: C:\certdatabase\cert8.db

   Note: The key3.db file must be in the same directory as the cert8.db file.

4. Restart the Policy Server.

   The Policy Server can communicate with the user directory over SSL.

Configure ODBC Storage Options

Use the ODBC context–sensitive storage controls to configure an ODBC data source for:

- A policy store
- A key store
- Audit logs
- A session store

Note: For more information about configuring ODBC data sources, see the *Policy Server Installation Guide*.

Configure an ODBC Data Source

To configure an ODBC data source

1. Specify the name of the ODBC data source in the Data Source Information field. You can enter multiple names in this field to enable ODBC failover.

   Data Source Information

   Indicates the name of the ODBC data source. You can enter multiple names in this field to enable failover.

   User Name

   Indicates the user name of the database account (if required) with full rights to access the database.

   Password

   Contains the password of the database account.

   Confirm Password

   Contains a duplicate of the database account password, for verification.

   Maximum Connections

   Indicates the maximum number of ODBC connections per database allowed at one time.

2. Click Test ODBC Connection to verify that the parameters you entered are correct and that the connection can be made.

Configure ODBC Failover

If you have multiple ODBC data sources and you want to configure failover, list the data source names in the Data Source Information field, separated by commas. For example, entering CA SiteMinder® Data Source1,CA SiteMinder® Data Source2 causes the Policy Server to look at Data Source 1 first. If CA SiteMinder® Data Source1 does not respond, the Policy Server automatically looks for CA SiteMinder® Data Source2.

Note: Using the method described above, you can configure failover for data sources used as policy stores, key stores, session stores, and audit logs.

Configure Limit to Number of Records Returned by a SQL Query

SQL queries that return large numbers of records can cause the Policy Server to hang or crash. To manage this outcome, you can output a warning message to the SMPS logs when the number of records returned exceeds a maximum value that you specify.

To configure the maximum, add the registry key, MaxResults, and set its value to one or more. When the number of records returned by a query equals or exceeds the limit specified by MaxResults, the Policy Server outputs a warning to the SMPS logs. When MaxResults is set to zero or undefined, no warning messages are output.

Adding the registry key, MaxResults, does not change the number of records returned. Adding the key does warn you when the number of results exceeds a limit that you set. You can use this feedback to modify your SQL queries and fine-tune the number of records returned, as needed.

To configure a limit to the number of records returned by a SQL query

1. Manually add the registry key MaxResults:

   Windows

   Add the registry key MaxResults to the following location:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersi
   on\Ds
   \ODBCProvider
   ```

   Solaris

   Add the following lines to the sm.registry file:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersi
   on\Ds
   \ODBCProvider=35921
   MaxResults=0x1; REG_DWORD
   ```

2. Assign MaxResults a value greater than or equal to one.

Configure ODBC Registry Settings for Timeout

The parameters listed following control timeout for the connection between and ODBC database and the Policy Server in various situations. The key on Windows and UNIX is available the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Database
```

"LoginTimeout"

The time that is allowed to connect to the database.

"QueryTimeout"

Allows 30 seconds for the query to complete. When the query does not complete within this time, a cancel request is sent to the database. For an ODBC user directory, the query timeout is overridden with the user directory object Searchtimeout. You set this value using XPSExplorer.

"ConnectionHangWaitTime"

The number of seconds before the Policy Server marks a connection as hung. This value must be larger than twice the value of QueryTimeout or SearchTimeout.

"ConnectionTimeout"

The maximum wait time on a connection. In cases where the query timeout or the log-in timeout apply, those values override the connection timeout.

Configure Text File Storage Options

Use the Text File storage options to configure a text file to store the Policy Store audit logs.

To specify a text file, type the full path of a file in the File name field or click the Browse button and browse to the required directory and click on or type the name of the desired file.

Audit Data Import Tool for ODBC

The Policy Server can store audit data in an ODBC database or output audit data to a text file. The smauditimport tool reads a CA SiteMinder® audit data text file and imports the data into an ODBC database. The database has been configured as an audit store using 5.x or 6.x schema.

The smauditimport tool imports authentication, authorization, and admin data into the corresponding tables in the ODBC database. The tool logs the number of rows successfully imported into the ODBC database. For each row that cannot be imported into the ODBC database, the tool logs the row number.

The characters '[', ']', or '\' appearing in a field in the policy or user store require a preceding escaping character '\' (backslash). These characters appear because they have been used in fields like username, realm name, and so on.

Set the following registry key, to escape these characters automatically:
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\LogConfig]
Value Type: DWORD VALUE
Value Name: EscapeAuditFields
Value Data: 1

When Value Data is set to 0, or if the key does not exist, there is no escaping, and the operation fails.

Note: In some CA SiteMinder® documentation, the terms audit and logging are used interchangeably.

Log More Audit Data to a Text File

By default, the Policy Server logs less audit data to a text file than to an ODBC database. You can log more audit data to a text file than the default and bring the amount of data in line with an ODBC database. To do so, manually add the following registry key and set its value to one: "Enable Enhance Tracing". To disable "Enable Enhance Tracing", set its value to zero (the default).

To log more audit data to a text file

1. Manually add the registry key "Enable Enhance Tracing":

   Windows

   Add the following key:

   ```
   TYPE=DWORD
   \netegrity\SiteMinder\CurrentVersion\Reports
   \"Enable Enhance Tracing"
   ```

   Solaris

   Follow these steps:

   a. Open the file: .../siteminder/registry/sm.registry.

   b. Locate the line:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder
   \CurrentVersion\Reports=25089
   ```

c. Below the line, add the following:

```
"Enable Enhance Tracing"=0x1;    REG_DWORD
```

d. Save and close the file.

2. Set "Enable Enhance Tracing" to one.

Note: The value of "Enable Enhance Tracing" does not affect logging of Entitlement Management Services (EMS) events.

Audit Data Import Prerequisites for ODBC

Before you run the tool smauditimport, verify that the following prerequisites have been satisfied:

- The Policy Server is installed on a Windows, Solaris, or Linux operating environment.

  Note: For Solaris and Linux platforms, run nete_ps_env.ksh before running the smauditimport tool.

- The ODBC database is configured as an audit (logging) store with 5.x or 6.x schema.

  Note: For more information about how to configure an ODBC database as an audit (logging) store, see the *Policy Server Installation Guide*.

- The registry key "Enable Enhance Tracing" is set to one.

Import Audit Data into an ODBC Database

The tool smauditimport reads a CA SiteMinder® audit data text file and imports it into an ODBC database. The tool is located in the \bin directory under the Policy Server installation directory.

Important! Before you import audit data into an ODBC database, configure the database as an audit store with CA SiteMinder® 5.x or 6.x schema. For more information about how to configure an ODBC database with the CA SiteMinder® schema, see the *Policy Server Installation Guide*.

Important! Before running a CA 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.

Follow these steps:

1. On the computer where the Policy Server is installed, navigate to *siteminder_installation*\bin.

   siteminder_installation

   Specifies the Policy Server installation path.

2. Run the following command:

   smauditimport *audit_file dsn user_name user_password* -f -v -b*bulk_load_size* -s5 | -s6 -a*number*

   audit_file

   Specifies the path and name of the text file containing the audit data.

   Note: The smauditimport tool requires the full path name of the audit data text file.

   dsn

   Specifies the Data Source Name (DSN) of the ODBC database.

   user_name

   Specifies the name of the ODBC database administrator.

   user_password

   Specifies the password of the ODBC database administrator.

   -a

   (Required) Specifies the value of the Enable Enhance Tracing registry setting on the Policy Server. This setting exists under HKEY_LOCAL_MACHINE\Software\Netegrity\SiteMinder\Currentversion\Reports. On Windows operating environments, this setting is in the Windows registry. For the UNIX or the Linux operating environments, this setting is in the sm.registry file. The value of the setting must match the value of used with this option.

   Example: -a2 (Indicates an Enable Enhance Tracing registry setting of 2).

   -f

   (Optional) When an error occurs while importing audit data, smauditimport logs the row number and continues processing.

   Default: Without the -f option, smauditimport logs the row number, but stops processing when an error occurs.

-v

(Optional) Validates the number of fields in the text file, validates that the values in numeric fields fall within specified ranges, validates the connection to the database, and outputs errors.

Note: When the smauditimport tool is run in the validation mode, no data is imported into the database.

-b *bulk_load_size*

(Optional) Specifies the number of rows to read and import into the ODBC database.

Default: 100

Note: If using the smauditimport tool to import audit data into an Oracle database using the -b option, do *not* set the Enable bulk load option in the ODBC Oracle Wire Protocol Driver Setup dialog. If the ODBC Oracle Wire Protocol Driver Setup Enable bulk load option is set, unexpected behavior occurs during the bulk load.

-s5 | -s6

(Optional) Supports an ODBC database that is configured as an audit store with either 5.x schema or 6.x schema.

Default: Supports an ODBC database that is configured as an audit store with 6.x schema.

Specify a Netscape Certificate Database File

If you are using an LDAP directory to store policies or user information over SSL, you must point the Policy Server to the directory that contains Netscape Certificate Database files. The directory must contain the cert8.db and key3.db files.

Before you install the Certificate Database file, make a copy of it. Use the certificate database copy instead of the original and do not use cert8.db if it is currently being used by Netscape Communicator.

Type the name of the Certificate database in the Netscape Certificate Database file field or browse the directory tree to locate and select the database. This field does not require a value for Active Directory user stores configured in the Administrative UI using the AD namespace. AD user stores use the native Windows certificate repository when establishing an SSL connection.

More information:

Configure a Separate Database for the Audit Logs (see page 32)

Chapter 4: Configuring General Policy Server Settings

This section contains the following topics:

Policy Server Settings Overview

The Policy Server allows you to configure a number of general settings that determine the way it behaves and performs from the Policy Server Management Console Settings tab:

- TCP ports for access control
- Administration settings including the TCP port, and Inactivity Timeout
- Connection settings
- RADIUS settings
- Performance settings
- OneView Monitor settings

Configure Policy Server Settings

To configure general Policy Server settings

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. Use Administrator permissions even if you are logged in to the system as an Administrator. For more information, see the release notes for your CA SiteMinder® component.

2. Click the Settings tab.

   Note: For more information about the settings and controls on this tab, click Help, Management Console Help.

3. Adjust the desired settings.

4. When you have finished, click Apply to save your settings, or click OK to save the settings and exit the Management Console.

Configure Access Control Settings

The Policy Server uses three separate TCP ports to communicate with CA SiteMinder® Agents for authentication, authorization, and accounting.

To enable or disable these Agent communication ports, as well as change the TCP port numbers used for each function, use the controls in the Access Control group box on the Management Console Settings tab.

Configure Policy Server Administration Settings

The Policy Server uses a TCP port to communicate with the Administrative UI to allow browser-based policy management.

To enable or disable and change the TCP port number used to communicate with the Administrative UI, as well as specifying a timeout value for administrative inactivity, use the controls in the Administration group box on the Management Console Settings tab.

Configure Policy Server Connection Options

To specify the maximum number of Policy Server threads, and the idle timeout for a connection to the Policy Server, use the controls in the Connection Options group box on the Management Console Settings tab.

Configure Policy Server Performance Settings

To configure cache and thread settings to tune Policy Server performance, use the Performance group box on the Management Console Settings tab.

Configure RADIUS Settings

To specify settings to enable support of RADIUS components in your deployment, use the RADIUS group box on the Management Console Settings tab.

Configure OneView Monitor Settings

By default the OneView Monitor runs locally on the Policy Server that it is monitoring.

To configure the monitor to accept connections from other Policy Servers to be monitored remotely or to specify a central remote Policy Server that is to monitor all Policy Servers in a cluster, use the OneView Monitor group box on the Management Console Settings tab.

Reschedule CA SiteMinder® Policy Data Synchronization

CA SiteMinder® automatically synchronizes Policy Data using the XPSSweeper tool. You can change how often this tool runs by setting the following parameter:

AutosweepSchedule

Specifies the days and times (hour and minute) at which the XPSSweeper process runs.

Default: Mondays at 08:30

Limits: GMT Time zone using the 24-hour clock. Separate multiple entries with commas or spaces

Example: Mon@13:30,Tue@14:00

Note: If you do *not* have write access to the CA SiteMinder® binary files (XPS.dll, libXPS.so, libXPS.sl), an Administrator must grant you permission to use the related XPS command line tools using the Administrative UI or the XPSSecurity tool.

Follow these steps:

1. Open a command line on the Policy Server, and enter the following command:

   ```
   xpsconfig
   ```

   The tool starts and displays the name of the log file for this session, and a menu of choices opens.

2. Enter the following:

   ```
   xps
   ```

   A list of options appears.

3. Enter the following:

   ```
   8 (AutosweepSchedule)
   ```

   The current schedule for the XPSSweeper tool appears.

4. Type C, and then enter the day and time you want. If you want to enter several days or times, separate them with commas or spaces. Use the following format:

   ```
   Mon@13:30,Tue@14:00
   ```

   The new and old settings appear. The values you added are shown at the bottom of the settings as a "pending value."

5. Do the following:
   a. Enter Q twice.
   b. Enter L.
   c. Enter Q to end your XPS session.

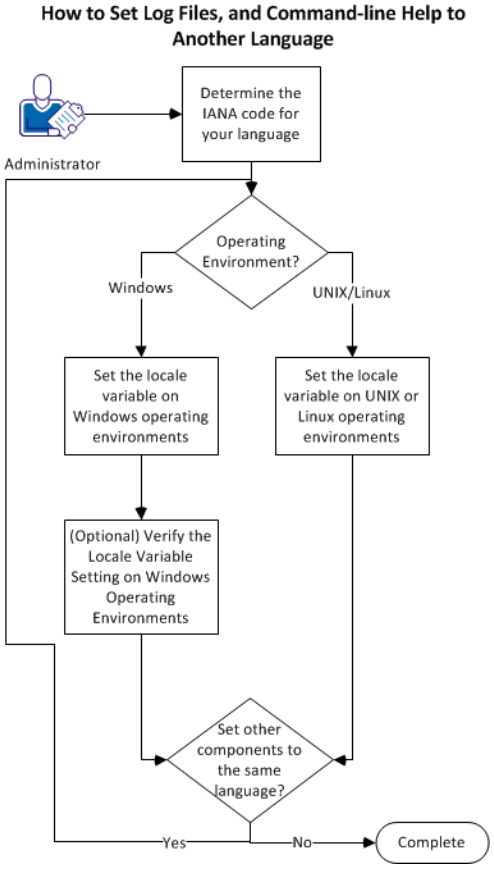
   Your changes are saved and the command prompt appears.

Set Log Files, and Command-line Help to Another Language

The following components support log files, and command-line help in other languages:

- The Policy Server
- The Web Agent
- The Report Server
- The CA SiteMinder Agent for SharePoint
- The CA SiteMinder® SPS
- [set AGENT value for your book]s
- Any custom software that is created with the CA SiteMinder® SDK.

The following graphic describes the work flow for setting log files, and command-line help to another language:



Follow these steps:

1. Determine the IANA code for your language (see page 56).
2. Create the environment variable for your operating environment using one of the following procedures:
   - Set the locale variable on Windows operating environments (see page 57).
   - Set the locale variable on UNIX or Linux operating environments (see page 59).
3. (Optional) Verify the locale variable setting on windows operating environments (see page 58).
4. (Optional) Repeat Steps 1 through 3 to set any other components in your environment to the same language.

Determine the IANA Code for Your Language

Each language has a unique code. The Internet Assigned Numbers Authority (IANA) assigns these language codes. Adding a language code to a locale variable changes the language that the software displays. Determine the proper code for the language that you want before creating the locale variable.

The following table lists the IANA codes that correspond to the languages supported by the software:

Language	IANA Code
Brazilian Portuguese	pt_BR
French	fr
German	de
Italian	it
Japanese	ja
Korean	ko
Simplified Chinese	zh-Hans
Spanish	es

Note: A list of IANA language codes is available from this third-party website.

Environment Variables

The environment variables are settings by which users can customize a computer to suit their needs. Examples of environment variables include the following items:

- A default directory for searching or storing downloaded files.
- A username.
- A list of locations to search for executable files (path).

Windows operating environments allow global environment variables, which apply to all users of a computer. The environment variables on UNIX or Linux operating environments must be set for each user or program.

To set the locale variable, pick the procedure for your operating environment from the following list:

- Set the locale variable on Windows operating environments (see page 57).
- Set the locale variable on UNIX or Linux operating environments (see page 59).

Set the Locale Variable on Windows Operating Environments

The following locale variable specifies the language settings for the software:

SM_ADMIN_LOCALE

Create this variable and set it to the language that you want. Set this variable on *each* component for which you want to use another language. For example, suppose you want to have a Policy Server and an agent that is set to French. Set this variable on both of those components to French.

Note: The installation or configuration programs do *not* set this variable.

Follow these steps:

1. Click Start, Control Panel, System, Advanced system settings.

   The system properties dialog appears.

2. Click the Advanced tab.

3. Click Environment Variables.

4. Locate the System variables section, and then click New.

   The New System Variable dialog opens with the cursor in the Variable name: field.

5. Type the following text:

   SM_ADMIN_LOCALE

6. Click the Variable name: field, and then type the IANA language code (see page 56) that you want.

7. Click OK.

   The New System Variable dialog closes and the SM_ADMIN_LOCALE variable appears in the list.

8. Click OK *twice*.

   The locale variable is set.

9. (Optional) Repeat Steps 1 through 8 to set other components to the same language.

Verify the Locale Variable Value on Windows Operating Environments

You can very the value to which the locale variable is set at any time. You can do this procedure after setting the variable to confirm that it is set correctly.

Note: Instructions for verifying the variable value on UNIX and Linux are in the setting procedure (see page 59).

Follow these steps:

1. Open a command-line window with the following steps:
   a. Click Start, Run.
   b. Type the following command:

      ```
      cmd
      ```

   c. Click OK.

      A command-line window opens.
2. Enter the following command:

   ```
   echo %SM_ADMIN_LOCALE%
   ```

   The locale appears on the next line. For example, when the language is set to German, the following code appears:

   ```
   de
   ```

   The value of the locale variable is verified.

Set the Locale Variable on UNIX or Linux Operating Environments

The following locale variable specifies the language settings for the software:

`SM_ADMIN_LOCALE`

Create this variable and set it to the language that you want. Set this variable on *each* component for which you want to use another language. For example, suppose you want to have a Policy Server and an agent that is set to French. Set this variable on both of those components to French.

Note: The installation or configuration programs do *not* set this variable.

Follow these steps:

1. Log in to the computer that is running the component that you want.
2. Open a console (command-line) window.
3. Enter the following command:

   `export SM_ADMIN_LOCALE=IANA_language_code`

   The command in the following example sets the language to French:

   `export SM_ADMIN_LOCALE=fr`

   The locale variable is set.
4. (Optional) Verify that the locale variable is set properly by entering the following command:

   `echo $SM_ADMIN_LOCALE`

   The locale appears on the next line. For example, when the language is set to German, the following code appears:

   `de`
5. (Optional) Repeat Steps 1 through 4 to set other components to the same language.

Chapter 5: Certificate Data Store Management

This section contains the following topics:

Certificate Revocation List Updates

CA SiteMinder® provides features that require certificate validation for certificates in the certificate data store. In 12.52 SP1, federation features use the certificate data store. These features include protecting the HTTP-Artifact back channel, verifying SAML messages, and encrypting SAML messages. The certificate data store can implement validity checking using certificate revocation lists (CRLs).

The certificate data store references the location of CRLs. By default CA SiteMinder® does not check for CRL updates. Enable the CRL updater (CRLUpdater) to check for updates.

Consider the following information:

- CA SiteMinder® uses the NextUpdate date of each CRL to determine when to reference the stored location and when to reload the CRL. CA SiteMinder® also uses the date to determine whether to invalidate any certificates.
- By default, CA SiteMinder® checks for updates once an hour. You can increase the default frequency.
- Enabling CRL updates is a local Policy Server administration setting. Only enable CRL updates for one Policy Server in the environment.
- If a CRL fails to load, all certificates are marked revoked until the CRL successfully loads.

Follow these steps:

1. Log in to a Policy Server host system.
2. Start the XPSConfig utility.
3. Type CDS and press Enter.
4. Type the number for EnableCRLUpdater and press Enter.
5. Type C and press Enter.

6. Type yes and press Enter.
7. Type Q.
8. Complete one of the following steps
   - To change the frequency at which CA SiteMinder® checks for updates:
     a. Type the number for DefaultCRLUpdaterSleepPeriod and press Enter.
     b. Type C and press Enter.
     c. Enter a new value and press Enter.
     d. Quit the utility.
   - To leave the default frequency, quit the utility.
9. Restart the Policy Server.

   CRL list updates are scheduled.

Change the Default CRL Update Period

The update period is the frequency that the certificate data store reloads a CRL. If a stored CRL file does not contain a NextUpdate value, configure the update period. The data store looks for the updated CRL in the location you specified when you added the CRL file to the CA SiteMinder® configuration.

Follow these steps:

1. Log in to the Administrative UI.
2. Select Infrastructure, X509 Certificate Management, CDS Settings.
3. Enter a new value for the update period. The default is one day.
4. Click Save.

The new value is the amount of time that passes between updates.

OCSP Updates

CA SiteMinder® provides features that require certificate validation for certificates in the certificate data store. In 12.52 SP1, federation features use the certificate data store. These features include protecting the HTTP-Artifact back channel, verifying SAML messages, and encrypting SAML messages.

To check the validity of certificates, the certificate data store can use an OCSP service. OCSP uses an HTTP service that a Certificate Authority (CA) provides to supply certificate validation on demand.

By default, CA SiteMinder® does not check the revocation status of a certificate in the certificate data store. To check the revocation status through an OCSP responder, use the OCSP updater utility (OCSPUpdater). When enabled, the OCSPUpdater checks the revocation status for configured OCSP responders every 5 minutes. This default frequency is configurable.

Configuration of the OCSPUpdater relies on the following components:

- SMocsp.conf File

  The OCSPUpdater uses the SMocsp.conf file for OCSP responder configuration. Each Certificate Authority (CA) that issues certificates has its own OCSP responder. In the SMocsp.conf file, include every OCSP responder for each CA certificate in the certificate data store.

  An SMocsp.conf file must exist to use the OCSPUpdater.

  Note: The SMocsp.conf file is the same file that the CA SiteMinder® X.509 certificate authentication scheme uses to configure its own OCSP implementation.

- XPSConfig utility

  XPSConfig lets you customize the behavior of the OCSPUpdater, such as enabling it and setting the frequency of updates. The customization is local to the Policy Server running the OCSPUpdater. Enable an OCSPUpdater on only one Policy Server in a CA SiteMinder® deployment.

Failover Between OCSP and CRL Checking

The certificate data store supports failover from OCSP to CRL validation. If you configure CRLs and OCSP checking, you can enable failover between the two.

CA SiteMinder® federation features do not support certificate distribution point extensions with failover configured, even if the extensions are in a certificate.

For more information about failover, refer to the certificate validity checking section in the *Policy Server Configuration Guide*.

Schedule OCSP Updates

OCSP updates are scheduled using XPSConfig.

Important! Enabling OCSP updates is a local Policy Server administration setting. Enable the OCSPUpdater on only one Policy Server in a CA SiteMinder® deployment.

To schedule OCSP updates

1. Log in to a Policy Server host system.
2. Start the XPSConfig utility.

3. Type CDS and press Enter.
4. Type the number for EnableOCSPUpdater and press Enter.
5. Type C and press Enter.
6. Type yes and press Enter.
7. Type Q.
8. Do one of the following tasks:
   - Change the frequency at which CA SiteMinder® checks for updates:
     a. Type the number for DefaultOCSPUpdaterSleepPeriod and press Enter.
     b. Type C and press Enter.
     c. Enter a new value and press Enter.
     d. Quit the utility.
   - Leave the default frequency by quitting the utility.
9. Restart the Policy Server.

OCSP revocation status updates are now scheduled. For updates to initiate, a federated single sign-on transaction must occur. The Policy Server where the OCSPUpdater is enabled must run this first transaction. Other Policy Servers in the deployment can make subsequent transactions.

Modify the SMocsp.conf file for OCSP Updates

The OCSPUpdater uses the SMocsp.conf file for responder configuration values. This file is the same file that the X.509 certificate authentication scheme uses to configure its OCSP implementation; however, not all settings for the authentication scheme apply for federation.

The SMocsp.conf file must reside in the directory *siteminder_home*/config.

Important! An entry for a given CA in the SMocsp.conf file does not mean that OCSP is enabled. You also have to set the EnableOCSPUpdater setting to Yes.

To edit the file

1. Navigate to *siteminder_home*/config.
2. Open the file in a text editor.

3. Do one of the following tasks:
   - Modify an existing OCSPResponder entry.
   - Add a unique OCSPResponder entry for each IssuerDN that matches an IssuerDN in your certificate mapping.

     Important! If an Issuer DN is missing a responder record or the configuration is invalid, the Policy Server performs certificate operations without confirming the validity of the certificate.
4. Edit the file settings which can affect updates.

   Important! Only one file can exist on the one Policy Server where OCSP is enabled.
5. Save the file.
6. If the OCSPUpdater is already enabled, restart the Policy Server. Otherwise, you can load the edited SMocsp.conf file using following smkeytool command:

   ```
   smkeytool -loadOCSPConfigFile
   ```

More information:

SMocsp.conf Settings Used by Federation (see page 65)

SMocsp.conf Settings Used by Federation

Guidelines for modifying the SMocsp.conf file are as follows:

- Names of settings are not all case-sensitive. Case sensitivity for entries is dependent on the particular setting.
- If a setting in the file is left blank, the Policy Server sends an error message. The message indicates that the entry is invalid. The Policy Server ignores the setting. If you intended to leave the setting blank, disregard the message.
- Do not put leading white spaces in front of the name of a setting.

In the SMocsp.conf file, you can configure the following settings for federation:

OCSPResponder

Required. Indicates that the entry is an OCSP responder record. Each OCSP Responder record must start with the name OCSPResponder.

IssuerDN

Required. Specifies the DN of the certificate issuer. This value labels each OCSP Responder record in the file.

Entry: The Issuer DN value in the certificate.

AlternateIssuerDN

Optional. Specifies a secondary IssuerDN or reversed DN.

ResponderLocation

Optional. Indicates the location of the OCSP responder server.

You can use the ResponderLocation setting or the AIAExtension setting, but note the following conditions:

- If the ResponderLocation setting is left blank or it is not in the SMocsp.conf file, set the AIAExtension setting to YES. Additionally, an AIA extension must be in the certificate.
- If the ResponderLocation setting has a value and the AIAExtension is set to YES, the Policy Server uses the ResponderLocation for validation. The ResponderLocation setting takes precedence over the AIAExtension.
- If the OCSP responder specified for this setting is down and the AIAExtension is set to YES, authentication fails. The Policy Server does not try the responder specified in the AIA extension of the certificate.

If you enter a location, enter the value in the form *responder_server_url*:*port_number*.

Enter a URL and port number of the responder server.

AIAExtension

Optional. Specifies whether the Policy Server uses the Authority Information Access extension (AIA) in the certificate to locate validation information.

You can use the AIAExtension or ResponderLocation settings, but note the following caveats:

- If AIAExtension is set to YES and the ResponderLocation is not configured, the Policy Server uses the AIA Extension in the certificate for validation. The extension has to be in the certificate.
- If the AIAExtension is set to YES and ResponderLocation setting also has a value, the Policy Server uses the ResponderLocation for validation. The ResponderLocation setting takes precedence over the AIAExtension.
- If AIAExtension is set to NO, the Policy Server uses the ResponderLocation setting. If a value for the AIAExtension exists, the Policy Server disregards it.

Enter YES or NO.

Default: NO

HttpProxyEnabled

Optional. Tells the Policy Server to send the OCSP request to the proxy server, not to the web server.

Enter YES or NO.

Default: NO

HttpProxyLocation

Optional. Specifies the URL of the proxy server. This value is only required if HttpProxyEnabled is set to YES.

Enter a URL beginning with http://.

Note: Do not enter a URL beginning with https://.

HttpProxyUserName

Optional. Specifies the user name for the login credentials to the proxy server. This user name must be the name of a valid user of the proxy server. This value is only required if HttpProxyEnabled is set to YES.

Enter an alphanumeric string.

HttpProxyPassword

Optional. Specifies the password for the proxy server user name. This value is displayed in clear text. This value is only required if HttpProxyEnabled is set to YES.

Enter an alphanumeric string.

SignRequestEnabled

Optional. Instructs the Policy Server to sign the generated OCSP request. Set this value to Yes to use the signing feature.

This value is independent of any user certificate signatures and is only relevant for the OCSP request.

Note: This setting is required only if the OCSP responder requires signed requests.

Enter YES or NO.

Default: NO

SignDigest

Optional. Designates the algorithm the Policy Server uses when signing the OCSP request. This setting is not case-sensitive. This setting is required only if the SignRequestEnabled setting is set to YES.

Enter one of the following options: SHA1, SHA224, SHA256, SHA384, SHA512

Default: SHA1

Alias

Optional. Specifies the alias for the key/certificate pair that signs the OCSP request that is sent to an OCSP responder. This key/certificate pair must be in the CA SiteMinder® certificate data store.

Note: The alias is required only if the SignRequestEnabled setting is set to YES.

Enter an alias using lower-case ASCII alphanumeric characters.

IgnoreNonceExtension

Optional. Tells the Policy Server not to include the nonce in the OCSP request. The nonce (number that is used once) is a unique number sometimes included in authentication requests to prevent the reuse of a response. Setting this parameter to Yes instructs the Policy Server *not* to include the nonce in the OCSP request.

Enter YES or NO.

Default: NO

PrimaryValidationMethod

Optional. Indicates whether OCSP or CRL is the primary method the Policy Server uses to validate certificates. This setting is only required if the EnableFailover setting is set to Yes.

Enter OCSP or CRL.

Default: OCSP

EnableFailover

Tells the Policy Server to failover between OCSP and CRL certificate validation methods.

Enter YES or NO.

Default: NO

ResponderCertAlias

Required for federation only. Names the alias of the certificate that verifies the signature of the OCSP response. For the Policy Server to perform response signature verification, specify an alias for this setting. Otherwise, the CA issuer has no available OCSP configuration.

Note: The Policy Server does not use this setting for X.509 certificate authentication.

Enter a string that names the alias.

You can see whether each issuer has an OCSP configuration after the SMocsp.conf file is loaded. The following message is a sample status message:

```
The SMocsp.conf file was loaded.
OCSP configuration was added for the following issuer aliases:
ocspcacert
ocspcacert1
ocspcacert2
```

The issuer alias in the status message refers to the alias you specified in the Administrative UI when adding a CA certificate to the data store. If an issuer alias is not in the list, check the SMocsp.conf and the cds.log file. The log file is located in *siteminder_home*\log.

RevocationGracePeriod

Optional–for federation only. Specifies the period (in days) to delay the invalidation of a certificate after it is revoked. The OCSP grace period gives you time to update certificates so that the configuration does not suddenly stop working. A value of 0 indicates that when a certificate is revoked it becomes invalid immediately.

If you do not specify a value for this field, the Policy Server uses the default revocation grace period setting in the Administrative UI. You can find the default setting by navigating to Infrastructure> X509 Certificate Management > Certificate Management.

Default: 0

Disabling OCSP

Disable the OCSP configuration for a specific CA by removing the issuer entry from the SMocsp.conf file. If you disable the OCSPUpdater, remove all entries from the file previously enabled.

Follow these steps:

1. Open the SMocsp.conf file in an editor. The SMocsp.conf file resides in the directory *siteminder_home*/config.
2. Delete the associated issuer entry from the SMocsp.conf file.
3. Using the smkeytool utility, enter the following command:

```
smkeytool -loadOCSPConfigFile
```

OCSP for the specific CA issuer is disabled.

Adding a CA Certificate When OCSP is Disabled

If you disable the OCSPUpdater but a given issuer has an entry in the SMocsp.conf file, the Policy Server prevents the addition of a certificate for that same issuer. If you try to add a certificate, the Policy Server logs an error message. The error occurs because OCSP is configured for the issuer, but the OCSPUpdater is not enabled. As a result, the revocation status check cannot be performed. If you try adding a certificate with the same issuer, the addition fails.

To add a CA certificate without causing an error

1. Open the SMocsp.conf file in an editor. The SMocsp.conf file resides in the directory *siteminder_home*/config.
2. Remove the configuration for the relevant CA.
3. Using XPSConfig, set the EnableOCSPUpdater to Yes to reenable OCSP.
4. Load the SMocsp.conf file by entering the following command at a command line:

```
smkeytool -loadOCSPConfigFile
```

5. Reset the EnableOCSPUpdater parameter to No as you originally intended.

Certificate Cache Refresh Period

The certificate cache refresh period indicates how often the certificate data store updates the certificate data in the policy store. Certificate data is cached in memory to improve CA SiteMinder® performance. Refresh the information in memory so that the data is current.

Follow these steps:

1. Log in to the Administrative UI.
2. Select Infrastructure, X509 Certificate Management, CDS Settings.
3. Enter a new value for the certificate cache refresh period, in seconds. The default is 300 seconds.
4. Click Save.

The refresh period is configured.

Default Revocation Grace Period

The default revocation grace period is the delay, in days, from when a certificate is revoked and the time the certificate becomes invalid. During the grace period, CA SiteMinder® can use a revoked certificate before it becomes invalid. After the certificate becomes invalid, it is no longer active and CA SiteMinder® cannot use it.

This default grace period applies to CRLs and OCSP responders. If you do not specify a value for the CRL grace period when adding a CRL to the system, CA SiteMinder® uses the default grace period. If you do not configure an OCSP grace period in the SMocsp.conf file, CA SiteMinder® uses the default grace period. The individual grace period settings for a CRL or OCSP take precedence over this default grace period value.

Follow these steps:

1. Log in to the Administrative UI.
2. Select Infrastructure, X509 Certificate Management, CDS Settings.
3. Enter a new value for the revocation grace period, in days. The default is 0, which means that when a certificate is revoked it becomes invalid immediately.
4. Click Save.

The revocation grace period is defined.

Chapter 6: Changing the Policy Server Super User Password

This section contains the following topics:

Super User Password Overview

The Super User is the Policy Server administrator account established automatically by the Policy Server installation process. You can change the Super User password from the Management Console Super User tab.

Note: Changing the Super User Account Password in this dialog box does not enable the Super User if it has been previously disabled by using the Administrative UI.

Change the Policy Server Super User Password

To change the Policy Server super user password

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. Use Administrator permissions even if you are logged in to the system as an Administrator. For more information, see the release notes for your CA SiteMinder® component.

2. Click the Super User tab.

   Note: For more information about the settings and controls on this tab, click Help, Management Console Help.

3. In the Old Password field, enter the current password of the Super User.

4. In the New Password field, enter the new password of the Super User.

   Note: The CA SiteMinder® superuser administrator's password may not contain the pipe (|), greater than (>), or less than (<) characters.

5. In the Confirm Password field, enter the new password to verify it.

6. Click Apply to save the Super User changes, or click OK to save the settings and close the Console.

   Note: Changes to the Super User account password take effect without restarting the Policy Server process.

Chapter 7: Configuring Policy Server Logging

This section contains the following topics:

Policy Server Logging Overview

The Policy Server log file records information about the status of the Policy Server and, optionally, configurable levels of auditing information about authentication, authorization, and other events in the Policy Server log file. If the Policy Server is configured as a RADIUS Server, RADIUS activity is logged in the RADIUS log file.

You configure these logs from the Management Console Logs tab.

Configure the Policy Server Logs

To configure the Policy Server logs

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. Use Administrator permissions even if you are logged in to the system as an Administrator. For more information, see the release notes for your CA SiteMinder® component.

2. Click the Logs tab.

   Note: For more information about the settings and controls on this tab, click Help, Management Console Help.

3. Adjust the settings presented in the Policy Server Log and Policy Server Audit Log group boxes to configure the location, rollover characteristics and required level of audit logging for the Policy Server log.

4. If the Policy Server is configured as a RADIUS server, adjust the settings presented in the RADIUS Log group box.
5. Click Apply to save your changes.

Record Administrator Changes to Policy Store Objects

By default, CA SiteMinder® administrator changes to policy store objects are written to a set of XPS text files that are located at *siteminder_home*\audit.

The audit logs are stored as text files, as shown in the following example:

policy_server_home/audit/xps-*process_id-start_time-audit_sequence*.*file_type*

The name of each audit log file contains the following information:

process_id

Indicates the number of the process associated with the audited event.

start_time

Indicates the time the transaction *started* in the following format:

YYYYMMDDHHMMSS

A four-digit year and the 24-hour clock are used.

Example: 20061204133000

audit_sequence

Provides a sequence number for the audited event.

file_type

Indicates one of the following event types:

access

Indicates an audit log file that contains the following access events:

- a Administrative UI or a reports server is registered
- a Administrative UI or a reports server acts as a proxy on behalf of another user
- an administrator is denied access for a requested action

audit

Indicates an audit log file that contains the following events:

- an object is modified (using an XPS Tool or Administrative UI)
- administrator records are created, modified, or deleted

txn

Indicates an audit log file that contains the following transaction events:

- An XPS tool begins, commits, or rejects a change to an object.

Note: If you do *not* have write access to the CA SiteMinder® binary files (XPS.dll, libXPS.so, libXPS.sl), an Administrator must grant you permission to use the related XPS command line tools using the Administrative UI or the XPSSecurity tool.

To change the default setting

1. Access the Policy Server host system.
2. Open a command line and enter the following command:

   ```
   xpsconfig
   ```

   The tool starts and displays the name of the log file for this session, and a menu of choices opens.

3. Enter the following:

   xps

   A list of options appears.

4. Enter the following:

   1

   The current policy store audit settings appear.

5. Enter C.

   Note: This parameter uses a value of TRUE or FALSE. Changing its value toggles between the two states.

   The updated policy store audit settings appear. The new value is shown at the bottom of the list as "pending value."

6. Do the following:

   a. Enter Q twice.

   b. Enter Q to end your XPS session.

   Your changes are saved and the command prompt appears.

How to Process Old Log Files Automatically

You can configure CA SiteMinder® Policy Server to automatically process old log files by customizing one of the following scripts:

- Harvest.bat (Windows)
- Harvest.sh (UNIX or Linux)

The script runs when one of the following events occurs:

- When the XPSAudit process starts (using the following option)

  CLEANUP

  Processes all of the log files in the directory at once.
- Whenever the log files are rolled over
- When the XPSAudit process exits

  During a rollover or an exit, the files are processed one-at-a-time by file name.

You can customize the script to process the files any way you want. For example, you could modify the script to delete them, move them to a database or archive them to another location.

Note: This script is provided only as an example. It is not supported by CA.

To automatically process old log files, do the following:

1. Open the following directory on your Policy Server:

   policy_server_home/audit/samples
2. Open the appropriate script for your operating system with a text editor, and then save a copy to the following directory:

   policy_server_home/audit/Harvest.*extension*

   Note: Do *not* rename the file or save it to a location different from the one specified.
3. Use the remarks in the script as a guide to customize the script according to your needs.
4. Save your customized script and close the text editor.

How to Include CA SiteMinder® Administrative Audit Events in Reports

If you have a CA SiteMinder® report server and an audit database, you can configure the Policy Server to collect administrative audit events. You import this data in to the audit database, so you can include it in any reports you generate.

A sample Perl script is installed with the CA SiteMinder® Policy Server that you can customize to meet your needs.

To include administrative audit events in your CA SiteMinder® reports, use the following process:

1. Copy the sample scripts on the Policy Server by doing the following:
   a. Open the following directory:

      policy_server_home\audit\samples

      Note: The following directories are the default locations for the *policy_server_home* variable:

      - C:\Program Files\ca\siteminder (Windows)
      - /opt/ca/siteminder (UNIX, Linux)

   b. Locate the following files:

      - Harvest.bat (for Windows)
      - Harvest.sh (for UNIX, Linux)
      - ProcessAudit.pl
      - Categories.txt

   c. Copy the previous files to the following directory:

      policy_server_home\audit
2. (Optional) Customize the ProcessAudit.pl script.
3. After the next scheduled run of the XPSAudit command, copies of the audit logs are created using the comma-separated value (CSV) format, and stored as .TMP files in the following directory:

   policy_server_home\audit_R6tmp

   Note: If you have events you want to generate manually to a .tmp file, run the following command in the policy_server_home\audit directory:

   ```
   ProcessAudit.pl <Transaction id>
   ```

   The smobjlog4 database table lists the following 11 attributes and values. Only the first 8 are generated in the .TMP file:

   ```
   sm_timestamp        DATE DEFAULT SYSDATE NOT NULL,
   sm_categoryid       INTEGER DEFAULT 0 NOT NULL,
   sm_eventid          INTEGER DEFAULT 0 NOT NULL,
   sm_hostname         VARCHAR2(255) NULL,
   sm_sessionid        VARCHAR2(255) NULL,
   sm_username         VARCHAR2(512) NULL,
   sm_objname          VARCHAR2(512) NULL,
   sm_objoid           VARCHAR2(64) NULL,
   sm_fielddesc        VARCHAR2(1024) NULL,
   sm_domainoid        VARCHAR2(64) NULL,
   sm_status           VARCHAR2(1024) NULL
   ```

4. Copy the .TMP files from the previous directory on the Policy Server to the server that hosts your audit database.
5. Create one of the following files to map the CSV-formatted contents of the .TMP files to your database schema:
   - *control_file_name*.ctl (control file for Oracle databases)
   - *format_file_name*.fmt (format file for SQL Server databases)

   Note: For more information, see the documentation or online help provided by your database vendor.
6. On the server that hosts your audit database, run whichever of the following commands is appropriate for your type of database:
   - sqlldr (for Oracle databases)
   - bcp (for SQL Server databases)

   Note: For more information, see the documentation or online help provided by your database vendor.
7. After the command finishes, use the reports server to generate a report of administrative events.

   The administrative audit events appear in the report.

Mirror ODBC Audit Log Content in Text-based Audit Logs on Windows

When the CA SiteMinder® audit logs are stored as text files, they include a partial list of the available fields by default. If you want the text files that contain your audit logs to include all of the available fields, like an ODBC Audit database does, you can add a registry key to your Policy Server.

To mirror ODBC Audit log content in text-based audit logs

1. Open the registry editor.
2. Expand the following location:

   `HKEY_LOCAL_MACHINE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Reports\`
3. Create a new DWORD value with the following name:

   `Enable Enhance Tracing`
4. Set the Value to 1. If you want to disable this setting in the future, change the value back to 0.
5. Restart your Policy Server.

   The ODBC Audit log content will appear in your text-based audit logs.

Mirror ODBC Audit Log Content in Text-based Audit Logs on Solaris

When the CA SiteMinder® audit logs are stored as text files, they include a partial list of the available fields by default. If you want the text files that contain your audit logs to include all of the available fields, like an ODBC Audit database does, you can add a registry key to your Policy Server.

To mirror ODBC Audit log content in text-based audit logs

1. Open the following file:

   ```
   sm.registry
   ```

2. Locate the following line:

   ```
   -
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\R
   eports=25089
   ```

3. Add a new line beneath the previous one with the following text:

   ```
   - Enable Enhance Tracing= 0x1; REG_DWORD
   ```

   Note: If you want to disable this feature in the future, change the 0x1 to 0x0.

4. Restart your Policy Server.

   The ODBC Audit log content will appear in your text-based audit logs.

Report Logging Problems to the System Log

You can configure the Policy Server to log information about exceptions that can occur while preparing or executing audit logs to the Windows event log viewer. This configuration can prevent you from missing this information in a production environment where debug logs are disabled. To configure this feature, set the value of the CategoryCount registry key to 7.

The CategoryCount registry key is found in the following registry location:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application
\SiteMinder
```

These events are logged under the event log categories ObjAuditLog and AccessAuditLog.

CA SiteMinder® calls object events when objects are created, updated, or deleted. Any exceptions that occur while preparing/executing CA SiteMinder® obj audit logs are logged to Windows event viewer under the 'ObjAuditLog' category.

Access events result from user-related activities and are called in the context of authentication, authorization, administration, and affiliate activity. Any exceptions that occur while preparing/executing CA SiteMinder® access audit logs are logged to Windows event viewer under the 'AccessAuditLog' category.

Configure Certificate Data Store Logging

Configure the certificate data store log to change the default settings. By default, the log is configured to:

- Log information to the following file:

  cds.log

  This log is located in *siteminder_home*\log.

  siteminder_home

  Specifies the Policy Server installation path.

- Include informational and error messages.
- Rollover and create a backup when the file size reaches 500 KB.
- Keep ten backup copies before the oldest is erased.

Follow these steps:

1. Navigate to *siteminder_home*\config\properties and open the following file:

   cdslog4j.properties

   Note: For more information about log4j, see the Apache website.

2. Do one or more of the following:

   - To change the logging level, update the value at the end of the following parameter:

     `log4j.logger.com.ca.CertificateDataStore=`

     Important! Do not remove the following from the parameter or logging fails:

     `, CertificateDataStore`

   - To change the output location or log name, update the file path at the end of the following parameter:

     `log4j.appender.CertificateDataStore.File=`

   - To change the size at which a file rolls over and a backup is created, update the value at the end of the following parameter:

     `log4j.appender.CertificateDataStore.MaxFileSize=`

- To change the number of backup copies that are kept before the oldest is erased, update the value at the end of the following parameter:

  `log4j.appender.CertificateDataStore.MaxBackupIndex=`

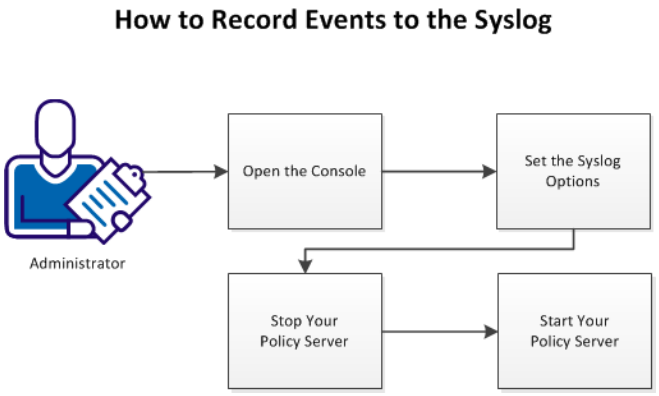
Note: Do not modify the settings in the ClientDispatcher section, unless CA SiteMinder® Support asks you. These settings are for debugging purposes only.

3. Save the file.

   Certificate data store logging is configured.

How to Record Events to the Syslog

Administrators can record Policy Server events to the syslog on supported operating environments. The following graphic describes how to record events to the syslog:



Follow these steps:

1. Open the console (see page 85).
2. Set the syslog options (see page 85).
3. Restart your Policy Server with the following steps:
   - Stop your Policy Server (see page 88).
   - Start your Policy Server (see page 88).

Open the Console

To change your settings, open the console.

Follow these steps:

1. Verify that an X-windows server is running on your system.
2. Open a terminal window.
3. Set the DISPLAY variable with the following command:

   ```
   export DISPLAY=IP_address:0.0
   ```

   IP_address

   Specifies the IP address of where the console window appears. Use the IP address of the system from which you are *connecting to* the console.

   Example: (IPV4) 192.168.1.1

   Example: (IPV6) 2001:DB8::/32
4. Log in to the system hosting the console.
5. Navigate to the following directory:

   ```
   installation_directory/siteminder/bin
   ```

   installation_directory

   Specifies the location in the file system where the Policy Server is installed.

   Default: /opt/CA/siteminder
6. Open the console by running the following command:

   ```
   ./smconsole
   ```

Set the Syslog Options

Setting the syslog options on the console specifies which events are recorded in the syslog.

Note: For more information about the Syslog and its settings, see this website.

Follow these steps:

1. Enable syslog recording with the following steps:
   a. Click the Data tab.
   b. Click the Database drop-down list, and then pick Audit Logs.
   c. Click the Storage drop-down list, and then pick Syslog.

2. Select the text in the Priority field, and then type the value that you want from the following list:

   Priority

   Specifies the event priority recorded in the syslog. Pick *one* of the following values:

   - LOG_EMERG
   - LOG_ALERT
   - LOG_CRIT
   - LOG_ERR
   - LOG_WARNING
   - LOG_NOTICE
   - LOG_INFO
   - LOG_DEBUG

   Default: LOG_INFO

3. Select the text in the Facility field, and then type value that you want from the following list:

   Facility

   Specifies which events in the operating environment are recorded to the syslog. Pick *one* of the following values:

   - LOG_AUTH
   - LOG_AUTHPRI
   - LOG_CRON
   - LOG_DAEMON
   - LOG_FTP
   - LOG_KERN
   - LOG_LPR
   - LOG_MAIL
   - LOG_NEWS
   - LOG_SYSLOG
   - LOG_USER
   - LOG_UUCP
   - LOG_LOCAL0
   - LOG_LOCAL1
   - LOG_LOCAL2
   - LOG_LOCAL3
   - LOG_LOCAL4
   - LOG_LOCAL5
   - LOG_LOCAL6
   - LOG_LOCAL7

   Default: LOG_AUTH

4. (Optional) Replace the text in the following field:

   Text

   Specifies the text in an event that you want to record in the syslog. For example, if you specify the word tiger, then any events containing the word tiger are recorded in the syslog.

   Default: Siteminder

5. Click OK.

   The console closes and the syslog options are set.

Stop a UNIX Policy Server

Stopping a Policy Server has the following results:

- The Policy Server is temporarily removed from your environment.
- Agents who need authorization or authentication decisions cannot contact the stopped Policy Server. Those Agents can still connect to other Policy Servers that are available.
- All logging activity stops.

Follow these steps:

1. Log in to the system hosting the Policy Server with the same user account that installed the Policy Server originally.
2. Stop all Policy Server processes, with *one* of the following actions:
   - Open the Management Console, click the Status tab, and then click the Stop buttons.
   - Use the following script. This script also stops the UNIX executive so that the processes do not restart automatically.

     ```
     installation_path/siteminder/stop-all
     ```

     The Policy Server logs all UNIX executive activity in the installation_directory/log/smexec.log file. Log entries are always appended to the existing log file.

Start a UNIX Policy Server

Starting Policy Server has the following results:

- Agents contact the Policy Server for authorization or authentication decisions.
- Logging begins.

Start all Policy Server processes, with *one* of the following actions:

- Open the Management Console, click the Status tab, and then click the Start buttons.
- Use the following script. This script also starts the UNIX executive.

  ```
  installation_path/siteminder/start-all
  ```

  The Policy Server logs all UNIX executive activity in the installation_directory/log/smexec.log file. Log entries are always appended to the existing log file.

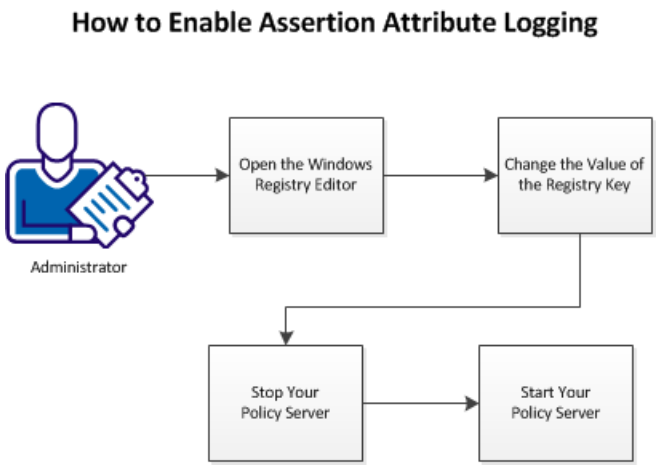
How to Enable Assertion Attribute Logging on Windows Operating Environments

You can record information about the assertion attributes to the audit logs. Use these logs for a security audit, or during an investigation. The type of event determines the information that is recorded in the log. The following events are recorded when you enable assertion-attribute logging:

- Any assertion generations
- Any assertion consumptions
- Any authentication success
- Any authentication failures
- Any authentication attempts
- Any application access

The logging of assertion attributes is disabled by default. Enable assertion-attribute logging on your Policy Server.

The following graphic describes how to enable assertion attribute logging:



Follow these steps:

1. Open the Windows registry editor (see page 90).
2. Change the value of the registry key.
3. Restart your Policy Server with the following steps:
   a. Stop your Policy Server (see page 92).
   b. Start your Policy Server (see page 92).

Open the Windows Registry Editor

Change this setting by opening the Windows registry editor on the system hosting your Policy Server.

Follow these steps:

1. Click Start, Run.
2. Type the following text in the Open: Field.

   ```
   regedit
   ```

3. Click OK.

   The Windows registry editor opens.

Change the Value of the Registry Key

The following registry key controls attribute assertion logging:

Enable Enhance Tracing

Indicates whether attribute assertions are recorded in the audit logs. A value of 2 enables logging. A value of 3 enables logging and records the authentication method of the user. A value of 4 enables logging for Enhanced Session Assurance with DeviceDNA™

Limits: 0, 2, 3, 4

Default: 0 (logging disabled)

Follow these steps:

1. In the registry editor, expand the following item:

   `HKEY_LOCAL_MACHINE`
2. Click Software, Netegrity, SiteMinder, Currentversion, Reports.
3. Locate the following registry key:

   `Enable Enhance Tracing`
4. Right-click the key, and then pick Modify.
5. Do *one* of the following tasks:
   - To enable the logging of assertion attributes, change the value to 2.
   - To enable the logging of the assertion attributes and the authentication method used, change the value to 3.
   - To enable the logging for Enhanced Session Assurance with DeviceDNA™, change the value to 4.
   - To disable the logging of assertion attributes, change the value to 0.
6. Click OK.
7. Close the registry editor.

   The value of the Enable Enhance Tracing registry key is changed.

Stop a Windows Policy Server

Stop your Policy Server before continuing. Stopping a Policy Server has the following results:

- The Policy Server is temporarily removed from your environment.
- Agents who need authorization or authentication decisions cannot contact the stopped Policy Server. Those Agents can still connect to other Policy Servers that are available.
- All logging activity stops.

Follow these steps:

1. Log in to the Policy Server host system.

   Note: Use an account with administrator privileges.
2. Click Start, Programs, SiteMinder, SiteMinder Policy Server Management Console.
3. Click the Stop button.
4. Click OK.

   The Policy Server stops and the console closes.

Start a Windows Policy Server

Start the Policy Server. Starting Policy Server has the following results:

- Agents contact the Policy Server for authorization or authentication decisions.
- Logging begins.

Follow these steps:

1. Click Start, Programs, SiteMinder, SiteMinder Policy Server Management Console.

   The console opens with the Status tab selected.
2. Click the Start buttons.
3. Click OK.

   The Policy Server starts.

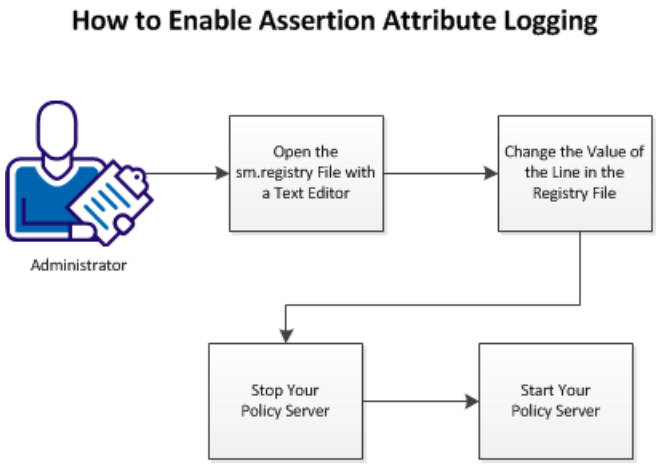
How to Enable Assertion Attribute Logging on UNIX or Linux Operating Environments

You can record information about the assertion attributes to the audit logs. Use these logs for a security audit, or during an investigation. The type of event determines the information that is recorded in the log. The following events are recorded when you enable assertion-attribute logging:

- Any assertion generations
- Any assertion consumptions
- Any authentication success
- Any authentication failures
- Any authentication attempts
- Any application access

The logging of assertion attributes is disabled by default. Enable assertion-attribute logging on your Policy Server.

The following graphic describes how to enable assertion-attribute logging:



Follow these steps:

1. Open the sm.registry file with a text editor (see page 94).
2. Change the value of the line in the registry file.
3. Restart your Policy Server with the following steps:
   a. Stop your Policy Server (see page 88).
   b. Start your Policy Server. (see page 88)

Open the sm.registry File with a Text Editor

Change this setting on UNIX or Linux operating environments by opening the sm.registry file with a text editor. The sm.registry file is stored on your Policy Server.

Follow these steps:

1. Navigate to the following directory:

   Installation_Directory/registry

   installation_directory

   Specifies the location in the file system where the Policy Server is installed.

   Default: /opt/CA/siteminder

2. Open the following file with a text editor:

   sm.registry

   You can now change the settings.

Change the Value of the Line in the Registry File

The following entry in the sm.registry file controls attribute assertion logging:

Enable Enhance Tracing

Indicates whether attribute assertions are recorded in the audit logs. A value of 2 enables logging. A value of 3 enables logging and records the authentication method of the user. A value of 4 enables logging for Enhanced Session Assurance with DeviceDNA™

Limits: 0, 2, 3, 4

Default: 0 (logging disabled)

Follow these steps:

1. Locate the following section of the sm.registry file:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Reports=
   ```

2. Locate the following line in the Reports section:

   ```
   Enable Enhance Tracing=      0; REG_DWORD
   ```

3. Change the zero to *one* of the following values:
   - 2 (enables logging)
   - 3 (enables logging and records the authentication method)
   - 4 (enables logging for Enhanced Session Assurance with DeviceDNA™)

4. Verify that the line in your sm.registry file matches *one* of the following examples:

   ```
   Enable Enhance Tracing=      2; REG_DWORD
   ```

   ```
   Enable Enhance Tracing=      3; REG_DWORD
   ```

   ```
   Enable Enhance Tracing=      4; REG_DWORD
   ```

5. Save the changes to the sm.registry file, and then close the text editor.

   The value of the line in the registry file is changed.

Stop a UNIX Policy Server

Stopping a Policy Server has the following results:

- The Policy Server is temporarily removed from your environment.
- Agents who need authorization or authentication decisions cannot contact the stopped Policy Server. Those Agents can still connect to other Policy Servers that are available.
- All logging activity stops.

Follow these steps:

1. Log in to the system hosting the Policy Server with the same user account that installed the Policy Server originally.
2. Stop all Policy Server processes, with *one* of the following actions:
   - Open the Management Console, click the Status tab, and then click the Stop buttons.
   - Use the following script. This script also stops the UNIX executive so that the processes do not restart automatically.

     ```
     installation_path/siteminder/stop-all
     ```

     The Policy Server logs all UNIX executive activity in the installation_directory/log/smexec.log file. Log entries are always appended to the existing log file.

Start a UNIX Policy Server

Starting Policy Server has the following results:

- Agents contact the Policy Server for authorization or authentication decisions.
- Logging begins.

Start all Policy Server processes, with *one* of the following actions:

- Open the Management Console, click the Status tab, and then click the Start buttons.
- Use the following script. This script also starts the UNIX executive.

  ```
  installation_path/siteminder/start-all
  ```

  The Policy Server logs all UNIX executive activity in the installation_directory/log/smexec.log file. Log entries are always appended to the existing log file.

Chapter 8: Configuring and Managing Encryption Keys

This section contains the following topics:

Policy Server Encryption Keys Overview

The Policy Server and Agents use encryption keys to encrypt and decrypt sensitive data passed between Policy Servers and Agents in a SiteMinder environment.

- Agent keys are used to encrypt SiteMinder cookies that may be read by all agents in a single sign-on environment, and are shared by all agents in a single sign-on environment, since each agent must be able to decrypt cookies encrypted by the other agents. Agent keys are managed by the Policy Server, and distributed to agents periodically.
- Session ticket keys are used by the Policy Server to encrypt session tickets. Session tickets contain credentials and other information relating to a session (including user credentials). Agents embed session tickets in SiteMinder cookies, but cannot access the contents since they do not have access to session ticket keys which never leave the Policy Server.

Both types of keys are kept in the Policy Server's key store and distributed to Agents at runtime. By default, the key store is part of the Policy Store, but a separate key store database can be created if desired.

Other, special keys are:

- A policy store key is used to encrypt certain data in the policy store. The policy store key is stored, encrypted, in an on-disk file. The Policy Server encrypts the policy store key using a proprietary technique. The policy store key is derived from the encryption key specified when you installed the Policy Server.
- A key store key is used to encrypt agent and session ticket keys in a separately configured key store. The key store key is kept in the registry (or UNIX equivalent) encrypted with the policy store key.

Key Management Overview

To keep key information updated across large deployments, the Policy Server provides an automated key rollover mechanism. You can update keys automatically for Policy Server installations that share the same key store. Automating key changes helps ensure the integrity of the keys.

For CA SiteMinder® agents that are configured for single sign–on:

- Replicate the key store.
- Share the replicated store across all CA SiteMinder® environments in the single sign–on environment.

If the Policy Server determines that a stand–alone key store is unavailable, it attempts to reconnect to the key store to determine availability. If the connection fails, the Policy Server:

- Goes in to a suspended state and refuses any new requests on established connections until the key store comes back online.

  A Policy Server in a suspended state remains up for the length of time specified in SuspendTimeout. The Policy Server then shuts down gracefully. If SuspendTimeout is equal to zero, the Policy Server remains in the suspended state until the key store connection is reestablished.
- Returns an error status to let web agents failover to another Policy Server.
- Logs the appropriate error messages.

Additionally, when the Policy Server is started and the key store is unavailable, the Policy Server shuts down gracefully.

Use the Administrative UI to manage keys.

FIPS 140-2 Algorithms

The Federal Information Processing Standards (FIPS) 140-2 publication specifies the requirements for using cryptographic algorithms within a security system protecting sensitive, unclassified data. SiteMinder embeds RSA 's Crypto-C ME v2.0 cryptographic library, which has been validated as meeting the FIPS 140-2 *Security Requirements for Cryptographic Modules.* The validation certificate number for this module is 608.

SiteMinder's Java-based APIs use a FIPS-compliant version of the Crypto-J cryptographic library.

SiteMinder can operate in a pre-FIPS mode or in a FIPS-only mode. The cryptographic boundaries, that is, the way SiteMinder applies encryption, are the same in both modes, but the algorithms are different.

In FIPS-only mode, SiteMinder uses the following algorithms:

- AES Key Wrap for key encryption.
- AES in OFB mode (HMAC-SHA 256) for channel encryption.
- AES in CBC mode (HMAC-SHA 224) for encrypting tokens used to facilitate single sign-on.

The SiteMinder core components make extensive use of encrypted data:

- The Web Agent encrypts:
  - Cookies using an Agent Key retrieved from the Policy Server
  - Data sent to the Policy Server using a Session Key
  - A Shared Secret using the Host Key. The encrypted Shared Secret is stored in the Host Configuration file.
- The Policy Server encrypts:
  - Data sent to the Web Agent using a Session Key
  - The Policy Store Key using the Host Key
  - Sensitive data in the Policy Store using the Policy Store Key
  - Session Spec using the Session Ticket Key
  - Data sent to the Administrative UI using a Session Key
  - Password Services data in a user directory using the Session Ticket Key

The Policy Store Key is used to encrypt sensitive data stored in the Policy Store. It is derived from a seed string entered during the installation of the Policy Store. The Policy Store Key is also encrypted, using the Host Key, and stored in a system-local file. To support unattended operation, the Host Key is a fixed key embedded in the Policy Store code. Agents use this same Host Key mechanism to encrypt and store their copies of their Shared Secrets.

The Session Ticket Key (used by the Policy Server to form authentication tokens) and Agent Keys (primarily used by Web Agents to encrypt cookie data) are encryption keys stored in the Policy Store (or Key Store, depending on SiteMinder configuration settings) in encrypted form. They are encrypted using the Policy/Key Store Key. The Key Store Key is encrypted in the Policy Store. Agent Shared Secrets (used for Agent authentication and in the TLI Handshake), along with other sensitive data, are also encrypted with the Policy Store Key and stored in the Policy Store.

Agent Keys Introduced

SiteMinder Web Agents use an Agent key to encrypt cookies before passing the cookies to a user's browser. When a Web Agent receives a SiteMinder cookie, the Agent key enables the Agent to decrypt the contents of the cookie. Keys must be set to the same value for all Web Agents communicating with a Policy Server.

The Policy Server provides the following types of Agent keys:

- *Dynamic Keys* are generated by a Policy Server algorithm and are distributed to connected Policy Servers and any associated SiteMinder Web Agents. Dynamic keys can be rolled over at a regular interval, or by using the Key Management dialog box of the Administrative UI. For security reasons, this is the recommended type of Agent key.
- *Static Keys* remain the same indefinitely, and can be generated by a Policy Server algorithm or entered manually. SiteMinder deployments uses this type of key for a subset of features that require information to be stored in cookies on a user's machine over extended periods of time.

  Note: A static agent key is always generated at installation. This static key is used for certain other product features, such as user management, whether or not you use the static key as the Agent key.

More information:

Dynamic Agent Key Rollover (see page 101)

Dynamic Agent Key Rollover

Dynamic Agent key rollover is configured in the Key Management dialog of the FSS Administrative UI. Web Agents poll the Policy Server for key updates at a regular interval. If keys have been updated, Web Agents pick up the changes during polling. The default polling time is 30 seconds, but can be configured by changing the pspollinterval parameter of a Web Agent.

Note: For information about changing the parameters of a Web Agent, see the *CA SiteMinder® Web Agent Configuration Guide*.

The Policy Server uses an algorithm to generate dynamic keys at a regular interval. These keys are saved in the key store. When a Web Agent detects new keys, it retrieves them from the key store.

Dynamic Agent Key Rollover

You configure dynamic agent key rollover in the Administrative UI. Web agents poll the Policy Server for key updates at a regular interval. If keys have been updated, web agents pick up the changes during polling. The default polling time is 30 seconds, but you can change the default by changing the pspollinterval parameter of a web agent.

Note: For information about changing the parameters of a web agent, see the *CA SiteMinder® Web Agent Configuration Guide*.

The Policy Server uses an algorithm to generate dynamic keys at a regular interval. These keys are saved in the key store. When a web agent detects new keys, it retrieves them from the key store.

Agent Keys Used in Dynamic Key Rollover

CA SiteMinder® deployments use the following keys in a dynamic key rollover and maintain them in the key store:

- An Old Key is a Dynamic key that contains the last value used for the Agent key before the current value.
- A Current Key is a Dynamic key that contains the value of the current Agent key.
- A Future Key is a Dynamic key that contains the next value that will be used as the Current key in an Agent key rollover.
- Static Key

When the Policy Server processes a dynamic Agent key rollover, the value of the current key replaces the value of the old key. The value of the future key replaces the value of the current key, and the Policy Server generates a new value for the future key.

When receiving a cookie from a client browser, the Web Agent uses the current key from the key store to decrypt the cookie. If the decrypted value is not valid, the Web Agent tries the old key, and if necessary, the future key. The old key may be required to decrypt cookies from an Agent that has not yet been updated, or to decrypt existing cookies from a client's browser. The future key may be required for cookies created by an updated Agent, but read by an Agent that has not yet polled the key store for updated keys.

Rollover Intervals for Agent Keys

At a specified time, the Agent key rollover process begins. To prevent multiple rollovers from multiple Policy Servers, each server sets a rollover wait time of up to 30 minutes. If no update has been performed by the end of the wait time, that Policy Server updates the keys.

All Policy Servers wait for updated keys and then process the new keys to their Agents. Even for a single Policy Server, the update time may be up to 30 minutes beyond the time specified for the rollover.

The Agent Key Rollover process begins at the time(s) specified in the CA SiteMinder® Agent Key Management dialog box. The process can take up to three minutes. In that time period, all Web Agents connected to the Policy Server receive updated keys.

Note: In a deployment that involves multiple replicated Policy Servers, the process for distributing Agent keys may take up to 30 minutes.

Static Keys

A static key is a string used to encrypt data which remains constant. In a SiteMinder deployment that uses the Agent Key rollover feature, a static key provides a method for maintaining user information across an extended period of time.

The following SiteMinder features and situations make use of the static key:

- Saving User Credentials for HTML Forms Authentication

  If an HTML Forms authentication scheme has been configured to allow users to save credentials, the Policy Server uses the static key to encrypt the user's credentials.

- User Tracking

  If user tracking is turned on, the Policy Server uses the static key to encrypt user identity information.

- Single Sign-on Across Multiple Key Stores

  In a SiteMinder deployment that includes multiple key stores, the static key may be used for single sign-on. In this situation, SiteMinder Agents use the static key for all cookie encryption.

  Note: If you change the static key, any cookies created with the former static key are invalid. Users may be forced to re-authenticate, and user tracking information becomes invalid. In addition, if the static key is used for single sign-on, users are challenged for credentials when they attempt to access resources in another cookie domain.

More information:

Multiple Policy Stores with Separate Key Stores (see page 108)

Session Ticket Keys

When a user successfully logs into a protected resource, the Policy Server creates a session ticket. The session ticket is what the Policy Server uses to determine how long a user's authentication remains valid. This session ticket is encrypted using the *session ticket key* and cached in the Agent User Cache.

You can choose to have the Policy Server generate the session ticket key using an algorithm, or you can enter a session ticket key in the CA SiteMinder® Key Management dialog box. For security reasons, the randomly generated key is recommended.

However, if your CA SiteMinder® implementation includes multiple key stores in a single sign-on environment, you must use the same session ticket key for all key stores.

More information:

Manage the Session Ticket Key (see page 117)
Cache Management Overview (see page 137)

Key Management Scenarios

There are three types of scenarios for key management based on how you implement Policy Servers, policy stores and key stores, along with your single sign-on requirements. These scenarios include:

- Common Policy Store and Key Store

  In this scenario, a group of Policy Servers shares a single policy store and key store, providing access control and single sign-on in a single cookie domain.

  The policy store data is maintained in a single policy store. Key data is maintained in a single key store. The key store may be part of the policy store, or may be a separate store.

  Both policy store and key store data may be replicated for failover purposes. Replication must be configured based on the database or directory type selected for the policy store. For information about replication schemes, consult the documentation provided by your database or directory vendor.

- Multiple Policy Stores with a Common Key Store

  In this scenario, groups of Policy Servers connect to separate policy stores, but share a common key store, providing access control and single sign-on across multiple cookie domains.

  The policy store data for each group of Policy Servers is maintained in a single policy store. Key data for all groups of Policy Servers is maintained in a single key store. The separate key store allows Agents associated with all Policy Servers to share keys, enabling single sign-on across separate cookie domains.

  Both policy store and key store data may be replicated for failover purposes. Replication must be configured based on the database or directory type selected for the policy store. For information about replication schemes, consult the documentation provided by your database or directory vendor.

- Multiple Policy Stores and Multiple Key Stores

  In this scenario, each group of Policy Servers shares a single policy store and key store, providing access control and single sign-on across multiple cookie domains where it is desirable for the Policy Servers in each cookie domain to have a separate key store.

  The policy store data for each group of Policy Servers is maintained in a single policy store. Key data for each group of Policy Servers is maintained in a single key store. The key store may be part of the policy store, or may be a separate store. The same set of static keys allows for single sign-on across all Web Agents.

  Both policy store and key store data may be replicated for failover purposes. Replication must be configured based on the database or directory type selected for the policy store. For information about replication schemes, consult the documentation provided by your database or directory vendor.

More information:

Configure LDAP Failover (see page 35)
Configure ODBC Failover (see page 45)

Key Management Considerations

When deciding on the key management scenario for your enterprise, consider the following:

- When configuring dynamic keys in an environment with multiple Policy Servers that share a common key store, a single Policy Server must be nominated to perform Agent Key generation. You should disable key generation on all other Policy Servers.
- In a network configuration with multiple Policy Servers, the Policy Server Management Console enables you to specify a policy store for each Policy Server. Policy stores can be master policy stores that are the primary location for storing CA SiteMinder® objects and policy information, or they can be replicated policy stores that use data copied from a master policy store.
- Master/slave directories or databases must be configured according to the specifications of the directory or database provider. The Policy Server provides the ability to specify a failover order for policy stores, but it does not control data replication. For information about replication schemes, see your directory or database provider's documentation.
- In any network that uses dynamic key rollover, the key store for a Policy Server may be a master key store or a replicated slave key store. Master key stores receive keys directly from the Policy Server process that generates the keys. Slave key stores receive copies of the keys in the master key store.
- In a master/slave environment, you must configure key generation from Policy Servers that point to the master policy store and key store. The master policy store and key store data must then be replicated across all other policy stores and key stores included in your failover order.
- In any single sign-on environment for multiple cookie domains, dynamic keys can only be used if there is a single master key store, or slave key stores with keys replicated from a single master key store.
- Policy stores and keys stores can be installed on mixed LDAP and ODBC directories. The policy store can reside in an ODBC database and the key store can reside in an LDAP Directory Server or vice versa. For a list of supported databases, go to the Technical Support site and search for the CA SiteMinder® 12.52 SP1 Platform Support Matrix.

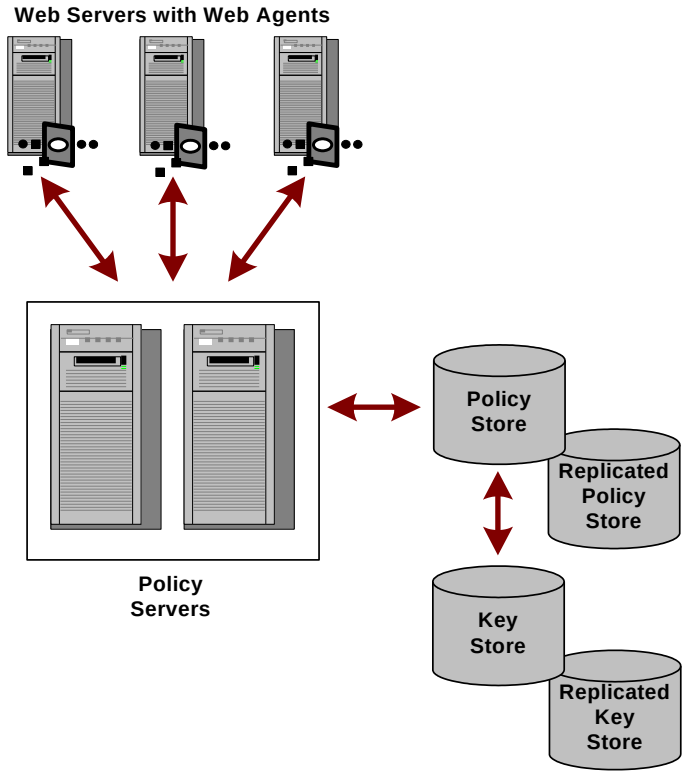
More information:

Configure Agent Key Generation (see page 113)
Configure LDAP Failover (see page 35)
Configure ODBC Failover (see page 45)

Common Policy Store and Key Store

The simplest scenario for a SiteMinder configuration that uses key rollover is when multiple Policy Servers use a single policy store (and its associated failover policy stores), along with a single key store.

The following figure shows multiple Policy Servers using a single policy store.



In this type of configuration, Policy Servers retrieve dynamic keys from the key store. The Web Agents associated with the Policy Servers collect new keys from the Policy Servers.

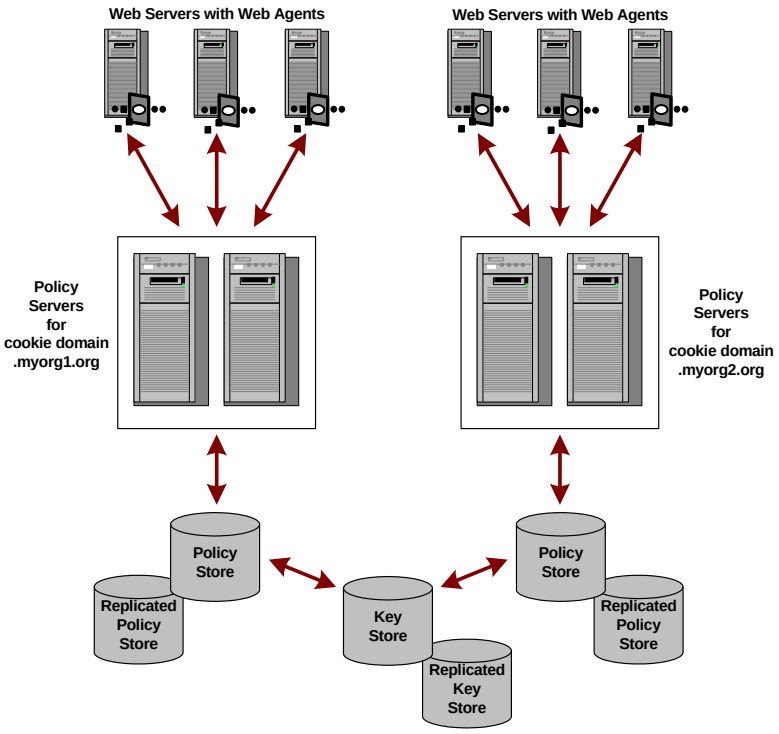
More information:

Key Management Considerations (see page 105)

Multiple Policy Stores with a Common Key Store

If a network configuration consists of multiple Policy Servers with separate policy stores in a single sign-on environment, it is possible to have a common key store that all of the Policy Servers use for key rollover.

The following figure shows multiple Policy Servers using a common key store.



One Policy Server generates dynamic keys and stores them in the central key store. Each Policy Server is configured using the Policy Server Management Console to use the central key store; Agent key generation should be disabled for all other Policy Servers. Agents poll their respective Policy Servers to retrieve new keys. The Policy Servers retrieve new keys from the common key store and pass them to the CA SiteMinder® Agents.

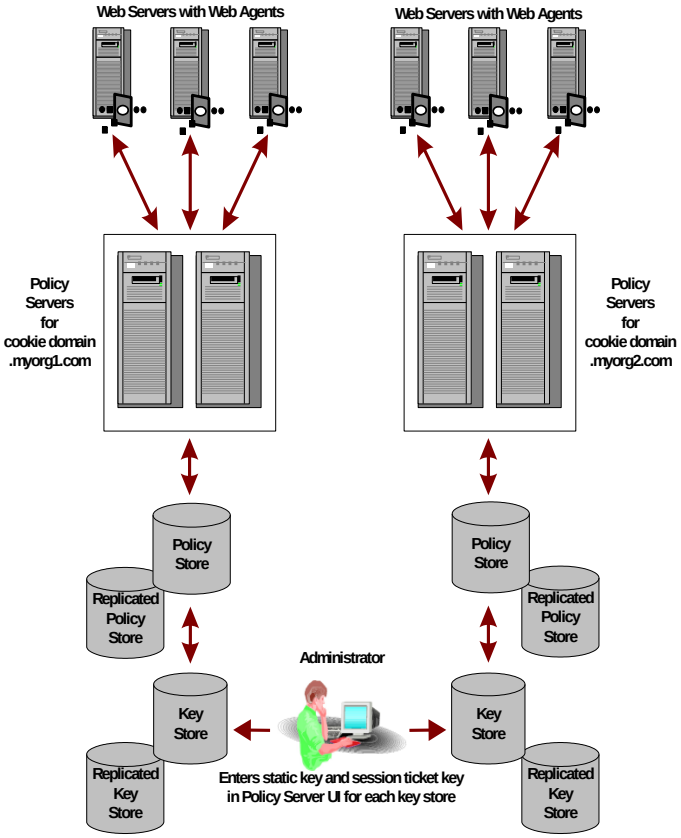
Note: This scenario requires an additional registry setting that forces Policy Servers that are not generating keys to poll the key store for key updates.

Multiple Policy Stores with Separate Key Stores

If a network configuration is composed of multiple Policy Servers, policy stores, and master key stores, an administrator with appropriate privileges can specify the same static key and session ticket key for each policy store in order to facilitate one or more of the following:

- Single sign-on across all Agents
- Password Services with a common user directory

The following figure shows an environment with multiple Policy Servers and stores.



In the previous example, the same static key is used to encrypt all cookies created by CA SiteMinder® Web Agents.

More information:

Key Management Considerations (see page 105)

Reset the r6.x Policy Store Encryption Key

To reset the r6.x policy store encryption key

1. Log into a Policy Server host system.
2. Run the following command:

   `smobjexport -d`*siteminder_administrator* `-w`*password* `-o`*file_name* `-c`

   -d*siteminder_administrator*

   Specifies the name of the CA SiteMinder® administrator account.

   Note: This administrator must be able to manage all CA SiteMinder® domain objects.

   -w*password*

   Specifies the password of the CA SiteMinder® administrator account.

   -o*file_name*

   Specifies the following:

   - The path to the output location
   - The name of smdif file the utility creates

   Note: If this argument is not specified, the default output file names are stdout.smdif and stdout.cfg.

   -c

   Exports sensitive data as clear–text.

   The utility exports the policy store data into the smdif file.
3. Be sure that the smreg utility is located in *policy_server_home*\bin.

   policy_server_home

   Specifies the Policy Server installation path.

   Note: If the utility is not present, you can find the utility in the Policy Server installation media, which is available on the Support site.
4. Run the following command:

   `smreg -key` *encryption_key*

   encryption_key

   Specifies the new encryption key.

   Limits: 6 to 24 characters.

   The policy store encryption key is changed.
5. Start the Policy Server Management Console and open the Data tab.

6. Re–enter the policy store administrator password and click Update.

   The administrator password is re–encrypted using the new encryption key.

7. Run the following command:

   `smreg -su password`

   password

   Specifies the CA SiteMinder® super user password.

   The super user password is set and encrypted using the new encryption key.

8. Run the following command:

   `smobjimport -dsiteminder_administrator -wpassword -ifile_name -r -f -c`

   -d*siteminder_administrator*

   Specifies the name of the CA SiteMinder® administrator account.

   Note: This administrator must be able to manage all CA SiteMinder® domain objects.

   -w*password*

   Specifies the password of the CA SiteMinder® administrator account.

   -i*file_name*

   Specifies the following:

   - The path to the smdif file
   - The name of the smdif file name

   Note: If this argument is not specified, the default input file names are stdout.smdif and stdout.cfg.

   -r

   Specifies that duplicate policy store information can be overwritten during the import.

   -f

   Turns off automatic renaming of objects. By default, when the utility attempts to import an object with a name that exists in the target policy store, the utility creates a duplicate object. The name of the object is *nameoid.*

   name

   Specifies the name of the object.

   oid

   Specifies the object ID of the new duplicate object.

   The utility returns errors messages for any objects that could not be created because of naming conflicts.

-c

Indicates that the input file contains sensitive data in clear–text.

9. Run the following command:

```
smreg -su password
```

password

Specifies the CA SiteMinder® super user password.

The super user password is set.

The policy store encryption key is reset.

Reset the r12.x Policy Store Encryption Key

Follow these steps:

1. Log in to the Policy Server host system.
2. Stop the Policy Server.

   Note: Stop all Policy Servers pointing to the policy store before changing the encryption key.
3. Export a full-backup of the policy store contents using XPSExport

   xpsexport <filename> -xb –npass

   or (for encrypted output)

   xpsexport <filename> -xb –pass <password>
4. Export the Agent Keys using smkeyexport (clear-text option is required)

   smkeyexport –o <filename> -d<sm admin name> -w<smadmin password> -c
5. Change the policy store encryption key

   smreg –key <new key>
6. Reset and test the policy store password using SmConsole

   Use the "Data" tab of SmConsole to re-enter the previously configured password, apply the change and then use the "Test Connection" button to verify.
7. Import the policy store contents using XPSImport using export taken in Step 3.

   xpsimport <filename> –fo –pass <password>

   or (if no password was used to create the export file):

   xpsimport <filename> –fo –npass
8. Import the Agent Keys using smkeyimport (clear-text option) using export taken in Step 4.

   smkeyimport –i<filename> -d<sm admin name> -w<sm admin password> -c
9. Restart the Policy Server.

The policy store encryption key is reset.

Configure Agent Key Generation

You use the Policy Server Management Console Keys tab to configure how the Policy Sever handles Agent key generation.

Note: Enable key generation only on the Policy Server that you want to generate Agent keys.

Follow these steps:

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. Use Administrator permissions even if you are logged in to the system as an Administrator. For more information, see the release notes for your CA SiteMinder® component.

2. Click the Keys tab.

   Note: For more information about the settings and controls on this tab, click Help, Management Console Help.

3. Complete the fields and controls presented on the Keys tab to configure Agent key generation.

4. When you are done, click Apply to save your changes.

Manage Agent Keys

The SiteMinder Key Management dialog box, which you access from the Administrative UI, enables you to configure periodic Agent key rollovers, execute manual rollovers, and change the static key. It also enables you to manage the session ticket key.

Note: To manage keys, you must log into the Administrative UI using an account with the Manage Keys and Password Policies privilege. For more information, see the *Policy Server Configuration Guide*.

More information:

Manage the Session Ticket Key (see page 117)

Configure Periodic Key Rollover

The Policy Server supports periodic Agent key rollovers at the following frequencies:

- Weekly
- Daily
- Fixed intervals in a single day

The shortest allowable period between rollovers is one hour.

Note: Be sure that your operating system is configured to adjust the system time for daylight savings time. A system that is not configured for daylight savings time can offset key rollover by one hour.

Follow these steps:

1. Access the Policy Server Management Console and open the Keys tab.
2. Select Enable Agent Key Generation and click OK.
3. Log in to the Administrative UI.
4. Click Administration, Policy Server.
5. Click Key Management, Agent Key Management.
6. Select Use dynamic Agent key in the Agent Key section.

   Important! After selecting Use dynamic Agent key, you cannot click Rollover Now until you save the periodic key rollover configuration settings.
7. Select Automatic key rollover in the Dynamic key Detail section.
8. Click Set rollover frequency.
9. Specify the frequency at which the rollovers must occur.
10. Click OK.
11. Click Submit.

    Agent key rollover is configured.

Manually Rollover the Key

You can roll over dynamic agent keys manually. This feature:

- Provides added security. You can execute a rollover at anytime.
- Permits flexibility. You can configure the Policy Server to generate dynamic keys, but do not have to specify a rollover frequency.

Follow these steps:

1. Access the Policy Server Management Console and open the Keys tab.
2. Select Enable Agent Key Generation and click OK.
3. Log in to the Administrative UI.
4. Click Administration, Policy Server.
5. Click Key Management, Agent Key Management.
6. Select Use dynamic Agent key in the Agent Key section.
7. Select Manual key rollover in the Dynamic key detail section.
8. Click Rollover Now.

   The Policy Server generates new agent keys immediately. Unless you manually execute an agent key rollover, the Policy Server does not generate new dynamic keys automatically.

Note: Do not click this button multiple times, unless you want to roll over keys more than once.

Web agents pick up the new keys the next time they poll the Policy Server. This action can take up to 3 minutes due to cache synchronization. If you want to use an entirely new set of keys for security reasons, roll over dynamic keys twice. This action removes the old key and the current key from the key store.

Coordinate Agent Key Management and Session Timeouts

You must coordinate the updating of agent keys and session timeouts or you may invalidate cookies that contain session information. This coordination is critical because the person designing policies in your organization may be different than the person configuring dynamic key rollover.

Session timeouts should be less than or equal to two times the interval configured between Agent key rollovers. If an administrator configures an agent key rollover to occur two times before a session expires, cookies written by the Web Agent before the first key rollover will no longer be valid and users will be re-challenged for their identification *before* their session terminates.

For example, if you configure key rollover to occur every three hours, you should to set the Maximum Session timeout to six hours or less to ensure that multiple key rollovers do not invalidate the session cookie.

Change Static Keys

You can change the static gent key web agents use to encrypt identity information for certain features.

Important! We do not recommend changing the static key. Change the static key only in extreme situations, such as security breaches. This action can cause some CA SiteMinder® features to lose the data they require to function properly. Features that establish and use an identity stored in a persistent cookie will no longer work. Authenticated users can be forced to log in again before single sign–on functions across multiple CA SiteMinder® installations.

A static key can also be used to maintain a single sign–on environment that requires multiple Policy Servers and multiple master key stores.

Follow these steps:

1. Log in to the Administrative UI.
2. Click Administration, Policy Server.
3. Click Key Management, Agent Key Management.
4. Select Use static Agent key in the Agent Key section.
5. Do one of the following:
   - Click Rollover Now in the Generate a random Agent Key section.

     The Policy Server generates a new random static key.
   - Enter a static agent key in the Specify an Agent Key section.

     Use this option in situations where two key stores must use the static key to maintain a single sign–on.
6. Click Rollover Now.
7. Click Submit.

   The static key rolls over within 3 minutes.

Manage the Session Ticket Key

The Policy Server can generate the session ticket key using an algorithm, or you can enter the session ticket key manually. A session ticket is established each time a user authenticates successfully and enables the Policy Server to determine how long a user's session can continue.

Note: The only implementation that requires a manually assigned session ticket key is one that includes multiple, independent key stores. Automatically generated keys cannot be propagated across independent key stores by the Policy Server. In all other instances it is recommended that you use the session ticket key generated by the Policy Server algorithm.

Generate a Session Ticket Key

The Policy Server can generate the session ticket key using a method similar to the one for generating dynamic agent keys. Randomly generating the session ticket key lets the Policy Server use an algorithm to create the key used for encryption and decryption.

Follow these steps:

1. Log in to the Administrative UI.
2. Click Administration, Policy Server.
3. Click Key Management, Session Key Management.
4. Do one of the following:
   - Click Rollover Now in the Generate a Random Session Ticket Key section.

     The Policy Server generates a new session ticket key. This key immediately replaces the one that is used to encrypt and decrypt session tickets.
   - Specify a session ticket in the Specify Session Ticket Key section and click Rollover Now.

     The Policy Server immediately replaces the existing session ticket key with the value you entered.
5. Click Submit.

Manually Enter the Session Ticket Key

If your Policy Server is part of an implementation that includes multiple key stores, you can manually enter the session ticket key.

Follow these steps:

1. Log in to the Administrative UI.
2. Click Administration, Policy Server.
3. Click Key Management, Session Key Management.
4. Specify a key in the Specify a Session Ticket key section.
5. Click Rollover Now.

   The Policy Server immediately replaces the existing session ticket key with the value you entered.
6. Click Submit.

Set the EnableKeyUpdate Registry Key

When a single Policy Server generates encryption keys in an environment with multiple Policy Servers that connect to disparate policy stores, but share a central key store, an additional registry setting is required. This registry setting configures each Policy Server to poll the common key store and retrieve new encryption keys at a regular interval.

To configure the EnableKeyUpdate registry key on a Windows Policy Server

1. From the Windows Start menu, select Run.
2. Enter regedit in the Run dialog box and click OK.
3. In the Registry Editor, navigate to:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\ObjectStore`
4. Change the following registry value:

   "EnableKeyUpdate"=0

   to

   "EnableKeyUpdate"=1
5. Restart the Policy Server.

To configure the EnableKeyUpdate registry key on a UNIX Policy Server

1. Navigate to:

   install_directory/siteminder/registry

2. Open sm.registry in a text editor.

3. Locate the following text in the file:

   HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\
   CurrentVersion\ObjectStore

4. Change the following registry value:

   "EnableKeyUpdate"=0

   to

   "EnableKeyUpdate"=1

5. Restart the Policy Server.

More information:

Multiple Policy Stores with a Common Key Store (see page 107)

Shared Secret for a Trusted Host

When you register a trusted host, the installation process:

- Automatically generates a shared secret for the web agent
- Stores the shared secret in the Host Configuration file (SmHost.conf) file.

If you enabled shared secret rollover when registering a trusted host, you can roll over the shared secrets for trusted hosts either manually or periodically.

During a manual or periodic shared secret rollover, shared secrets are only rolled over for agents that were configured at installation to allow rollovers.

Note: For more information about installing web agents and registering trusted hosts, see the *CA SiteMinder® Web Agent Installation Guide*.

Shared secret rollover occurs automatically only on servers that are configured to enable agent key generation. You enable agent key generation by selecting the Enable Agent Key Generation check box in the Keys tab of the Policy Server Management Console. This setting is enabled by default.

Important! We recommend that you only enable one Policy Server to generate keys. If there are multiple policy stores in an environment, but only a single shared key store, not all shared secrets roll over automatically. The shared secrets are only rolled over automatically if the Policy Server to which the policy store is configured is enabled for key generation. All other policy stores require that you execute a rollover manually.

Use one of the following to roll over the shared secret manually:

- The Administrative UI.
- The C Policy Management API running on a Policy Server that is configured with the target policy store.

Note: The shared secret policy object is kept in the key store. All policy stores that share the same key store share the same secret. The shared secrets themselves are kept in the trusted host objects, which are part of the policy store.

Configure Trusted Host Shared Secret Rollover

The Policy Server supports manual and periodic rollover of shared secrets for trusted hosts.

Periodic rollovers can be configured hourly, daily, weekly, or monthly; one hour is the shortest allowable period between rollovers. The Policy Server initiates periodic rollovers based on the age of the shared secret for each trusted host, rather than at a specific time of the day, week, or month. By rolling over each shared secret as it expires, the processing associated with the rollover is distributed over time, and avoids placing a heavy processing load on the Policy Server.

If you use the manual rollover feature, future periodic rollovers will generally be clustered together for all trusted hosts, since the manual rollover sets new shared secrets for all trusted hosts that allow shared secret rollover.

Important! If you enable key generation on more than one Policy Server associated with a single policy store, the same shared secret can be rolled over more than once in a short period of time due to object store propagation delays. This can result in orphaned hosts whose new shared secrets have been discarded. To avoid this potential problem, enable shared secret rollover for a single Policy Server per policy store.

Follow these steps:

1. In the Keys tab of the Policy Server Management Console, ensure that the Enable Agent Key Generation check box is selected.
2. Log into the Administrative UI.
3. Click Administration, Policy Server, Shared Secret Rollover.

4. In the Shared Secret Rollover group box, do one of the following:
   - For an immediate rollover, click Rollover Now.
   - To ensure that the shared secret is never rolled over, select Never Rollover Shared Secret.
   - To specify a period rollover, select Rollover Shared Secret every and complete the following fields:

     Rollover Frequency

     Enter an integer for the number of times a rollover should occur. This number works together with the value of the rollover period.

     Rollover Period

     From the pull-down list, select Hours, Days, Weeks or Months for the occurrence of the rollover.

   The Policy Server begins the process of rolling over shared secrets for all trusted hosts configured to allow shared secret rollover. The rollover may take some time depending on the number of trusted hosts in your deployment.
5. Click Submit to save your changes.

Chapter 9: Configuring the Policy Server Profiler

This section contains the following topics:

Configure the Policy Server Profiler

The Policy Server Profiler allows you to trace internal Policy Server diagnostics and processing functions.

Follow these steps:

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. Use Administrator permissions even if you are logged in to the system as an Administrator. For more information, see the release notes for your CA SiteMinder® component.

2. Click the Profiler tab.
3. Set the Enable Profiling option to enable profiling.
4. To select configuration settings for the Profiler, do one of the following:
   - Accept the Profiler settings specified by the default smtracedefault.txt file presented in the Configuration File drop-down list.
   - Select another configuration file that has already been selected during this management session from the Configuration File drop-down list.
   - Click the Browse button to select another configuration file.
5. To change the Profiler settings stored in a Profiler configuration file and save them in the same or a new file, click the Configure Settings button to open the Policy Server Profiler dialog.
6. Adjust the settings presented in the Output group box to specify the output format for information generated by the Policy Server Profiler.
7. Click Apply to save your changes.

Notes:

Changes to the Profiler settings take effect automatically. However, if you restart the Policy Server, a new output file (if the Profiler is configured for file output) is created. The existing Profiler output file is automatically saved with a version number. For example:

```
smtracedefault.log.1
```

If changes to the Logging or Tracing facility settings are not related to the Profiler output file, for example, enabling/disabling the console logging on Windows, the existing file is appended with new output without saving a version of the file.

By default The Policy Server retains up to ten output files (the current file and nine backup files). Older files are replaced automatically with newer files when the ten file limit is reached. You can change the number of files to retain by configuring the TraceFilesToKeep DWORD registry setting to the required decimal value. The TraceFilesToKeep registry setting must be created in the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\
LogConfig\TraceFilesToKeep
```

The Profiler tab has a "Buffered Tracing" option, which is set by default to improve Policy Server performance. This option is on Solaris systems only.

Change Profiler Settings

You can specify which components and data fields must be included in Policy Server tracing. You can then apply the filters to tracing output so that the profiler only captures specific values for a given component or data field.

Follow these steps:

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. Use Administrator permissions even if you are logged in to the system as an Administrator. For more information, see the release notes for your CA SiteMinder® component.

2. Click the Profiler tab.

   Note: For more information about the settings and controls on this tab, click Help, Management Console Help.

3. Click the Configure Settings button.

   Note: This button is only active when you select the Enable Profiling check box.

   The Policy Server Profiler dialog opens.

4. Optionally, select a Profiler template file that contains a predefined set of components and data fields appropriate for a particular tracing task from the Template drop down list:

   general_trace.template

   Provides the options for general, broad scope tracing.

   authentication_trace.template

   Provides the options for tracing user authentications.

   authorization_trace.template

   Provides the options for tracing user authorizations.

   samlidp_trace.template

   Provides the options for tracing the SAML Identity Provider assertions.

   samlsp_trace.template

   Provides the options for tracing SAML Service Provider Authentication.

   You can use the Profiler templates as a starting point for the Profiler configuration. Once a template has been loaded, you can manually modify the components and data fields that it specifies and apply the data filters.

5. Review/configure trace options by doing one or more of the following:
   - Select Components--Specify which components--actions that are executed by the Policy Server--to trace on the Components tab.
   - Select Data Fields--Specify which data fields--actual pieces of data that is used by the Policy Server to complete its tasks--to trace on the Data tab.
   - Add Filters--Specify data filters that include or exclude information from the tracing process on the Filters tab.
6. To save your new settings, do one of the following:
   - To save the settings in the currently selected configuration file, click OK.
   - To save the settings to a new configuration file, select File, Save As and specify a new text file.
7. Select File, Close to close the profiler and return to the Policy Server Management Console.
8. Select the Browse button to the right of the Configuration File field.

Avoid Profiler Console Output Problems on Windows

On Windows Policy Servers, you should disable QuickEdit Mode and Insert Mode to avoid problems when you enable console debugging. QuickEdit Mode and Insert Mode are features that you can enable from a Windows command prompt window.

To Disable QuickEdit Mode and Insert Mode

1. Access the command prompt window.
2. Right click in the window's title bar to display the pull-down menu.
3. Select Properties.
4. If QuickEdit Mode and Insert Mode are checked, deselect them.
5. Click OK.

Configure Profiler Trace File Retention Policy

By default the Policy Server retains up to ten output files (the current file and nine backup files). Older files are replaced automatically with newer files when the ten file limit is reached. You can change the number of files to retain by configuring the TraceFilesToKeep DWORD registry setting to the required decimal value. The TraceFilesToKeep registry setting should be created in the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\LogConfig\
TraceFilesToKeep
```

Manually Roll Over the Profiler Trace Log File

The Policy Server allows you to manually rollover the Policy Server Profiler trace log file using the smpolicysrv command.

Important! Before running a CA 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.

To start trace logging to a file, run the following command:

```
smpolicysrv –starttrace
```

This command starts logging to a trace file and does not affect trace logging to the console. It issues an error if the Policy Server is not running.

If the Policy Server is already logging trace data, running the –starttrace command causes the Policy server to rename the current trace file with a time stamp appended to the name in the form: *file_name*.YYYYMMDD_HHmmss.*extension* and create a new trace file with the original name. For example, if the trace file name in Policy Server Management Console's Profiler tab is C:\temp\smtrace.log, the Policy Server generates a new file and saves the old one as c:\temp\smtrace.20051007_121807.log. The time stamp indicates that the Policy Server created the file on October 7, 2005 at 12:18 pm.

If you have not enabled the tracing of a file feature using the Policy Server Management Console's Profiler tab, running this command does not do anything.

To stop trace logging to a file, run the following command:

```
smpolicysrv -stoptrace
```

This command stops logging to a file and does not affect trace logging to the console. It issues an error if the Policy Server is not running.

Note: On Windows systems, do *not* run the smpolicysrv command from a remote desktop or Terminal Services window. The smpolicysrv command depends on inter-process communications that do not work if you run the smpolicysrv process from a remote desktop or Terminal Services window.

Dynamic Trace File Rollover at Specified Intervals

You can also write a script to cause a trace file to be rolled over at a specified time interval. For example, to create a new trace file every hour, write a script similar to the following:

```
smpolicysrv –starttrace
repeat forever
wait 1 hour
smpolicysrv –starttrace
end repeat
```

This is similar to the time-based rollover option on the Policy Server Management Console's Logs tab.

Chapter 10: Configuring Administrative Journal and Event Handler

Administrative Journal and Event Handler Overview

The Policy Server Administrative Journal can be configured to specify how often administrative changes are applied to the Policy Server and how long the Policy Server maintains a list of applied changes.

Event Handlers are shared libraries that can be added to the Policy Server to handle certain events.

Configure Advanced Settings for the Policy Server

Follow these steps:

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. Use Administrator permissions even if you are logged in to the system as an Administrator. For more information, see the release notes for your CA SiteMinder® component.

2. Click the Advanced tab.

   Note: For more information about the settings and controls on this tab, click Help, Management Console Help.

3. Adjust the settings presented in the Administrative Journal group box to configure how often administrative changes are applied to the Policy Server, and how long the Policy Server maintains a list of applied changes.

4. Click Apply to save your changes.

Add Event Handler Libraries

You can add additional event handler libraries to the CA SiteMinder® Policy Server.

Note: If you do *not* have write access to the CA SiteMinder® binary files (XPS.dll, libXPS.so, libXPS.sl), an Administrator must grant you permission to use the related XPS command line tools using the Administrative UI or the XPSSecurity tool.

Follow these steps:

1. Open a command line on the Policy Server, and enter the following command:

   ```
   xpsconfig
   ```

   The tool starts and displays the name of the log file for this session, and a menu of choices opens.

2. Enter the following:

   ```
   xps
   ```

   A list of options appears.

3. Enter the following:

   ```
   5 (AuditSMHandlers)
   ```

   The settings for the event handler libraries appear.

4. Type C, and then enter the path and file name of the event handler library you want to add. Separate multiple library locations with commas.

   The settings for the event handler libraries appear. The value you added is shown at the bottom of the settings as a "pending value."

5. Do the following:

   a. Enter Q twice.

   b. Enter L.

   c. Enter Q to end your XPS session.

   Your changes are saved and the command prompt appears.

More information:

Event Handlers List Settings Warning when Opening Policy Server Management Console (see page 292)

Chapter 11: Adjusting Global Settings

This section contains the following topics:

Enable User Tracking

The Policy Server Global Tools task lets you enable and disable user tracking. If you enable user tracking, SiteMinder Web Agents save Global Unique Identifiers (GUIDs) in cookies. When users access a resource protected by an Anonymous authentication scheme for the first time, the Web Agent creates a cookie that includes the user's GUID. Each GUID is a unique value, therefore, it may be used to track an anonymous user and customize Web content.

Affiliate Agents require user tracking. If you are using SiteMinder for a network that includes Affiliate Agents, you must enable user tracking as described in the following procedure.

To enable user tracking

1. Log into the Administrative UI.
2. Click Administration, Policy Server, Global Tools.

   The Global Tools pane opens.
3. Select Enable User Tracking in the Global Settings group box.
4. Click Submit.

   The Policy Server enables user tracking.

Enable Nested Security

You can enable and disable nested security, which provides backwards compatibility for older versions of CA SiteMinder®.

To enable the nested security option

1. Log into the Administrative UI.
2. Click Administration, Policy Server, Global Tools.

   The Global Tools pane opens.

3. Select the Enable Nested Security checkbox.
4. Click Submit.

   The Policy Server enables nested security.

How to Enable Enhanced Active Directory Integration

The process of enabling enhanced active directory integration involves the following three steps:

1. Create the IgnoreADpwdLastSet registry key
2. Enable enhanced active directory integration
3. Configure a user directory connection

Create the IgnoreADpwdLastSet registry key

If the version of Active Directory in use does not include the pwdLastSet attribute, then create the Policy Server registry key IgnoreADpwdLastSet.

Important! Create the IgnoreADpwdLastSet registry key and set a value of 1, only for those installations that do not have the pwdLastSet attribute defined.

Follow these steps:

1. Access the Policy Server host system and complete one of the following steps:
   - (Windows) Open the Registry Editor and navigate to the following location:

     `SiteMinder\CurrentVersion\Ds\LDAPProvider`
   - (UNIX) Open the sm.registry file. The default location of this file is siteminder_home/registry.

     siteminder_home

     Specifies the Policy Server installation path.
2. Create IgnoreADpwdLastSet with a registry value type of REG_DWORD.

   Value: 1
3. Do one of the following steps:
   - (Windows) Exit the Registry Editor.
   - (UNIX) Save the sm.registry file.
4. Restart the Policy Server.

Enable Enhanced Active Directory Integration

Active Directory 2008 has several user and domain attributes that are specific to the Windows network operating system (NOS) and are not required by the LDAP standard. These attributes are:

- accountExpires
- userAccountControl
- pwdLastSet
- unicodePwd
- lastLogon
- lastLogonTimestamp
- badPasswordTime
- badPwdCount
- lockoutTime
- lockoutDuration
- pwdMaxAge

If you configure the Policy Server to use Active Directory as a user store, enable Enhanced Active Directory Integration from the Policy Server Global Tools task available from the Administrative UI. This option improves the integration between the Policy Server's user management feature and Password Services with Active Directory by synchronizing Active Directory user attributes with SiteMinder mapped user attributes.

Follow these steps:

1. Log into the Administrative UI.
2. Click Administration, Policy Server, Global Tools.

   The Global Tools pane opens.
3. Select Enhance Active Directory Integration. By default this feature is disabled.

   Note: After enabling this feature, you must have administrator credentials to modify the AD user store and have privileges to update AD attributes. If you do not have these credentials and privileges, the Policy Server returns an error message.
4. Click Submit.

   The Policy Server enables enhanced Active Directory integration.
5. Navigate to the User Directory dialog on the Infrastructure tab.
6. Open the Active Directory object for editing.

7. In the Root field, enter the default Windows domain's DN as the user directory root. For example:

   ```
   dc=WindowsDomain,dc=com
   ```

   Note: If the Root field is set to another value, AD-specific features may not work.

8. Click Submit.

Configure a User Directory Connection

After you enable enhanced active directory integration, configure a user directory connection.

Follow these steps:

1. Click Infrastructure, Directory.
2. Click User Directories.
3. Click Create User Directory.

   The Create User Directory page appears with the required settings to configure an LDAP connection.

4. Complete the required connection information in the General and Directory Setup sections.

   Note: If the Policy Server is operating in FIPS mode and the directory connection is to use a secure SSL connection when communicating with the Policy Server, the certificates used by the Policy Server and the directory store must be FIPS compliant.

5. (Optional) Do the following in the Administrator Credentials section:
   1. Select Require Credentials.
   2. Enter the credentials of an administrator account.
6. Configure the LDAP search and LDAP user DN lookup settings in the LDAP Settings section.

   LDAP User DN Lookup

   Specifies the parameters for locating users in an LDAP user store.

   Start

   Specifies the text string that acts as the beginning of an LDAP search expression or user DN. When a user attempts to login, the Policy Server prepends this string to the beginning of the username.

   Value: (sAMAccountName=

7. Set the specified values for the following attributes in the User Attributes section:

   Universal ID

   Specifies the name of the attribute SiteMinder uses as the Universal ID.

   Value: sAMAccountName

   Disabled Flag

   Specifies the name of the user directory attribute that holds the disabled state of the user.

   Value: carLicense (or any integer attribute)

   Password

   Specifies the name of the user directory attribute that SiteMinder should use to authenticate a user's password.

   Value: unicodePwd

   Password Data

   Specifies the name of the user directory attribute that SiteMinder can use for Password Services data.

   Value: audio

   The value for Password Data can be any large binary attribute. A value is needed only if you are using Basic Password Services.

   Note: For more information about the other fields, see the *Administrative UI Help*.

8. (Optional) Click Create in the Attribute Mapping List section to configure user attribute mapping.
9. Click Submit.

   The user directory connection is created.

Chapter 12: Cache Management

This section contains the following topics:

Cache Management Overview

CA SiteMinder® provides several caches that can be configured to maintain copies of recently accessed data (for example, user authorizations) to improve system performance. These caches should be configured to suit the nature of the data in your environment, but may also require periodic manual flushing.

CA SiteMinder® deployments can be configured to maintain the following cache on the Policy Server:

- The *User Authorization Cache* stores user distinguished names (DNs) based on the user portion of policies and includes the users' group membership.

CA SiteMinder® also maintains an *Agent Cache* on each a CA SiteMinder® Agent machine. The Agent Cache has two components:

- The *Agent Resource Cache* stores a record of accessed resources that are protected by various realms. This cache speeds up Agent to Policy Server communication, since the Agent knows about resources for which it has already processed requests.
- The *Agent User Cache* maintains users' encrypted session tickets. It acts as a session cache by storing user, realm, and resource information. Entries in this cache are invalidated based on timeouts established by the realms a user accesses.

Manage Cache Updates

You can suspend and resume cache flush updates to help resolve policy evaluation issues. You manage cache updates using the Administrative UI or the smpolicysrv command.

If you change the cache update status, the central administration Policy Server issues the command to all secondary Policy Servers.

Note: Policy Server commands are processed according to a thread management model. As a result, changes to the cache status are not visible in the smps.log file immediately.

Manage Cache Updates Using the Administrative UI

View the status of and enable or disable Policy Server cache flush updates using the Administrative UI.

Follow these steps:

1. Log in to the Administrative UI.
2. Click Administration, Policy Server, Cache Management.
3. View the cache status in the Cache Updates section:

   Cache updates are disabled: Cache flushing is disabled.

   Cache updates are enabled: Cache flushing is enabled.
4. (Optional) Click the Enable/Disable button to switch cache updates.

Manage Cache Updates Using the smpolicysrv Command

View the status of and enable or disable Policy Server cache flush updates using the smpolicysrv command.

Follow these steps:

1. Open a command prompt.

   Consider the following points on Windows systems:

   - Do not run the smpolicysrv command from a remote desktop or Terminal Services window. The command depends on interprocess communications. If you run the smpolicysrv process from a remote desktop or Terminal Services window, these communications do not work.
   - Be sure to open the command line window with administrator permissions. Use these permissions even if you are logged in to the system as an administrator. For more information, see the release notes for your CA SiteMinder® component.
2. Enter one of the following commands:

   smpolicysrv -disablecacheupdates

   Disables cache flushing.

   smpolicysrv -enablecacheupdates

   Enables cache flushing.

smpolicysrv -statuscacheupdates

Reports the refresh status of Policy Server caches to the log file: smps.log.

Disabled: Cache flushing is disabled.

Enabled: Cache flushing is enabled.

Flush Caches

When you change CA SiteMinder® objects, CA SiteMinder® automatically flushes the appropriate cache entries. The cache settings also specify a regular interval for applying administrative changes. When making sensitive changes (for example, changing the access rights to highly critical information), you have the option of flushing CA SiteMinder® caches manually. This manual step helps ensure that unauthorized users cannot access protected resources based on information stored in the caches.

Cache Management features are accessible from the Policy Server Global Tools pane in the Administrative UI. They let you force an update of SiteMinder data by manually flushing the following caches:

All Caches

Enables you to flush all caches, including user sessions, resource information, and user directory caches (including certificate CRLs).

User Session Caches

Enables you to force users to reauthenticate when they try to access protected resources.

Resource Caches

Enables you to flush cached information about resources.

Flush All Caches

The Cache Management options provide a method for administrators to flush the contents of all caches. Flushing all caches can possibly adversely affect the performance of a Web site, since all requests immediately following the cache flush must retrieve information from user directories and the policy store. However, this action can be necessary if critical user privileges and policy changes must go into effect immediately.

Cache management features are only available to administrators who have either the Manage Users or Manage System and Domain Objects privileges. The Flush All button is only available for administrators with the Manage System and Domain Objects. This menu selection appears only when the account you used to log in has enough privileges to access the cache function.

To flush all caches

1. Log in to the Administrative UI.
2. Click Administration, Policy Server, Cache Management.
3. In the All Caches group box, click Flush All.

   Note: The Flush All button is only enabled for administrators that have both the Manage Users and Manage the SiteMinder Objects privileges.

   The Policy Server and associated SiteMinder Agents flush all caches. This process can take up to twice the time of your policy server poll interval while the Policy Server synchronizes caches.
4. Click Submit.

   All caches are cleared.

Flush User Session Caches

When a user successfully authenticates, the Policy Server begins a session for the authenticated user. During the session, the web agent stores authorization information in the user cache.

Consider the following:

- If you change user access rights, it can be necessary to force the Policy Server to flush user session information from the web agent cache.
- The option to flush user caches is only enabled for administrators that have permission to manage users.

Follow these steps:

1. Log in to the Administrative UI.
2. Click Administration, Policy Server, Cache Management.
3. Select one of the following options in the User Session Caches section.

   All

   Flushes all user sessions from the user cache.

   Specific User DN

   Flushes a specific DN from the user cache.

   If you select this option:

   a. Select the user directory from the Directory list that contains the DN you want to remove.

   b. Enter the distinguished name in the DN field. Specify a user DN, not a DN of a group. If you do not know the DN, click Lookup and search for the DN.

4. Click Flush.

   CA SiteMinder® flushes the respective users from the user cache. This process takes up to twice the time specified by your Policy Server poll interval while the Policy Server synchronizes caches.

5. Click Submit.

   The user session caches are cleared.

Flush Resource Caches

SiteMinder Web Agents stores information about specific resources that users access in a resource cache. The resource cache records the following:

- Record of the Resources that have been accessed by users
- Whether or not the resources are protected by SiteMinder
- If a resource is protected, how the resource is protected

If you change rules or realms, you may want the changes to take effect immediately. If so, you must flush the resource cache.

Note: For detailed information about flushing resource caches for a realm or for a specific policy, see the *Policy Server Configuration Guide.*

To flush resource caches

1. Log into the Administrative UI.
2. Click Administration, Policy Server, Cache Management.
3. In the Resource Caches group box, click Flush.

   This flushes all resource caches and forces Web Agents to authorize requests against the Policy Server. This process will take up to twice the time specified by your policy server poll interval while the Policy Server synchronizes caches.

   Note: For an administrator with the Manage Domain Objects privilege for specific policy domains, flushing all resource caches only flushes the caches for the realms within the administrator's policy domains.

4. Click Submit.

   The resource cache are cleared.

Flush the Requests Queue on the Policy Server

Requests from CA SiteMinder® agents are set to time out after a certain interval. However, the Policy Server continues to process all agent requests in the queue, even those requests that have timed out, in the order that they were received. The following situations can cause the queue to fill with agent requests faster than the Policy Server can process them:

- Network lag between the Policy Server and the policy store or user store databases
- Heavy loads on the policy store or user store databases
- Policy Server performance problems

When the Policy Server requests queue fills with agent requests, you can flush the timed-out agent requests from the queue, so that only the current agent requests remain. Only use this procedure in the following case:

1. Agent requests waiting in the Policy Server queue time out.
2. One or more Agents resend the timed-out requests, overfilling the queue.

Important! Do not use -flushrequests in normal operating conditions.

To flush the requests queue on the Policy Server

1. Open a command prompt on the Policy Server.
2. Run the following command:

   ```
   smpolicysrv -flushrequests
   ```

   The request queue is flushed.

Note: On Windows systems, do *not* run the smpolicysrv command from a remote desktop or Terminal Services window. The smpolicysrv command depends on inter-process communications that do not work if you run the smpolicysrv process from a remote desktop or Terminal Services window.

Important! Before running a CA 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.

Chapter 13: User Session and Account Management

This section contains the following topics:

User Session and Account Management Prerequisites

The Policy Server provides user session and account management functionality, allowing you to flush the session cache, enable and disable users, and manage passwords for individual users.

To manage user sessions and accounts, the following prerequisites must be met:

- You must have an administrator account with the Manage Users privilege.
- To enable or disable user accounts, the user directory that contains user information must be configured with a Disable User attribute.
- To change passwords or force password changes, a password policy must be configured on the Policy Server and the user directory that contains user information must be configured with the Password Data attribute.

Note: For more information about configuring administrator privileges, user directories, and password policies, see the *Policy Server Configuration Guide*.

Enable and Disable Users

SiteMinder begins a user session after a user logs in and is authenticated. SiteMinder stores user attributes in its user session cache. When you disable a user, the Agent flushes the session cache, removing user identification and session information.

When the user attempts to access additional resources in the current session, the Web Agent no longer has the user's data in its cache. The Agent contacts the Policy Server and attempts to re-authenticate the user. The Policy Server determines that this user is disabled in the user directory and rejects the Agent's request to authenticate, which ends the session.

Follow these steps:

1. Log into the Administrative UI.
2. Click Administration, Users, Manage User Accounts.

   The Manage User Accounts pane opens.
3. Select the user directory connection for the directory that contains the user you want to enable or disable.
4. Click the Search icon.

   The Policy Server displays the Directory Users pane.
5. Enter search criteria in the Users/Groups group box and click GO to execute a search for the user you want to enable or disable. The search criteria is determined by the type of user directory you selected. You can enter the search criteria as either an attribute and a value, or as an expression. You can click Reset to clear the search criteria.

   The Policy Server displays search results in the Users/Groups group box.
6. Select a single user from the list of results.

   The Change user's state group box contains a button. This button is labeled Enable for a disabled user, or Disable for an enabled user.
7. Click Enable/Disable.

   The Policy Server disables or enables the selected user by changing a value in the user's profile.

Manage User Passwords

The Manage User Accounts pane in the Administrative UI enables you to force password changes for users, or change user passwords to new values.

Be sure that a password policy exists before you force users to change passwords. If no password policy exists, users will not be able to change their passwords, and therefore will not be able to access protected resources.

If you force a user to change passwords, and the user is accessing resources through an Agent that is not using an SSL connection, the user's new password information will be received over the non-secure connection. To provide a secure change of passwords, set up a password policy that redirects the user over an SSL connection when changing passwords.

Follow these steps:

1. Log into the Administrative UI.
2. Click Administration, Users, Manage User Accounts.
   The Manage User Accounts pane opens.

3. Select the user directory connection for the directory that contains the user for whom you want to manage passwords.
4. Click the Search icon.

   The Policy Server displays the user directory search dialog box associated with the type of directory you selected from the Directory drop-down list.
5. Enter search criteria in the Users/Groups group box and click GO to execute a search for the user you want to enable or disable. The search criteria is determined by the type of user directory you selected. You can either enter an attribute and a value, or enter an expression. You can click Reset to clear the search criteria.

   The Policy Server displays search results in the Users/Groups group box.
6. Select a single user from the list of results.
7. To force the selected user to change passwords on their next login, click Force Password Change in the Reset User's Password group box.
8. To change a user's password to a new value, enter a new password in the Change user's password group box. Re-enter the password to confirm.

   Note: The password that you specify is constrained by the password policy and is recorded in the user's password history.

Auditing User Authorizations

Use the Web Agent's auditing feature to track and log successful authorizations stored in the user session cache, allowing you to track user activity and measure how often applications on your Web site are used.

When you select this option, the Web Agent sends a message to the Policy Server each time a user is authorized from cache to access resources. You can then run log reports that shows user activity for each SiteMinder session.

If you do not enable auditing, the Web Agent will only audit authentications and first-time authorizations.

Note: For instructions on how to enable auditing, see the *Web Agent Configuration Guide*.

Web Agents automatically log user names and access information in native Web Server log files when users access resources. Included in the audit log is a unique transaction ID that the Web Agent generates automatically for each successful user authorization request. The Agent also adds this ID to the HTTP header when SiteMinder authorizes a user to access a resource. The transaction ID is then available to all applications on the Web server. The transaction ID is also recorded in the Web Server audit logs. Using this ID, you can compare the logs and follow the user activity for a given application.

To view the output of the auditing feature, you can run a SiteMinder report from the Administrative UI.

Chapter 14: Configuring SiteMinder Agent to Policy Server Communication Using a Hardware Load Balancer

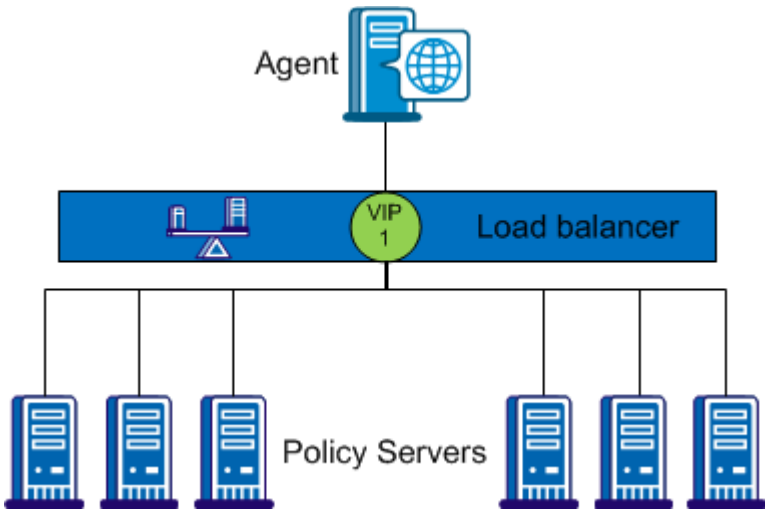
This section contains the following topics:

Hardware Load Balancing

CA SiteMinder® supports the use of hardware load balancers configured to expose multiple Policy Servers through one or more virtual IP addresses (VIPs). The hardware load balancer then dynamically distributes request load between all Policy Servers associated with that VIP. The following hardware load balancing configurations are supported:

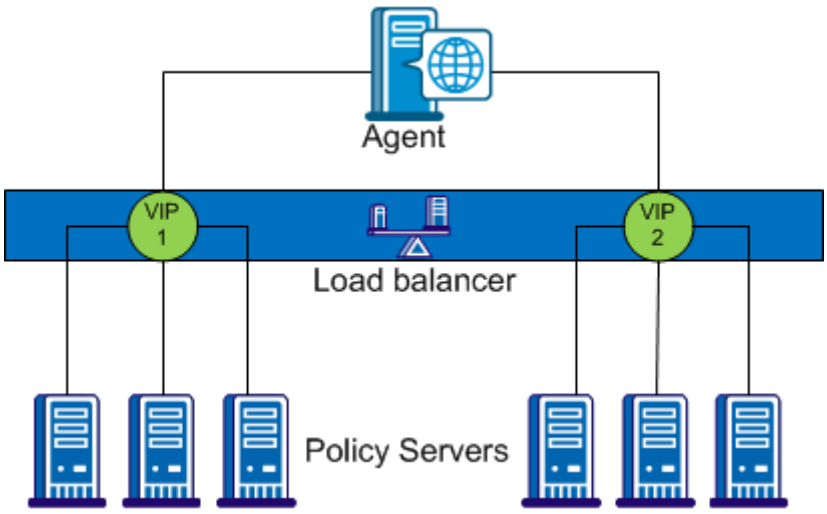
- Single VIP with multiple Policy Servers exposed by each VIP
- Multiple VIPs with multiple Policy Servers exposed by each VIP

Single VIP, Multiple Policy Servers Per VIP



In the configuration shown in the previous diagram, the load balancer exposes multiple Policy Servers using a single VIP. This scenario presents a single point of failure if the load balancer handling the VIP fails.

Multiple VIPs, Multiple Policy Servers Per VIP



In the configuration shown in the previous diagram, groups of Policy Servers are exposed as separate VIPs by one or more load balancers. If multiple load balancers are used, this amounts to failover between load balancers, thus eliminating a single point of failure. However, all major hardware load balancer vendors handle failover between multiple similar load balancers internally such that only a single VIP is required. If you are using redundant load balancers from the same vendor, you can therefore configure Agent to Policy Server communication with a single VIP and still have robust load balancing and failover.

Note: If you are using a hardware load balancer to expose Policy Servers as multiple virtual IP addresses (VIPs), we recommend that you configure those VIPs in a failover configuration. Round robin load balancing is redundant as the hardware load balancer performs the same function more efficiently.

Configure CA SiteMinder® Agent to Policy Server Connection Lifetime

Once established, the connection between an Agent and a Policy Server is maintained for the duration of the session. Therefore, a hardware load balancer only handles the initial connection request. All further traffic on the same connection goes to the same Policy Server until that connection is terminated and new Agent connections established.

By default, the Policy Server connection lifetime is 360 minutes—typically too long to be effective using a hardware load balancer. To help ensure that all Agent connections are renewed frequently for effective load balancing, configure the maximum Agent connection lifetime on the Policy Server.

To configure the maximum connection lifetime for a Policy Server, set the following parameter:

AgentConnectionMaxLifetime

Specifies the maximum Agent connection lifetime in minutes.

Default: 0. Sets no specific value; only the SiteMinder default connection lifetime (360 minutes) limit is enforced.

Limits: 0 - 360

Example: 15

Note: If you do not have write access to the CA SiteMinder® binary files (XPS.dll, libXPS.so, libXPS.sl), an Administrator must grant you permission to use the related XPS command line tools using the Administrative UI or the XPSSecurity tool.

The AgentConnectionMaxLifetime parameter is dynamic; you can change its value without restarting the Policy Server

To configure the maximum Agent connection lifetime for hardware load balancers

1. Open a command line on the Policy Server, and enter the following command:

   ```
   xpsconfig
   ```

   The tool starts and displays the name of the log file for this session, and a menu of choices opens.

2. Enter the following:

   ```
   sm
   ```

   A list of options appears.

3. Enter the numeric value corresponding to the AgentConnectionMaxLifetime parameter: For example, 4.

   The AgentConnectionMaxLifetime parameter menu appears.

4. Type c to change the parameter value.

   The tool prompts you whether to apply the change locally or globally.

5. Enter one of the following:

   - l—The parameter value is changed for the local Policy Server only, overriding the global value.
   - g—The parameter value is changed globally for all Policy Servers (that do not have a local value override set) using the same policy store.

6. Enter the new maximum Agent connection lifetime, in minutes, for example:

   ```
   30
   ```

   The AgentConnectionMaxLifetime parameter menu reappears, showing the new value. If a local override value is set, both the global and local values are shown.

7. Enter Q three times.to end your XPSConfig session.

   Your changes are saved and the command prompt appears.

More information

XPSConfig (see page 240)

Monitoring the Health of Hardware Load Balancing Configurations

Different hardware load balancers provides various methods of determining the health of the hardware and applications that they are serving. This section describes general recommendations rather than vendor-specific cases.

Complicating the issue of server health determination is that SiteMinder health and load may not be the only consideration for the load balancer. For example, a relatively unburdened Policy Server can be running on a system otherwise burdened by another process. The load balancer should therefore also take into account the state of the server itself (CPU, Memory Usage and Disk Activity).

Active Monitors

Hardware load balancers can use active monitors to poll the hardware or application for status information. Each major vendor supports various active monitors. This topic describes several of the most common monitors and their suitability for monitoring the Policy Server.

TCP Half Open

The TCP Half Open monitor performs a partial TCP/IP handshake with the Policy Server. The monitor sends a SYN packet to the Policy Server. If the Policy Server is up, it sends a SYN-ACK back to the monitor to indicate that it is healthy.

Simple Network Management Protocol (SNMP)

An SNMP monitor can query the SiteMinder MIB to determine the health of the Policy Server. A sophisticated implementation can query values in the MIB to determine queue depth, socket count, threads in-use, and threads available, and so on. SNMP monitoring is therefore the most suitable method for getting an in-depth sense of Policy Server health.

To enable SNMP monitoring, configure the SiteMinder OneView Monitor and SNMP Agent on each Policy Server. For more information, refer to Using the OneView Monitor and Monitoring CA SiteMinder® Using SNMP.

Note: Not all hardware load balancers provide out-of-the-box SNMP monitoring.

Internet Control Message Protocol (ICMP)

The ICMP health monitor pings the ICMP port of almost any networked hardware to see if it is online. Because the ICMP monitor does little to prove that the Policy Server is healthy, it is not recommended for monitoring Policy Server health.

TCP Open

The TCP Open Monitor performs a full TCP/IP handshake with a networked application. The monitor sends well-known text to a networked application; the application must then respond to indicate that it is up. Because the Policy Server uses end-to-end encryption of TCP/IP connections and a proprietary messaging protocol, TCP Open Monitoring is unsuitable for monitoring Policy Server health.

More information:

SNMP Monitoring (see page 179)
OneView Monitor Overview (see page 161)

Passive Monitors

In-band health monitors run on the hardware load balancer and analyze the traffic that flows through them. They are lower impact than active monitors and impose very little overhead on the load balancer.

In-band monitors can be configured to detect a particular failure rate before failing over. In-band monitors on some load balancers can detect issues with an application and specify an active monitor that will determine when the issue has been resolved and the server is available once again.

Chapter 15: Clustering Policy Servers

This section contains the following topics:

Clustered Policy Servers Introduced

Load balancing and failover in a CA SiteMinder® deployment provide a high level of system availability and improve response time by distributing requests from CA SiteMinder® Agents to Policy Servers. Defining clusters in combination with load balancing and failover further enhance the level of system availability and system response time.

Traditional round robin load balancing without clusters distributes requests evenly over a set of servers. However, this method is not the most efficient in heterogeneous environments, where computing powers differ, because each server receives the same number of requests regardless of its computing power.

Another problem with efficiency can occur when data centers are located in different geographical regions. Sending requests to servers outside a certain locale can lead to the increased network communication overhead, and in some cases to the network congestion.

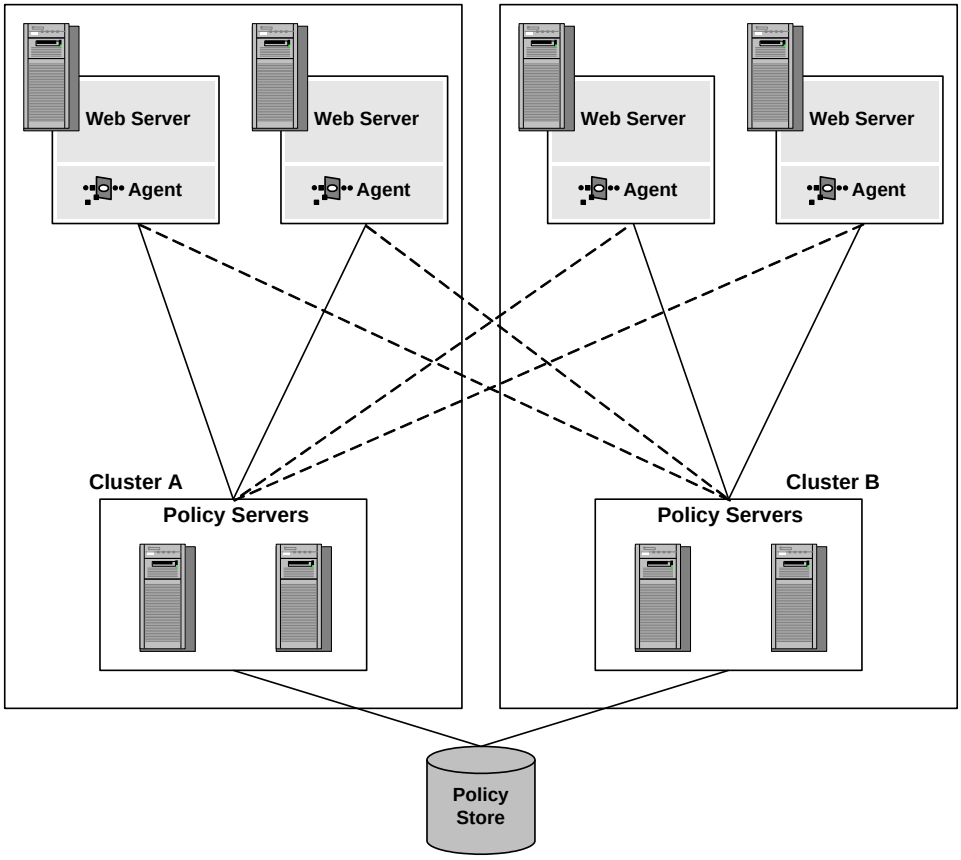
To address these issues and to improve system availability and response time, you can define a cluster of Policy Servers and associated CA SiteMinder® Agents configured to perform (software-based) load balancing and failover.

Policy Server clusters provide the following benefits over a traditional load balancing/failover scheme:

- Load is dynamically distributed between Policy Servers in a cluster based on server response time.
- A cluster can be configured to failover to another cluster when the number of available servers in the cluster falls below a configurable threshold.

Note: Policy Servers clusters are not suitable or necessary for environments in which Policy Servers communicate with Agents through hardware load balancers.

The following figure illustrates a simple CA SiteMinder® deployment using two clusters:



Consider Cluster A and Cluster B as distributed in two different geographical locations, separated by several time zones. By dividing the Web Agents and Policy Servers into distinct clusters, the network overhead involved with load balancing across geographically separate regions is only incurred if the Policy Servers in one of the clusters fail, requiring a failover to the other cluster.

More information:

Failover Thresholds (see page 155)
Clustered Environment Monitoring (see page 173)

Failover Thresholds

In any clustered CA SiteMinder® environment, you must configure a failover threshold. When the number of available Policy Servers falls below the specified threshold, all requests that would otherwise be serviced by the failed Policy Server cluster are forwarded to another cluster.

The failover threshold is represented by a percentage of the Policy Servers in a cluster. For example, if a cluster consists of four Policy Servers, and the failover threshold for the cluster is set at 50%, when three of the four Policy Servers in the cluster fail, the cluster fails, and all requests fail-over to the next cluster.

The default failover threshold is zero, which means that all servers in a cluster must fail before failover occurs.

Hardware Load Balancing Considerations

If you are deploying a hardware load balancer between the CA SiteMinder® Policy Server and Web Agents, consider the following:

- Do not configure a TCP heartbeat or health–check directly against the Policy Server TCP ports. Heartbeats and health–checks applied directly against the TCP ports of the Policy Server can adversely affect its operation.
- Design a comprehensive facility for the load balancer to test the operational health of the Policy Server.
- Consider the impact of a single Policy Server configuration on the Web Agent failover algorithm as opposed to a multiple Policy Server configuration.
- Consider performance and failure scenarios in Web Agent and Policy Server tuning and monitoring.
- If the load balancer is configured to proxy Agent-to-Policy-Server connections, consider the timeouts and the socket states of the load balancer.

  Note: For more information about deploying a hardware load balancer between Web Agents and Policy Servers, see the related Knowledge Base article (TEC511443) on the Support site.

More information:

Contact CA Technologies (see page 3)

Configure Policy Server Clusters

Policy Server clusters are defined as part of a Host Configuration Object. When a CA SiteMinder® agent initializes, the settings from the Host Configuration Object are used to setup communication with Policy Servers.

Note: For more information about Host Configuration Objects, see the *Web Agent Configuration Guide* and the *Policy Server Configuration Guide.*

Follow these steps:

1. Click Infrastructure, Hosts. Host Configuration Objects.
2. Click Create Host Configuration.
3. In the Clusters section, click Add.

   The Cluster Setup section opens.

   Note: You can click Help for a description of fields, controls, and their respective requirements.
4. Enter the IP address and the port number of the Policy Server in the Host and Port fields respectively.
5. Click Add to Cluster.

   The Policy Server appears in the servers list in the Current Setup section.
6. Repeat these steps to add other Policy Servers to the cluster.
7. Click OK to save your changes.

   Your return to the Host Configuration dialog The Policy Server cluster is listed in a table.
8. In the Failover Threshold Percent field, enter a percentage of the number of Policy Servers that must be active and click Apply.

   If the percentage of active servers in the cluster falls below the percentage you specify, the cluster fails over to the next available cluster in the list of clusters. This setting applies to all clusters that use the Host Configuration Object.

   Important! The Policy Server specified in the Configuration Values section is overwritten by the Policy Servers specified in a cluster. This Policy Server is no longer used because a cluster is configured. For the value of the Policy Server parameter in the Configuration Values section to apply, do not specify any Policy Servers in a cluster. If clusters are configured, and you decide to remove the clusters in favor of a simple failover configuration delete all Policy Server information from the cluster.
9. Click Submit to save your changes.

Configure a Policy Server as a Centralized Monitor for a Cluster

The OneView Monitor can be configured to monitor a Policy Server cluster. To enable this configuration, one Policy Server must be set up as a centralized monitor with the other clustered Policy Servers pointing to it.

Follow these steps:

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. Use Administrator permissions even if you are logged in to the system as an Administrator. For more information, see the release notes for your CA SiteMinder® component.

2. In the Settings tab, select Allow Incoming Remote Connections.

   Note: For more information about the settings and controls on this tab, click Help, Management Console Help.

3. Click OK to save your changes and close the Policy Server Management Console.
4. Restart the OneView Monitor.

This setting allows the centralized Policy Server monitor to accept remote connections from the other clustered Policy Servers.

Note: The network channel between a Policy Server and a Monitor process is non-secure.

After you configure a Policy Server as a centralized monitor, configure the Policy Server Management Console to point the other clustered Policy Servers to it.

More information:

Configure OneView Monitor Port Numbers (see page 173)

Point Clustered Policy Servers to the Centralized Monitor

Follow these steps:

1. For each Policy Server that will point to the monitoring service, open the Policy Server Management Console.

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

2. In the Settings tab, under OneView Monitor, select Connect to Remote Monitor.

   Note: For more information about the settings and controls on this tab, click Help, Management Console Help.

3. In the field below, enter the hostname and TCP port number of the system where the monitoring service is configured. For example:

   server.company.com:44449.

4. Click OK to save your changes and close the Policy Server Management Console.
5. Restart the Policy Server.

Chapter 16: Using the OneView Monitor

This section contains the following topics:

Chapter 17: OneView Monitor Overview

The CA SiteMinder® OneView Monitor identifies performance bottlenecks and provides information about resource usage in a CA SiteMinder® deployment. It also displays alerts when certain events, such as component failure, occur. It does this by collecting operational data from the following CA SiteMinder® components:

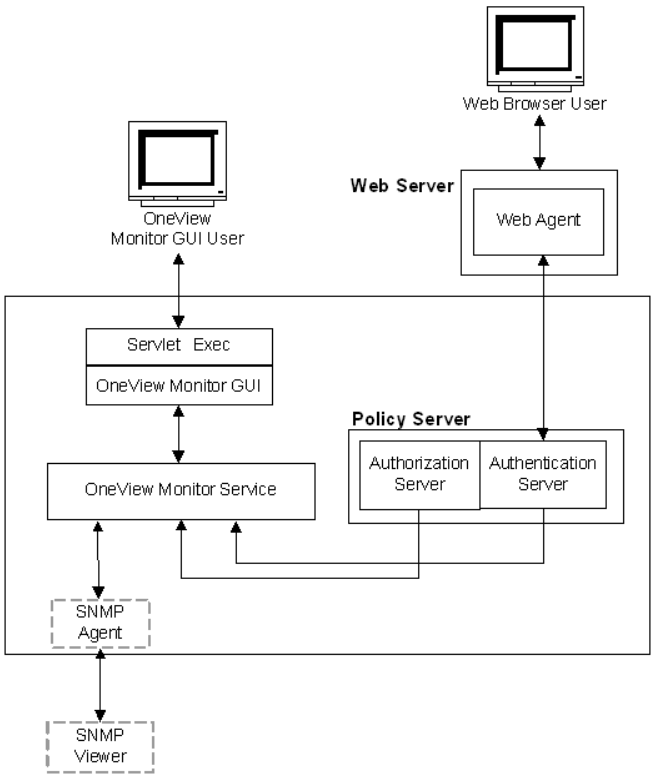
- Policy Server
- CA SiteMinder® Web Agent

As these components are added to a CA SiteMinder® deployment, they are automatically registered with OneView Monitor. You do not need to configure OneView to monitor these components.

Each machine that hosts a monitored component includes a OneView agent. The agent sends operational data to the OneView Monitor, which resides on the machine where the Policy Server is installed. The OneView Monitor sends the operational data to a Web browser or (optionally) an SNMP agent. The SNMP agent sends the data to the SNMP manager.

OneView Monitor data can be accessed from a Web browser, or from a third-party SNMP monitoring application.

The following graphic illustrates how the OneView Monitor is integrated in a CA SiteMinder® deployment.



The OneView Monitor collects properties, such as the IP address of the component's host machine, and counters that reflect a component's activity, such as how many times users have logged into your site. Counters are reset when the component is restarted.

Using the Web-based OneView viewer, administrators can define tables to view some or all of the data for a specific component. The data is refreshed at configurable intervals.

SNMP support enables monitoring applications to retrieve operational data from the OneView Monitor. SNMP support includes a Management Information Base (MIB) and an SNMP agent.

Note: In an environment that includes a clustered Policy Servers, you can specify a single OneView Monitor to monitor activity on all Policy Servers in a cluster. To configure a central monitor, you must adjust the OneView Monitor settings in the Policy Server Management Console for each Policy Server in the cluster.

More information:

SNMP Monitoring (see page 179)
Setting The OneView Data Refresh Rate and Heartbeat (see page 172)

Policy Server Data

The following lists and describes Policy Server data:

AgentTable

Table of agents that are connected to this server.

Note: AgentTable is not available using SNMP.

AuthAcceptCount

Number of successful authentications.

AuthRejectCount

Number of failed authentication attempts. These attempts failed because of invalid credentials.

AzAcceptCount

Number of successful authorization attempts.

AzRejectCount

Number of rejected authorization attempts. These attempts were rejected because of insufficient access privileges.

CacheFindCount

Number of find operations in the authorization cache. Updated each time an authorization process asks whether a user belongs to a policy.

CacheFindCount/sec

Number of authorization cache find operations occurring per second.

CacheHitCount

Number of hits on the authorization cache. Updated each time the cache answers true when an authorization process asks whether a user belongs to a policy.

CacheHitCount/sec

Number of hits on the authorization cache occurring per second.

CacheTTLMissCount

Number of authorization cache misses because an element is found in the cache but considered too old.

Component Path

Path of the Policy Server, which uniquely identifies the server. The component path includes the following information:

- Host IP address
- Component type
- Component instance ID

Note: Component Path is not available using SNMP.

Crypto bits

Length of the encryption key used to encrypt/decrypt data sent between the Web Agent and the Policy Server.

HitRate

The ratio of authorization cache hits to authorization find operations. This is an indicator of authorization cache effectiveness.

Host

IP address of the machine where the authentication server is installed.

Note: The Host IP address is included in the Component Path.

IsProtectedCount

Number of IsProtected calls received from an Agent.

Label

Policy Server build number.

LastActivity

Date and time of the Policy Server's last interaction with the Monitor.

MaxSockets

Maximum number of Web Agent sockets available to submit concurrent requests to a Policy Server.

MaxThreads

Maximum number of worker threads in the thread pool.

MaximumThreadsEverUser

Maximum number of worker threads from the thread pool ever used.

PriorityQueueLength

Number of entries in the priority queue. The priority queue holds entries of high priority. See ServerQueueLength.

Platform

Operating system of the machine where the Policy Server is installed.

PolicyCacheEnabled

Indicates whether the policy cache is enabled.

Port

Policy Server port number.

Product

Policy Server product name.

ServerQueueLength

Number of entries in the normal queue. The normal queue holds entries of normal priority. See PriorityQueueLength.

SocketCount

Number of open sockets, which corresponds to the number of open connections between the Policy Server and Web Agents.

Status

Status of the Policy Server. The status can be Active or Inactive.

Inactive status indicates that there was no interaction between the Policy Server and the monitor for a specified period of time. The period of time is determined by the heartbeat interval.

ThreadsAvailable

Number of a worker threads that are available from within the thread pool. All worker threads, which process requests, are organized into a thread pool. Not all threads are busy immediately--only when enough load is applied. This value shows how many threads are not currently busy.

ThreadsInUse

Number of worker threads from the thread pool that are in use.

Time Zone

Time zone for the geographical location where the Policy Server is installed.

Type

Type of Policy Server.

Universal Coordinated Time

The startup time of the Policy Server.

UserAzCacheEnabled

Indicates whether the user authorization cache is enabled.

Update

Version number of the most recently applied update.

Version

Version number of the Policy Server.

Web Agent Data

The following lists and describes Web Agent data:

AuthorizeAvgTime

Indicates the average time it takes to authorize a user (in milliseconds).

AuthorizeCount

Number of authorization attempts made by this Agent. An authorization attempt occurs when a user supplies credentials to the Policy Server in order to access a protected resource.

AuthorizeErrors

Number of errors that occurred during authorization attempts made by this Web Agent. An error indicates a communication failure between the Web Agent and Policy Server during an authorization call.

AuthorizeFailures

Number of failed authorization attempts. An authorization attempt fails when a user lacks sufficient privileges to access a resource.

BadCookieHitsCount

Number of cookies that the Web Agent could not decrypt.

BadURLcharsHits

Number of requests that the Agent refuses because of bad URL characters. Bad URL characters are specifically blocked to prevent a Web client from evading SiteMinder rules. These characters are specified in the Web Agent's configuration.

Component Path

Path of the Web Agent. The component path includes the following information:

- Host IP address
- Component type
- Component instance ID

Note: Component Path is not available using SNMP.

CrosssiteScriptHits

Number of cross-site scripting hits. A cross-site scripting hit consists of malicious code embedded in pages at your site.

Note: For more information about cross-site scripting, see the *Web Agent Configuration Guide*.

Crypto bits

Length of the encryption key used to encrypt/decrypt data sent between the Web Agent and the Policy Server.

ExpiredCookieHitsCount

Number of requests that contained an expired cookie.

Host

IP address of the machine where the Web Agent is installed.

Note: The Host IP address is included in the Component Path.

IsProtectedAvgTime

The average amount of time it takes (in milliseconds) for the Web Agent to determine from the Policy Server whether or not a resource is protected.

IsProtectedCount

Number of times the Web Agent has checked the Policy Server to see if a resource is protected.

Note: If the resource cache is set to 0, the OneView Monitor may record two or more IsProtected calls per login attempt. If the Web Agent is not caching information, it must check with the Policy Server to determine whether or not a resource is protected each time a request is made to the Web server.

If the resource cache is not set to 0, the OneView Monitor only records one IsProtected call. In this case, the Web Agent makes one IsProtected call to the Policy Server; subsequent requests to the Web server for the same resource are satisfied against the Web Agent's resource cache until the resource in the cache expires or the resource cache is flushed.

IsProtectedErrors

Number of times an error has occurred when the Web Agent asks the Policy Server whether or not a resource is protected. An error indicates a communication failure between the Web Agent and the Policy Server.

Label

Web Agent build number.

Last Activity

Date and time of the Web Agent's last activity.

LoginAvgTime

Average time it takes for a user to log in.

LoginCount

Number of login attempts made from this Web Agent.

LoginErrors

Number of errors that occurred during login attempts. An error indicates a communication failure between the Web Agent and the Policy Server.

LoginFailures

Number of failed login attempts. Login failures occur when users supply invalid credentials.

Name

Name of the Web Agent.

Platform

Operating system of the machine where the Web Agent is installed.

Product

Web Agent product name.

ResourceCacheCount

Number of entries in the resource cache. The resource cache stores information about recently accessed resources to speed up subsequent requests for the same resource.

The number of entries in the resource cache can be 0 to *n*, where *n* is the maximum cache size specified in the Web Agent's configuration.

ResourceCacheHits

Number of times that the Web Agent located a resource in the resource cache. This number indicates how frequently SiteMinder is using cached resources.

ResourceCacheMax

The maximum number of entries the resource cache can contain. This number is specified in the Web Agent's configuration.

Note: Details on setting the resource cache size exist in the *Web Agent Configuration Guide*.

ResourceCacheMisses

- The number of times the Web Agent could not locate a resource in the resource cache. This occurs when:
- The resource has not been accessed before
- The cached information has expired

SocketCount

Number of open sockets, which corresponds to the number of open connections between the Policy Server and the Web Agent.

Note: Because the Web Agent architecture has changed, SocketCount has no value.

Status

Status of the Web Agent. The status can be Active or Inactive.

Inactive status indicates that there was no interaction between the Web Agent and the monitor for a specified period of time. The period of time is determined by the heartbeat interval.

Time Zone

Time zone for the geographical location where the Web Agent is installed.

Type

Type of monitored component. In this case, the Web Agent.

Universal Coordinated Time

The startup time of the Web server where the Web Agent is installed.

Update

Version number of latest software update.

UserSessionCacheCount

Number of entries in the user session cache. The user session cache stores information about users who have recently accessed resources. Storing user information speeds up resource requests.

The number of entries in the user session cache can be 0 to *n*, where *n* is the maximum cache size specified in the Web Agent's configuration. see the *Web Agent Configuration Guide* for information on setting the user session cache size.

Note: The user session cache count may differ based on the Web server where the session cache is located.

For Web Agents that use multi-thread cache, such as IIS Web Agents, iPlanet 4.*x* and 6.0 Web Agents (on Windows operating systems), and Domino Web Agents (on Windows and UNIX operating systems), the OneView Monitor increases the user session cache count when a user is successfully authenticated and receives a session cookie from the Web Agent.

Apache and iPlanet 4.*x* and 6.0 Web Agents running on UNIX operating systems, which use multi-process cache, count sessions differently. A user's session is not added to the session cache until he presents a session cookie to the Web Agent. The Web Agent creates a session cookie for the user *after* he is successfully authenticated. SiteMinder uses that cookie to authenticate the user if he makes additional resource requests. This means that the user's first login is not recorded in the user session cache count. If the user makes another request and SiteMinder authenticates the user using the session cookie, the user session cache count increases.

In all Web Agents, the user session is valid for resources in one realm. If the user accesses a resource in a different realm using a session cookie, he is given another user session, which increases the user session cache count.

UserSessionCacheHits

Number of times that Web Agent accessed the user session cache.

UserSessionCacheMax

The maximum number of entries the user session cache can contain. This number is specified in the Web Agent's configuration.

Note: Details on setting the user session cache size exist in the *Web Agent Configuration Guide*.

UserSessionCacheMisses

The number of times the Web Agent could not locate user session information in the user session cache. This occurs when:

- The user has not accessed a resource before
- The cached information has expired

ValidationAvgTime

Average amount of time it takes to validate a cookie used to authenticate a user (in milliseconds). Cookies may be used to authenticate a user in a single sign-on environment.

ValidationCount

The number of times a specific Web Agent attempted to validate a session cookie against the Policy Server to authenticate a user, instead of matching that user's credentials to a user directory entry. (The Web Agent creates a session cookie on the user's browser when a user is successfully authenticated, and uses that cookie to authenticate the user on subsequent requests for new resources.)

The following conditions affect the ValidationCount:

User Session Cache size

If a Web Agent's user session cache is set to a value greater than 0, the user's session information is stored in the cache. The Web Agent validates the session against the session cache instead of the Policy Server, so the ValidationCount does not increase. If the user session cache is set to 0, the ValidationCount increases each time a user requests a protected resource because the Web Agent must validate the session against the Policy Server.

Multi-thread vs. Multi-process cache

Web Agents that use multi-threaded cache, such as IIS Web Agents, iPlanet 4.x and 6.0 Web Agents (on Windows operating systems, and Domino Web Agents (on Windows and UNIX operating systems), add a session to the session cache (if the session cache size is greater than 0) when a user is successfully authenticated. If that user requests additional resources from the same realm, the Web Agent validates the user against the session cache, so the ValidationCount does not increase.

Apache and iPlanet 4.x and 6.0 Web Agents running on UNIX operating systems, which use multi-process cache, do not add the session cookie to the session cache until the user presents the cookie to the Web Agent during a request for another resource in the realm where she was authenticated. The Web Agent validates the first request made with a session cookie against the Policy Server, which increases the ValidationCount. Subsequent requests are validated against the cache.

ValidationErrors

The number of errors that occurred when the Web Agent attempted to validate a user session. Errors indicate a communication failure between the Web Agent and the Policy Server.

ValidationFailures

The number of times the Web Agent has failed to validate a user session because of an invalid session cookie.

Version

Version number of the Web Agent.

Configure the OneView Monitor

Configuring the OneView Monitor includes:

- Setting the data refresh rate and heartbeat
- Configuring port numbers

Setting The OneView Data Refresh Rate and Heartbeat

You can change how often data is sent between the OneView Monitor and a monitored component by modifying the following settings:

- Refresh rate determines how often the OneView Monitor requests data from the authentication and authorization servers. The default refresh rate is 5 seconds.
- Heartbeat specifies how often monitored components send a heartbeat to the Monitor. For the authentication and authorization servers, the heartbeat indicates whether or not the component is active. For the Web Agent, the heartbeat determines how often the Monitor receives the Web Agent's operational data. The default value is 30 seconds.

To modify the default values

1. Open *Policy_Server_installation*/monitor/mon.conf.
2. Change the value paired with the following properties, as necessary:
   - Refresh rate: nete.mon.refreshPeriod
   - Hearbeat: nete.mon.hbPeriod

   Note: The value for these properties is specified in seconds.
3. Save and close mon.conf.
4. Restart the OneView Monitor.

More information:

Start and Stop Policy Server Services on Windows Systems (see page 24)
Start and Stop Policy Server Processes on UNIX Systems (see page 24)

Configure OneView Monitor Port Numbers

The One View Monitor uses the following default port numbers:

- OneView Agent--44449

  Note: When the default port is used, the OneView Agent only listens on that port. If the default port is changed, the One View Agent listens on port you specify, *and* connects to the same port on the remote host you specify. For example, if you change the port to 55555, the OneView Agent listens on port 55555, *and* connects to port 55555 on the remote host.

- OneView Monitor--44450

To change the default port numbers

1. Open *Policy_Server_installation_directory*/config/conapi.conf file in a text editor.
2. Change the values of the following OneView Agent properties, as necessary:

   `nete.conapi.service.monagn.port=`*`port_number`*

   `nete.conapi.service.monagn.host=`*`fully_qualified_domain_name_of_remote_host`*
3. Change the value of the following OneView Monitor properties, as necessary:

   `nete.conapi.service.mon.port=`*`port_number`*
4. Save and close the conapi.conf file.

   Note: For more information about the properties in conapi.conf, see the notes in the conapi.conf file.
5. Restart the OneView Monitor.

More information:

Start and Stop Policy Server Services on Windows Systems (see page 24)
Start and Stop Policy Server Processes on UNIX Systems (see page 24)
Configure a Policy Server as a Centralized Monitor for a Cluster (see page 157)

Clustered Environment Monitoring

In a non-clustered CA SiteMinder® deployment, a Monitor process is located on the same system as the Policy Server. The Monitor user interface and the SNMP provide information for a single Policy Server. To monitor a cluster, the Policy Servers in the cluster must be configured to point to a single Monitor process. The Policy Server Management Console allows you to specify a Monitor process host.

Consider the following when implementing a monitoring in a clustered environment:

- The network channel between a Policy Server and a Monitor process is non-secure.
- If the Monitor process fails, all monitoring stops. If the Monitor host is disconnected, the monitoring stops.
- Monitoring through SNMP is supported for a cluster.

Note: By not enabling clustering, all servers are in the default cluster. Centralized monitoring can be enabled for non-clustered environments.

More information:

Point Clustered Policy Servers to the Centralized Monitor (see page 157)

Access the OneView Viewer

Be sure the OneView Monitor service is running before you access the OneView viewer.

To access the OneView viewer, enter the following URL in a browser:

http://*your_server.your_company.org:port*/siteminder monitor

where *your_server.your_company.org:port* is the host name or IP address, and the port number of the Web server which is configured for the OneView Monitor.

Note: For instructions on configuring a Web server for the OneView Monitor, see the *Policy Server Installation Guide*.

Protect The OneView Viewer

To protect the OneView viewer, create a CA SiteMinder® policy that protects the resources in siteminder monitor.

View Monitored Components

OneView Monitor provides the following default tables:

- All Components (displayed)
- Policy Servers
- Agents

The All Components table is displayed when you open OneView.

Note: A Web Agent installed on an Apache or iPlanet 6.0 Web server will not appear in the OneView viewer until that Web Agent asks the Policy Server if a resource is protected. When the Web Agent requests information from the Policy Server, it is registered with the OneView Monitor.

The OneView viewer displays operational data in configurable tables. A table may contain a Details column. Clicking an icon in the Details column opens a window that displays all the monitored data for a particular component.

How to Customize OneView Displays

Customizing OneView displays includes:

- Setting up tables (see page 175)
- Configuring alerts (see page 176)
- Displaying tables (see page 176)
- Sorting tables (see page 177)
- Configuring data updates (see page 177)
- Saving settings (see page 177)
- Changing the default display (see page 178)
- Loading settings (see page 178)

Set Up Tables

To set up tables

1. Click Configure.

   The Table Configuration dialog box opens.
2. Complete one of the following options:
   - Select Existing Table. Choose a table from the list box.
   - Select New Custom Table. Enter a name in the Table Name field.
3. Select components to display in the table.

4. Select the fields to display in the table. Specify the order in which the fields are displayed by selecting a field and using the up or down arrow to position the field. The available fields are determined by the type of component(s) selected for the table.

   Note: The value for some of the fields can be displayed as a continuously increasing number (reset when the component is restarted) or as an average since the last update period. To view the average value, select a field name with /sec appended to it.

5. Click OK.

   Note: Make sure to save the table after configuring it.

More information:

Save Settings (see page 177)

Configure Alerts

To configure alerts

1. Click Configure.
2. Click the Alerts tab.
3. Select a field from the left list box. This list box contains all of the fields in the currently loaded tables.
4. Select an operator from the middle list box.
5. Specify a value for the field that you selected in step 3.
6. Optionally, select Highlight the table cell to have OneView highlight the specified table cell when the specified criteria is met.
7. Optionally, select Pop up a warning message to have OneView display a pop-up window when the specified criteria is met.

Display Tables

To display tables, select a table from the View Table list box in the main viewer page. When you select a table from this list, OneView displays the selected table below the existing table.

To hide a table, click the Hide button.

Sort Tables

You can sort the data in each column in a table in ascending or descending order. Sorting columns helps organize a table. For example, sorting a table based on Status enables you to view all inactive components grouped together.

Note: An arrow in the column heading indicates which column is sorted.

Configure Data Updates

By default, OneView updates data every thirty seconds. You can:

- Modify the amount of time that passes between automatic updates
- Configure the OneView to update data only when you refresh the browser

To configure data updates

1. Click Updates.

   CA SiteMinder® opens the Updates dialog box.
2. Select one of the following:
   - Live Updates--Updates the data after a specified period of time. Specify the time interval in seconds.
   - Manual Updates--Updates the data when a user refreshes the page.
3. Click OK.

Save Settings

Saving a setting saves:

- Table definitions
- Main page display
- Table sorting
- Update rate

To save settings

1. Click Save Settings.

   CA SiteMinder® displays a dialog box where you can name the settings.
2. Enter a name in the text box.
3. Click OK.

Change the Default Display

To change the default display

1. Rename the defaults file in *siteminder_installation*\monitor\settings.
2. In the OneView Monitor console, configure the settings.
3. Save the settings as defaults.

Load Settings

To load settings

1. Click Load Settings.

   CA SiteMinder® displays a dialog box where you can select settings to load.
2. Select a setting from the list box.
3. Click OK.

Chapter 18: Monitoring CA SiteMinder® Using SNMP

This section contains the following topics:

SNMP Monitoring

The CA SiteMinder® SNMP module enables many operational aspects of the CA SiteMinder® environment to be monitored by SNMP-compliant network management applications.

SNMP Overview

Network management takes place between two types of systems: those in control, called managing systems, and those observed and controlled, called managed systems. Managed systems can include hosts, servers, and the software components that run on those systems, or network components such as routers or intelligent repeaters.

To promote interoperability, cooperating systems adhere to the industry standard Simple Network Management Protocol (SNMP), an application-layer protocol designed to facilitate the exchange of management information between network devices.

A complete SNMP solution comprises three components:

- SNMP Management Information Base (MIB) is a database of managed objects. The managed objects, or variables, can be read by a managing system to provide information about the managed system.
- SNMP Agents are low-impact software modules that access information about the managed system and make it available to the managing system. For software systems, agent functionality is sometimes split between a master agent (provided by the host operating system) and subagent (provided by the managed application).

  Note: SNMP agents, which are a standard component of all SNMP implementations should not be confused with CA SiteMinder® Agents.
- SNMP Manager is typically a Network Management System (NMS) application such as HP OpenView.

The CA SiteMinder® SNMP module provides SNMP request handling and configurable event trapping for the CA SiteMinder® environment. It does this by collecting operational data from the CA SiteMinder® OneView Monitor and making it available in a MIB to third-party NMS applications that support the SNMP protocol (for example, HP OpenView).

Note: The 6.0 SNMP agent is backwards compatible with all CA SiteMinder® 5.x-based Agent applications.

CA SiteMinder® SNMP Module Contents

The CA SiteMinder® SNMP module consists of:

- CA SiteMinder® SNMP MIB is the database of CA SiteMinder® objects that can be monitored by an SNMP-compliant network management system.
- A CA SiteMinder® SNMP Subagent responds to SNMP requests (GET and GETNEXT only) passed to it from an SNMP master agent.
- CA SiteMinder® Event Manager captures Policy Server events and, if configured to do so, generates SNMP traps (unsolicited messages sent by an SNMP agent to a SNMP NMS indicating that some event has occurred).

More information:

CA SiteMinder® MIB (see page 182)
Start and Stop SiteMinder SNMP Support (see page 192)

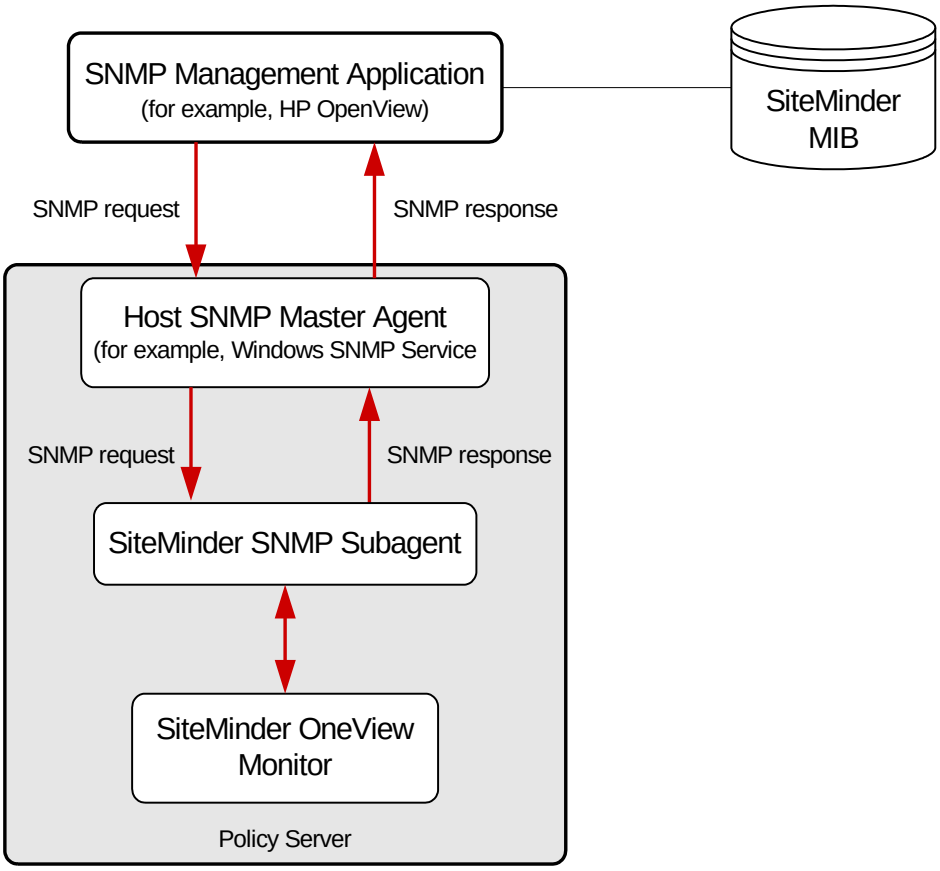
Dependencies

The CA SiteMinder® SNMP Module has the following dependencies:

- **CA SiteMinder® OneView Monitor**—The CA SiteMinder® SNMP Module obtains operational information from the OneView Monitor. OneView Monitor *must* also be configured and running on any Policy Server on which you want to run the CA SiteMinder® SNMP Module.
- **SNMP Master Agent**—The CA SiteMinder® SNMP Module does *not* provide an SNMP Master Agent. You will need to ensure that the SNMP Master Agent (Windows SNMP Service or Solstice Enterprise Master Agent) appropriate to the Operating System of the Policy Server on which you are running the CA SiteMinder® SNMP Module is also installed and enabled.

SNMP Component Architecture and Dataflow

The following figure illustrates SNMP module dataflow:



CA SiteMinder® SNMP Dataflow:

1. The SNMP Master Agent receives SNMP requests from a management application.
2. The SNMP Master Agent forwards the SNMP request to the SNMP Subagent.
3. The CA SiteMinder® SNMP Subagent retrieves the requested information from OneView Monitor.
4. The CA SiteMinder® SNMP Subagent passes the retrieved information back to the SNMP Master Agent.
5. The SNMP Master Agent generates an SNMP response and sends it back to the requesting management application.

CA SiteMinder® MIB

The CA SiteMinder® MIB provides a SNMPv2-compliant data representation of all monitored components in the CA SiteMinder® environment.

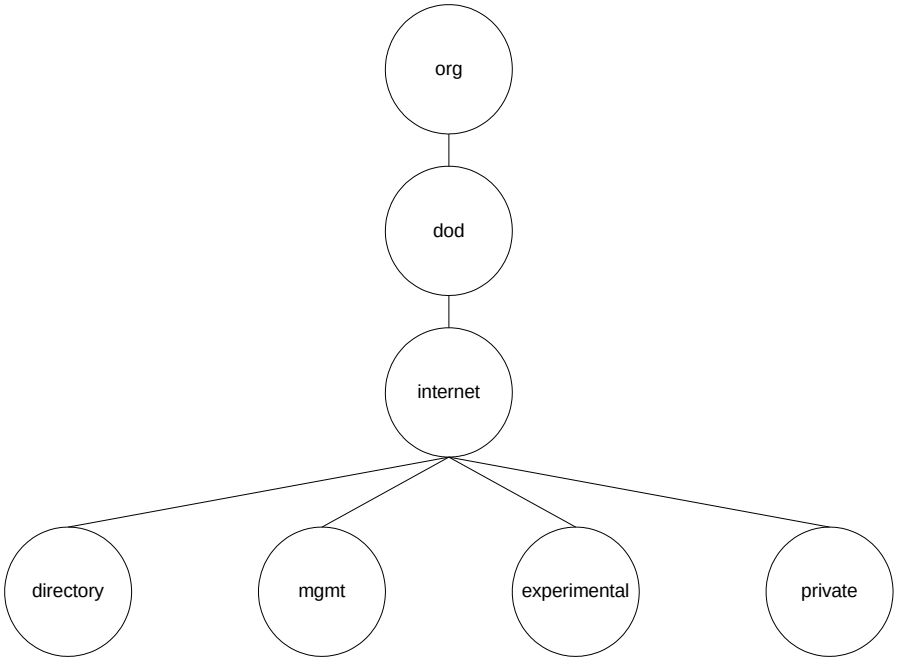
The CA SiteMinder® MIB is supplied in an ASCII text file:

SiteMinder_Install_Directory\mibs\NetegritySNMP.mib.

MIB Overview

SNMP MIB structure is logically represented by an inverse tree hierarchy. MIBs for internet-related products such as CA SiteMinder® are located under the ISO main branch of the MIB hierarchy.

The upper part of the ISO branch is shown in the following figure.

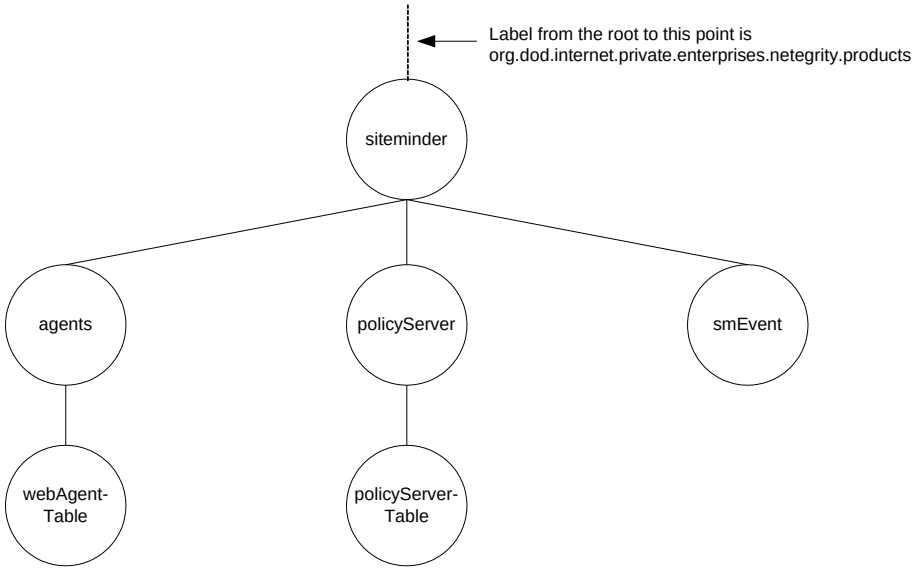


MIB branches, MIBs, and managed objects within MIBs are all identified by short text strings. Complete MIB hierarchies can be expressed notationally by concatenating branch and object identifiers, separating each entry with a period. For example, the private sub-branch of the internet entry shown above can be expressed as *iso.org.dod.internet.private.*

SiteMinder MIB Hierarchy

The CA SiteMinder® MIB can be expressed as *iso.org.dod.internet.private.enterprises.netegrity.products.siteminder*.

Supported managed components represented by MIB objects are Policy Servers and Web Agents. Because there can be multiple instances of each of these components, the managed properties of each of these components are columnar objects.



The CA SiteMinder® MIB has three sub-branches:

Policy Server

Contains the Policy Server (policyServerTable) objects.

agents

Contains Web Agent (webAgent) objects.

smEvent

Contains SNMP trap types for system events.

MIB Object Reference

The following sections contain detailed lists of the Policy Server, Web Agent, and Event MIB objects.

Authentication Server Data

The following table contains the subset of Authentication Server properties that are exposed as objects in the CA SiteMinder® MIB, which are under iso.org...siteminder.policyServer.policyServerTable.

Object Name	SNMP Type	Object Description
policyServerIndex	Integer32	A unique identifier for the current Policy Server instance.
policyServerHostID	IP address	IP address of the machine where the Policy Server is installed.
policyServerType	Display string	Type of component.
policyServerStatus	Integer32	Status of the Policy Server. The status can be Active or Inactive.
policyServerPort	Integer32	Policy Server port number.
policyServerProduct	Display string	Policy Server product name.
policyServerPlatform	Display string	Operating system of the machine where the Policy Server is installed.
policyServerVersion	Display string	Version number of the Policy Server.
policyServerUpdate	Display string	Version number of the most recently applied update.
policyServerLabel	Display string	Policy Server build number.
policyServerCrypto	Integer32	Length of the encryption key used to encrypt/decrypt data sent between the Web Agent and the Policy Server.
policyServerUTC	Display string	The startup time of the Web server where the Policy Server is installed. The time is specified in Universal Coordinated Time format.
policyServerTime Zone	Integer32	Time zone for the geographical location where the Policy Server is installed.
policyServerMaxSockets	Integer32	Maximum number of open sockets (which correspond to the number of open connections between the Policy Server and Web Agents) that the Policy Server can support.
policyServerSocketCount	Gauge32	Number of open sockets, which corresponds to the number of open connections between the Policy Server and Web Agents.
policyServerAuth AcceptCount	Counter32	Number of successful authentications.

Object Name	SNMP Type	Object Description
policyServerAuthReject-Count	Counter32	Number of failed authentication attempts. These attempts failed because of invalid credentials.
policyServerAzAccept-Count	Counter32	Number of successful authorizations.
policyServerAzReject-Count	Counter32	Number of failed authorization attempts. These attempts failed because of invalid credentials.
policyServerPolicy-CacheEnabled	Truth Value	Indicates whether or not policy cache is enabled.
policyServerL2Cache-Enabled	Truth Value	Indicates whether or not L2 cache is enabled.

Web Agent Objects in the SiteMinder MIB

The following table contains the Web Agent properties that are exposed as objects in the CA SiteMinder® MIB, which are under iso.org...siteminder.webAgentTable.webAgentEntry.

Object Name	SNMP Type	Object Description
webAgentIndex	Integer32	A unique identifier for the current Web Agent instance.
webAgentHostID	IP address	IP address of the machine where the web agent server is installed.
webAgentType	Display string	Type of component.
webAgentStatus	Integer32	Status of the Web Agent. The status can be Active or Inactive.
webAgentPort	Integer32	Web Agent port number.
webAgentProduct	Display string	Web Agent product name.
webAgentPlatform	Display string	Operating system of the machine where the Web Agent is installed.
webAgentVersion	Display string	Version number of the Web Agent.
webAgentUpdate	Display string	Version number of the most recently applied update.
webAgentLabel	Display string	Web Agent build number.
webAgentCrypto	Integer32	Length of the encryption key used to encrypt/decrypt data sent between the Web Agent and the Policy Server.

Object Name	SNMP Type	Object Description
webAgentUTC	Display string	The startup time of the Web server where the Web Agent is installed. The time is specified in Universal Coordinated Time format.
webAgentTime Zone	Integer32	Time zone for the geographical location where the Web Agent is installed.
webAgentSocketCount	Gauge32	Number of open sockets, which corresponds to the number of open connections between the Policy Server and the Web Agent. **Note:** Because the Web Agent architecture has changed, SocketCount has no value.
webAgentResource-Cache Count	Integer32	Number of entries in the resource cache. The resource cache stores information about recently accessed resources to speed up subsequent requests for the same resource. The number of entries in the resource cache can be 0 to the *n*, where n is the maximum cache size specified in the Web Agent's configuration.
webAgentResource-Cache Hits	Integer32	Number of times that the resource cache is accessed. This number indicates how frequently CA SiteMinder® is using cached resources.
webAgentResource-Cache Misses	Integer32	The number of times the Web Agent could not locate a resource in the resource cache. This occurs when: ■ The resource has not been accessed before. ■ The cached information has expired.
webAgentUserSession-CacheCount	Integer32	Number of entries in the user session cache. The user session cache stores information about users who have recently accessed resources. Storing user information speeds up resource requests. The number of entries in the user session cache can be 0 to *n*, where *n* is the maximum cache size specified in the Web Agent's configuration. **Note:** The user session cache count may differ based on the Web server where the session cache is located.
webAgentUserSession-CacheHits	Integer32	Number of times that Web Agent accessed the user session cache.

Object Name	SNMP Type	Object Description
webAgentUserSession-CacheMisses	Integer32	The number of times the Web Agent could not locate user session information in the user session cache. This occurs when: ■ The user has not accessed a resource before. ■ The cached information has expired.
webAgentIsProtected-Count	Integer32	Number of times the Web Agent has checked the Policy Server to see if a resource is protected. **Note:** If the resource cache is set to 0, two or more IsProtected calls may be recorded per login attempt. If the Web Agent is not caching information, it must check with the Policy Server to determine whether or not a resource is protected each time a request is made to the Web server. If the resource cache is not set to 0, only one IsProtected call will be recorded. In this case, the Web Agent makes one IsProtected call to the Policy Server; subsequent requests to the Web server for the same resource are satisfied against the Web Agent's resource cache until the resource in the cache expires or the resource cache is flushed.
webAgentIsProtected-Errors	Integer32	Number of times an error has occurred when the Web Agent asks the Policy Server whether or not a resource is protected. An error indicates a communication failure between the Web Agent and the Policy Server.
webAgentIsProtected-AvgTime	Unsigned 32	The average amount of time it takes for the Web Agent to determine from the Policy Server whether or not a resource is protected.
webAgentLoginCount	Counter 32	Number of login attempts made from this Web Agent.
webAgentLoginErrors	Counter 32	Number of errors that occurred during login attempts. An error indicates a communication failure between the Web Agent and the Policy Server.
webAgentLoginFailures	Counter 32	Number of failed login attempts because users were not authenticated or authorized by the Policy Server.
webAgentLoginAvgTime	Unsigned 32	Average time it takes for a user to log into a resource.

Object Name	SNMP Type	Object Description
webAgentValidation-Count	Counter 32	The number of times a specific Web Agent attempted to validate a session cookie against the Policy Server to authenticate a user, instead of matching that user's credentials to a user directory entry. (The Web Agent creates a session cookie on the user's browser when a user is successfully authenticated, and uses that cookie to authenticate the user on subsequent requests for new resources.).
webAgentValidation-Errors	Counter 32	The number of errors that have occurred when the Web Agent attempted to validate a user session. Errors indicate a communication failure between the Web Agent and the Policy Server.
webAgentValidation-Failures	Counter 32	The number of times the Web Agent has failed to validate a user session because of an invalid session cookie.
webAgentValidation-AvgTime	Unsigned 32	Average amount of time it takes to validate a cookie used to authenticate a user (in milliseconds). Cookies may be used to authenticate a user in a single sign-on environment.
webAgentAuthorize-Count	Counter 32	Number of authorization attempts made by this Agent. An authorization attempt occurs when a user supplies credentials to the Policy Server in order to access a protected resource.
webAgentAuthorize-Errors	Counter 32	Number of errors that occurred during authorization attempts made by this Web Agent. An error indicates a communication failure between the Web Agent and Policy Server during an authorization call.
webAgentAuthorize-Failures	Counter 32	Number of failed authorization attempts. An authorization attempt fails when a user enters invalid credentials.
webAgentAuthorize-AvgTime	Integer32	Indicates the average time it takes to authorize a user (in milliseconds)
webAgentCrosssite-ScriptHits	Integer32	Number of cross-site scripting hits. A cross-site scripting hit consists of malicious code embedded in pages at your site. For more information about cross-site scripting, see the *CA SiteMinder® Web Agent Configuration Guide*.
webAgentBadURL-charsHits	Integer32	Number of requests that the Agent refuses because of bad URL characters. Bad URL characters are specifically blocked to prevent a Web client from evading CA SiteMinder® rules. These characters are specified in the Web Agent's configuration.

Object Name	SNMP Type	Object Description
webAgentBadCookie-HitsCount	Gauge32	Number of cookies that the Web Agent could not decrypt.
webAgentExpired-CookieHitsCount	Gauge32	Number of requests that contained an expired cookie.

Event Data

The following table contains the objects in the CA SiteMinder® MIB, under iso.org…siteminder.smEvents, for system events that can be mapped to SNMP traps using the CA SiteMinder® Event Manager

Event Name	Event ID	Event Category	Event Category Type
serverInit	SmLogSystemEvent_ServerInit	Server activity	System
serverUp	SmLogSystemEvent_ServerUP		
serverDown	SmLogSystemEvent_ServerDown		
serverInitFail	SmLogSystemEvent_ServerInitFail		
dbConnectionFailed	SmLogSystemEvent_DbConnectFail		
ldapConnection-Failed	SmLogSystemEvent_LDAP-ConnectFail		
logFileOpenFail	SmLogSystemEvent_LogFile-OpenFail	System Activity	
agentConnection-Failed	SmLogSystemEvent_Agent-ConnectionFail		
authReject	SmLogAccessEvent_AuthReject	Authentication	Access
validateReject	SmLogAccessEvent_ValidateReject		
azReject	SmLogAccessEvent_AzReject	Authorization	

Event Name	Event ID	Event Category	Event Category Type
adminReject	SmLogAccessEvent_AdminReject	Administration	
objectLoginReject	SmLogObjEvent_LoginReject	Authentication	Object
objectFailedLoginAttemptsCount	SmLogObjEvent_FailedLogin-AttemptsCount		
emsLoginFailed	SmLogEmsEvent_LoginFail	DirectorySession	EMS
emsAuthFailed	SmLogEmsAuthFail		

Configure the CA SiteMinder® Event Manager

The Event Manager application (supplied as a library file, EventSNMP.dll) that captures Policy Server events, determines whether SNMP traps are to be generated for those events (as specified by a configuration file) and if so, generates SNMP traps to specified NMS(s).

To configure the Event library (EventSNMP.dll), see Add Event Handler Libraries (see page 130).

You configure the CA SiteMinder® Event Manager by defining the Event Configuration File (*SM_Install_Directory*\config\snmptrap.conf), which defines what events are to be processed and the addresses of the NMSs to which the traps should be sent.

Event Configuration File Syntax

The snmptrap.conf is an editable ASCII file, with a simple one line per event syntax:

```
Event_Name      Destination_Address
```

Event_Name

The name of a MIB event object (or a comma-separated group of names of event objects).

Examples:

serverUP

serverUp,serverDown

serverUp,serverDown,serverInitFail

Destination_Address

The address of an NMS (or a comma-separated group of the addresses of NMSs) to which generated traps should be sent. Each address should be of the form: *HostID*:*port*:*community*

HostID

(mandatory) Either a hostname or IP address.

Port

(optional) IP port number.

Default: 162.

Community

(optional) An SNMP community. Note that if community is specified, Port must also be specified.

Default: "public"

Example: 100.132.5.166

Example: 100.132.5.166:162

Example: victoria:162:public

Note: Be careful to avoid event duplication. That is, you should avoid putting the same event in multiple entries. Also, comment lines can be added lines, prefixed with a "#" character.

Event Configuration File Examples

```
ServerDown,serverUp     111.123.0.234:567:public
```

This entry configures the Event Manager to send serverDown and serverUp SNMP traps to the NMS at IP address 111.123.0.234, port 567, community public.

```
agentConnectionFailed    111.123.0.234,victoria
```

This entry configures the Event Manager to send SNMP traps of agentConnectionFailed type will be sent to IP address 111.123.0.234, port 567, community public and to host "victoria", port 567, community public.

```
azReject
```

This entry configures the Event Manager to discard all events of the azReject type so that no traps are sent.

Start and Stop SiteMinder SNMP Support

If you chose to install CA SiteMinder® SNMP support when you installed the Policy Server, the CA SiteMinder® SNMP Agent service should start automatically whenever the Policy Server initializes.

This section describes how to manually start and stop the CA SiteMinder® SNMP subagent on Windows and UNIX Policy Servers.

Start and Stop the Windows Netegrity SNMP Agent Service

To start the CA SiteMinder® SNMP subagent on Windows Policy Servers

1. Open the Services control panel:
   - (Windows Server) Start, Settings, Control Panels, Administrative Tools, Services.
   - (Windows NT) Start, Settings, Control Panels, Services.
2. Select the Netegrity SNMP Agent service.
3. Click Start.

   Note: When you restart the Windows SNMP service, also manually restart the Netegrity SNMP Agent service.

To stop the CA SiteMinder® SNMP subagent on Windows Policy Servers

1. Open the Services control panel:
   - (Windows Server) Start, Settings, Control Panels, Administrative Tools, Services.
   - (Windows NT) Start, Settings, Control Panels, Services.
2. Select the Netegrity SNMP Agent service.
3. Click Stop.

   Note: If you stop the Windows SNMP service, the Netegrity SNMP Agent service is not generally available, but can then be accessed through port 801.

Start and Stop SNMP support on UNIX Policy Servers

On UNIX Policy Servers, the CA SiteMinder® service can only be started or stopped by starting or stopping the Sun Solstice Enterprise Master agent (snmpdx) daemon.

To start the Netegrity SNMP Agent service on UNIX Policy Servers

1. Login as super user (root)
2. Type cd /etc/rc3.d
3. Type sh SXXsnmpdx (S76snmpdx) start

To stop the Netegrity SNMP Agent service on UNIX Policy Servers

1. Login as super user (root)
2. Type cd /etc/rc3.d
3. Type sh SXXsnmpdx (S76snmpdx) stop

   Note: Stopping the Sun Solstice Enterprise Master agent operation will disable all SNMP services on the UNIX host.

Troubleshooting the SiteMinder SNMP Module

This section provides some advice and describes some tools that CA SiteMinder® provides to help you isolate the point of failure if you have trouble establishing a management connection to, or receiving SNMP traps from CA SiteMinder®.

SNMP Traps Not Received After Event

Symptom:

I am not receiving SNMP traps when events that should have generated them occur.

Solution:

1. Check network connectivity between the NMS and monitored Policy Server.
2. Check that the CA SiteMinder® SNMP subagent and SNMP master agent are running on the Policy Server.
3. Enable trap logging by setting the NETE_SNMPLOG_ENABLED system environment variable.

   CA SiteMinder® generates the following log files in sminstalldir/log:

   Windows:

   ```
   SmServAuth_snmptrap.log
   SmServAz_snmptrap.log
   SmServAcct_snmptrap.log
   SmServAdm_snmptrap.log
   ```

   UNIX:

   ```
   smservauth_snmptrap.log
   smservaz_snmptrap.log
   smservacct_snmptrap.log
   smservadm_snmptrap.log
   ```

Important! The log files generated can grow very rapidly. You should disable trap logging and delete the file as soon as you have resolved your trap receipt issues.

Chapter 19: SiteMinder Reports

This section contains the following topics:

Report Descriptions

SiteMinder reports are organized into two groups:

- Audit reports
- Analysis reports

Audit reports are created from existing audit capabilities of the Policy Server. The Policy Server must be configured to write to a database.

Analysis reports are based on run-time policy evaluation, for example, evaluating which users can perform what tasks.

You can generate the following reports using the SiteMinder Administrative UI:

Activity By User

Lists activities of all users during the specified time period.

Administrative Operations by Administrator

Lists all administrative operations in the policy store by administrator.

Applications

Lists all configured applications that the user is authorized to use.

Applications by User

Lists all users for a given set of applications.

Denied Authorizations

Lists all denied authorizations.

Denied Resources

Lists all denials of requested resources.

Policies by Role

Lists all policies for a specified set of roles in an application.

Protected Resources

Lists all protected resources (realm + rule filter).

Resource Activity

Lists all authentication and authorization activity by resource.

Resources by User

Lists all resources for a specified set of users.

Roles by Application

Lists all roles that are defined for each specified application.

Roles by Resource

Lists all roles that are defined for a specified resource.

Users by Resource

Lists all users that are associated with each specified resource. When you run this report, ensure that you set a valid Universal ID in the user directory.

Users by Role

Lists all users that belong to a specified role.

Schedule a CA SiteMinder® Report

You can schedule a CA SiteMinder® audit or analysis report under Reports in the Administrative UI.

Follow these steps:

1. Click Reports,Audit or Analysis.
2. Select the report that you want.
3. Fill in all the required parameters. These parameters vary depending on the type of report.
4. Click Next.
5. Select one option from the drop-down list.
6. Enter a description.
7. Click Submit.

View CA SiteMinder® Reports

On the Reports tab in the Administrative UI, you can view any CA SiteMinder® report whose status is Complete. If the status is Failed, you can view the status details.

To view CA SiteMinder® reports

1. Click Reports, General, View SiteMinder Reports.

   The SiteMinder Report Search pane appears.

2. Click the radio button for the report you want to view. Note that the Status field must indicate that the report has completed.

3. Click Select.

   The report is displayed on the screen.

4. (Optional) Click the file icon if you want to save the report to a file. Select the output file format from the drop-down list.

5. (Optional) Click the printer icon to print the report.

6. (Optional) You can page through the report or enter a search string.

7. Click Close when you are finished viewing the report.

Delete CA SiteMinder® Reports

You can delete one or more CA SiteMinder® reports on the Reports tab of the Administrative UI.

To delete CA SiteMinder® reports

1. Click Reports, General, Delete CA SiteMinder® Reports.

   The Delete CA SiteMinder® Reports pane opens.

2. Search for CA SiteMinder® reports to delete by Report Name or Description or search for all CA SiteMinder® reports.

3. Select one or more or all CA SiteMinder® reports to delete, and click Submit.

The Delete CA SiteMinder® Reports task is submitted for processing.

Chapter 20: Policy Server Tools

This section contains the following topics:

Policy Server Tools Introduced

CA SiteMinder® provides a number of administrative tools to help manage your environment. The following list describes the function of each tool.

smobjimport

Imports policy data into the CA SiteMinder® policy store.

Note: This utility is available only to import an existing backup smdif file into the policy store. To migrate a policy store manually, use the XPSExport and XPSImport utilities.

smkeyexport

Exports keys from the key store.

smkeyimport

Imports keys into the key store.

smkeytool

Lets you manage the certificate data store.

You can also use this utility with the access legacy key store flag (-accessLegacyKS) to manage an existing smkeydatabase during a migration to 12.52 SP1.

Note: For more information about migrating the contents of a smkeydatabase to the certificate data store, see the *CA SiteMinder® Upgrade Guide*.

smldapsetup

Manages the CA SiteMinder® policy store in an LDAP directory.

ODBC database SQL scripts

Removes CA SiteMinder® policy store, token data, and log schema from ODBC databases.

smpatchcheck

Verifies that all required/recommended patches are installed on your Solaris system.

smreadclog

Reads RADIUS log files that the Policy Server generates.

smreg

Lets you change the CA SiteMinder® superuser password.

In addition, CA SiteMinder® provides tools for working with policy data. The following list provides an overview of the XPS-family of tools. XPS tools are platform-independent command line utilities that XPS administrators can use to manage policy store data. To learn about the options for a particular tool, enter the tool name followed by a question mark at the command line. For example:

```
XPSConfig ?
```

XPSConfig

Manages configuration data including vendors, products, and product parameters.

Note: To use XPSConfig, your administrator account requires XPSConfig privileges.

XPSEvaluate

Evaluates expressions and lets you test performance.

Note: To use XPSEvaluate, your administrator account requires XPSEvaluate privileges.

XPSExplorer

Manages policy data including vendors, products, and applications.

Note: To use XPSExplorer, your administrator account requires XPSExplorer privileges.

XPSExport

Exports data from a policy store.

XPSImport

Imports data to a policy store.

XPSSecurity

Allows interactive creation and editing of XPS Administrators and their rights. To use this tool, copy it from either \win32\tools or /solaris/tools from the CA SiteMinder® installation file that you downloaded from Support to *siteminder_home*\bin.

siteminder_home

Specifies the Policy Server installation path.

Important! After you use XPSSecurity, delete it from *siteminder_home*\bin to prevent unauthorized use.

Note: To use XPSSecurity, your administrator account requires XPSSecurity privileges.

XPSSweeper

Synchronizes XPS and CA SiteMinder® policy stores.

Note: To use XPSSweeper, you require an administrator. No additional rights are required.

Windows 2008 Policy Server Tools Requirement

If you are running a CA SiteMinder® utility or executable on Windows Server 2008, be sure to open the command–line window with Administrator permissions, even if you are logged into the system as an Administrator. For more information, see the release notes for your CA SiteMinder® component.

Requirement When Using the Policy Server Tools on Linux Red Hat

For the Policy Server tools to work correctly on a Linux Red Hat operating system, define the Policy Server host name in /etc/hosts. You define the host name in this location because these utilities generate adminoids and OIDs. The operating system uses the gethostid() and gettimeofday() Linux functions when generating these OIDs.

Import Policy Data Using smobjimport

You can use the smobjimport tool to import the entire policy store or a single policy domain.

Note: This utility is available only to import an existing backup smdif file into the policy store. To migrate a policy store manually, use the XPSExport and XPSImport utilities.

Follow these steps:

1. Navigate to one of the following locations:
   - (Windows) *siteminder_home*\bin

     siteminder_home

     Specifies the Policy Server installation path.
   - (Unix) *siteminder_home*/bin
2. Run the following command:

   `smobjimport -ifile_name -dadmin-name -wadmin-pw -v -t [-cf | -cb]`

   Example 1: smobjimport -ipstore.smdif -dSiteMinder -wpassword -v -t -cf

   Example 2: smobjimport -ipstore.smdif -dSiteMinder -wpassword -v -t -cb

   -cf

   (Optional) Imports sensitive data using FIPS-compatible (AES) cryptographic algorithms.

   Note: This argument is required only if the Policy Server is operating in FIPS-only mode.

   -cb

   (Optional) Imports sensitive data using RC2 cryptographic algorithms.

   Important!

   - If the file you are importing contains sensitive data in clear-text, the following option is required to import the data:
     –c

     Failure to use this option can corrupt the policy store.
   - Only enter the smdif file with the smobjimport command. If the smdif and cfg files are in the same directory, the utility automatically imports both. The environment properties stored in the cfg file take precedence over the ones in the smdif file. You can overwrite the data of an environment by pairing the smdif file with a different cfg file.

Overview of the XML-based Data Format

Enterprise environments can require policy store data to be moved from one environment to another, such as from a development environment to a staging environment. In releases prior to r12, policy objects are represented using the proprietary SiteMinder Data Interchange Format (SMDIF), using smobjimport and smobjexport for migrating the data. This export format and these tools have been replaced by an XML-based export format, using XPSExport and XPSImport to migrate the data.

The XML-based export format uses the following fundamental schemas:

XPSDeployment.xsd

Describes the top-level schema, which includes the other schemas. It defines the root element and sub-elements. An XML file conforming to this schema can contain an instance of Data Dictionary, Policy, and Security Data.

XPSDataDictionary.xsd

Describes meta-data information about object types and their properties.

XPSPolicyData.xsd

Describes the meta-data information about objects stored in the policy store, such as domains, policies, rules, applications, and the relationships between them.

XPSSecurityData.xsd

Describes meta-data used for representing policy store administrators and their access rights.

XPSGeneric.xsd

Contains definitions of the generic data types used in the other schema files.

This format supports not only exporting and importing policy data in its entirety, but also exporting and importing a subset of the policy data. A granular export presupposes knowledge of how the data will be imported. On export, you can specify the entire policy data, or a portion of the data using an object identifier and optionally one of these three export types:

- Add—specifies that only additions can be done during import.
- Replace—specifies an overwrite of existing policy data during import.
- Overlay—specifies that updates to policy data are done during import.

Note: The XPSExport and XPSImport tools encrypt sensitive data based on the FIPS mode the Policy Server is operating in. There are no additional parameters in these tools to set for data encryption.

XPSExport

The XPSExport tool supports the following tasks for migrating Policy Store data:

- Export all the security data.
- Export all the policy data.
- Export all the configuration data.
- Export a portion of the policy data.

You can export a subset of policy data by specifying the identifier of a root object. Specify this identifier in the command line or in a file (using the -xf parameter). Only those objects that do not have a parent class can be exported. For example, to export a realm object, you specify the identifier (XID) of the parent domain for the realm.

You can also create and edit a custom export file using the "shopping cart", or XCart, capability in XPSExplorer (XPSExplorer -xf). You can set the import mode (ADD, OVERLAY, REPLACE, or DEFAULT) on a per object basis in the XCart file. You can then pass the XCart file to XSPExport using the -xf parameter.

Consider the following factors:

- XPSExport does *not* export keys from the key store. Use the smkeyexport command for this purpose.
- When moving policies from one environment to another, some objects that are environment–specific are included in the export file. Examples of these objects include:
  - Any Trusted hosts
  - Any HCO Policy Server settings
  - Any Authentication scheme URLs
  - Any Password services redirects
  - Any Redirect responses

Depending on the mode you select when using XPSExport, these objects could possibly be added to the new environment or can overwrite existing settings. Be sure that you do not adversely affect environment settings when importing the objects.

Syntax

The syntax of the XPSExport is following:

```
XPSExport output_file [-xo object_XID] [-xo-add object_XID] [-xo-replace object_XID]
[-xo-overlay object_XID] [-xf file_name] [-xb] [-xe] [-xp] [-xs] [-xc] [-xi] [-xm]
[-f] [-fm] [-q] [-m <number>[%]] [-pass <passphrase>][-npass] [-comment comment]
[-cf commentpath] [-?] [-vT] [-vI] [-vW] [-vE] [-vF] [-l log_file] [-e err_file]
```

Parameters

output_file

The output XML file.

-xo *object_XID*

Specifies one or more objects for granular export. You can optionally specify one of the following export types:

-xo-add *object_XID*

Specifies only additions are done during an import.

-xo-replace *object_XID*

Overwrites the policy data during an import.

-xo-overlay *object_XID*

Updates the policy data during an import.

-xf *file_name*

(Optional) Specifies the absolute name of a file that contains the list of XIDs of objects to be exported.

The entries in the file have the following format:

CA.SM::UserDirectory@0e-255e2456-556d-40fb-93cd-f2fed81f656e

ADD = CA.SM::AuthScheme@0d-4afc0e41-ae25-11d1-9cdd-006008aac24b

REPLACE = CA.SM::Agent@01-cb8b3401-a6aa-4794-964e-c569712269c0

OVERLAY = CA.SM::Domain@03-7bdf31f2-44d7-4d7b-a8f5-5de2eaa0b634

These entries correspond to the following command-line parameters:

```
-xo CA.SM::UserDirectory@0e-255e2456-556d-40fb-93cd-f2fed81f656e
-xo-add CA.SM::AuthScheme@0d-4afc0e41-ae25-11d1-9cdd-006008aac24b
-xo-replace CA.SM::Agent@01-cb8b3401-a6aa-4794-964e-c569712269c0
-xo-overlay CA.SM::Domain@03-7bdf31f2-44d7-4d7b-a8f5-5de2eaa0b634
```

-xb

(Optional) Exports all the objects of a policy store, including the location of the policy store. The policy store location is set on the Data tab of the Policy Server Management Console.

Important! Any Policy Server to which you import this data uses the policy store that is specified during the export. For example, you export data from Policy Server A, which uses an ODBC database as a policy store. Later, you import the data into Policy Server B, which uses Active Directory as a policy store. The location of the Active Directory policy store for Policy Server B is replaced with the ODBC database location for Policy Server A.

-xe

(Optional) Exports the object types that are related to the execution environment.

-xp

(Optional) Exports the object types that are related to the policies.

The -xe and -xp options cannot be used with -xo, -xo-add, -xo-replace, -xo-overlay, or -xf.

Important! The -xe and -xp options supersede the -xa option to extract all policy data, except federation related objects. You can also use the -xb option, which lets you backup the entire policy store, including Policy Server location-specific data, such as the policy store location.

-xs

(Optional) Exports the entire security data.

-xc

(Optional) Exports the entire configuration data.

-xi

(Optional) Exports the object types that were initially installed.

Example: AgentType

-xm

(Optional) Exports the objects that are specified in an ExtractManifest object.

-f

(Optional) Overwrites the output file.

-fm

(Optional) Uses less memory, but affects the performance.

-q

(Optional) Suppresses progress messages.

-m <number>[%]

(Optional) Indicates that progress messages are output after every <number> of objects.

If the optional percent sign ("%") is included, then <number> is a percentage of the total objects, not a number of objects.

Default: Ten percent.

-pass <passphrase>

(Optional) Specifies the passphrase that is required for encryption of sensitive data. This passphrase must be at least eight characters long and must contain at least one digit, one uppercase, and one lowercase character. The passphrase can contain a space that is enclosed in quotes. If not specified as a command-line option, the export process prompts for a passphrase when sensitive data is being exported.

-npass

(Optional) Specifies that no passphrase is used.

Important! Sensitive data is exported as clear text.

-comment

(Optional) Adds a comment to the output file.

-cf commentpath

(Optional) Obtains the comment from the <commentpath> and adds it to the output file.

-?

Displays command-line help.

-nb

(Optional) Averts the beeps on error.

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING (default).

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

-l log_file

(Optional) Outputs log to the specified file.

-e err_file

(Optional) Specifies the file to which errors and exceptions are logged. If omitted, stderr is used.

Example

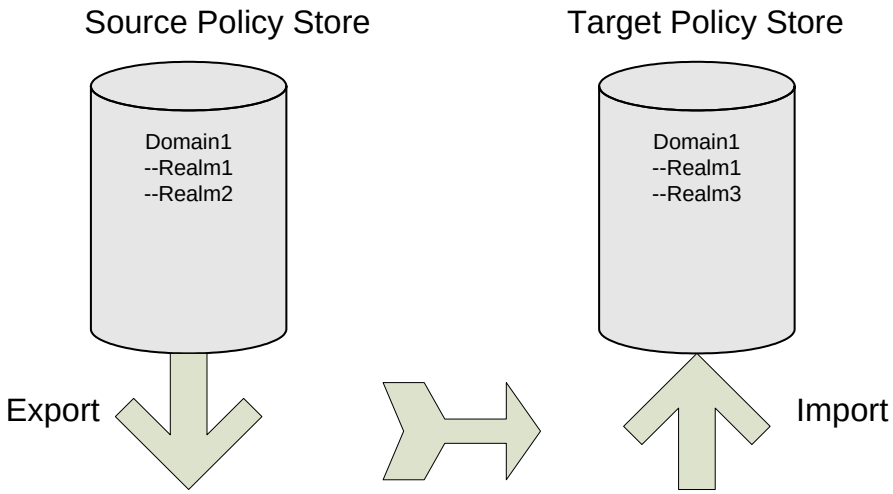
```
XPSExport PolicyData.xml -xo
CA.SM::UserDirectory@0e-255e2456-556d-40fb-93cd-f2fed81f656e
-xo-overlay CA.SM::Domain@03-7bdf31f2-44d7-4d7b-a8f5-5de2eaa0b634
```

Note: For granular exports, the export type is specified explicitly on the command line or is retrieved from the data dictionary. For dump exports, the export type attribute for all objects is Replace. A load import of the policy data overwrites all of the policy data in the policy store.

If the XPSExport tool encounters any errors in the command-line options, the tool aborts and records the errors in the exception file (or stderr). The export process also aborts when the export of *any* object fails. The appropriate errors are logged to the exception file (or stderr) and the XML output file (if it has been created) is deleted.

Add Policy Data

The diagram following shows a SiteMinder policy domain named Domain1 in the source policy store that has to be exported and imported to the target policy store.



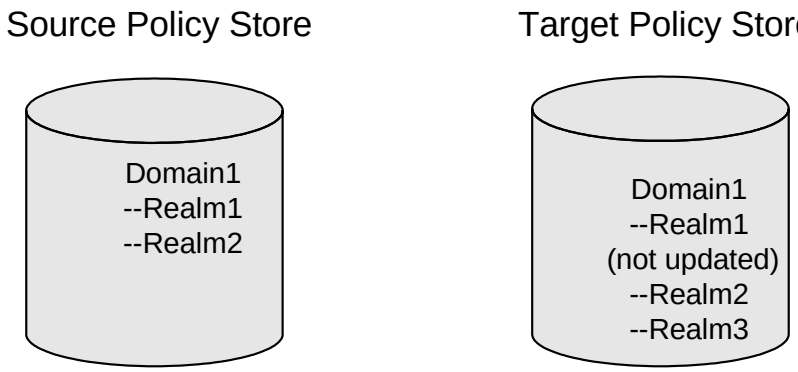
The target policy store already has a domain with the same name, but there are differences between the two:

- The properties of Realm1 have been updated in the source policy store and consequently have different values from their counterparts in the target policy store.
- There is a Realm2 in Domain1 that does not exist in the target policy store.

To specify a granular import of only one object (Realm2) into the target policy store, the command line on export would look like this:

```
XPSExport gran-add.xml -xo-add CA.SM:
:Domain@03-0fb7bd02-6986-4bb9-b240-c232358958b1
```

After a successful import Domain1 in the target policy store has three realms. The properties of Realm1 are not updated, as shown in the figure following.



To specify a granular export of an explicitly specified object (domain) into the target policy store using the add method, use the following command:

```
XPSExport –ma –xo <object_XID>
```

-ma

Adds all the objects appearing after this parameter on the command line.

To specify a granular export of all the relevant objects of the explicitly specified object (domain) into the target policy store using the add method, use the following command:

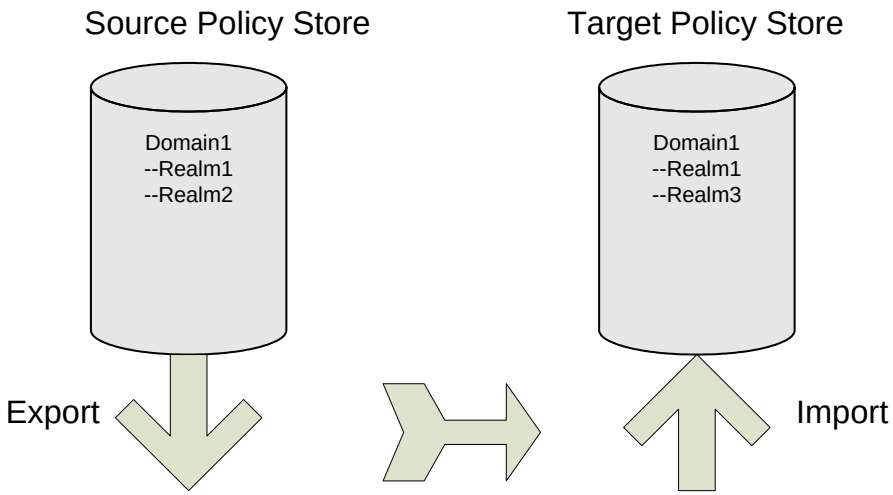
```
XPSExport –ra –xo <object_XID>
```

-ra

Adds the relevant system objects of the objects appearing after this parameter on the command line.

Overlay Policy Data

The diagram following shows a SiteMinder policy domain named Domain1 in the source policy store that has to be exported and imported to the target policy store.



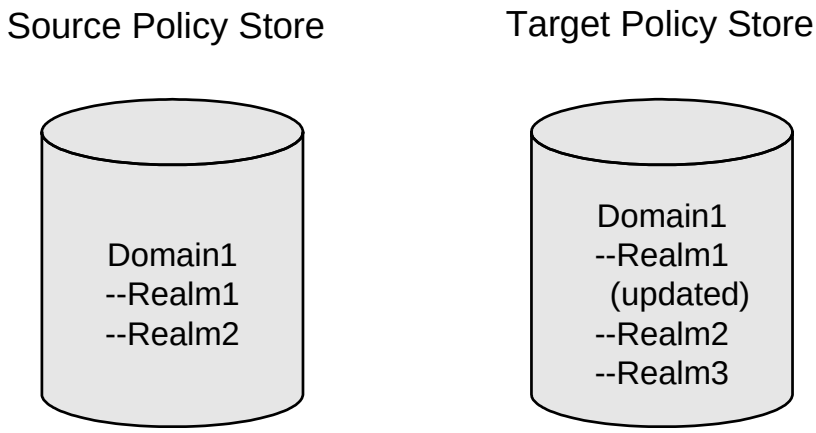
The target policy store already has a domain with the same name, but there are differences between the two:

- The properties of Realm1 have been updated in the source policy store and consequently have different values from their counterparts in the target policy store.
- There is a Realm2 in Domain1 that does not exist in the target policy store.

To specify a granular import where the target policy store is updated with the latest changes from the source policy store, the command line on export would look like this:

```
XPSExport gran-add.xml -xo-overlay CA.SM:
:Domain@03-0fb7bd02-6986-4bb9-b240-c232358958b1
```

After a successful import the properties of Realm1 on the target policy store are updated, as shown in the figure following.



To specify a granular export of an explicitly specified object (domain) into the target policy store using the overlay method, use the following command:

```
XPSExport –mo –xo <object_XID>
```

-mo

Overlays all the objects appearing after this parameter on the command line.

To specify a granular export of all the relevant objects of the explicitly specified object (domain) into the target policy store using the overlay method, use the following command:

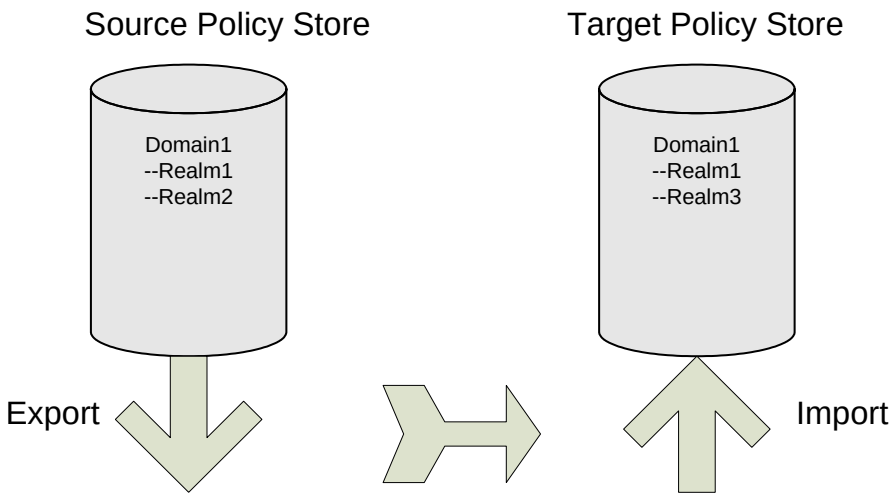
```
XPSExport –ro –xo <object_XID>
```

-ro

Overlays the relevant system objects of the objects appearing after this parameter on the command line.

Replace Policy Data

The diagram following shows a SiteMinder policy domain named Domain1 in the source policy store that has to be exported and imported to the target policy store.



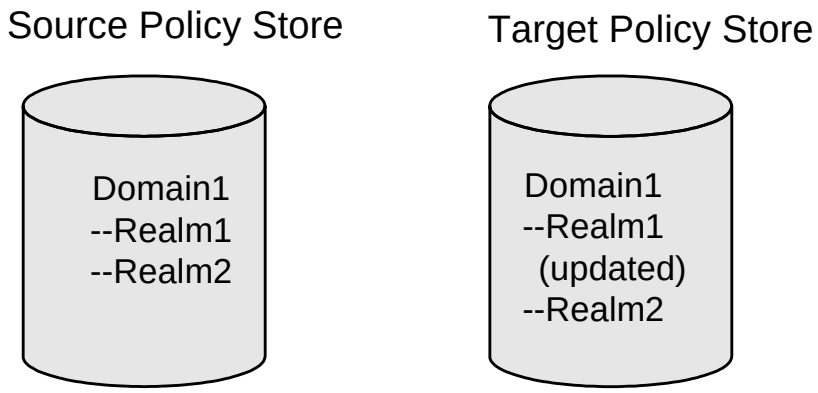
The target policy store already has a domain with the same name, but there are differences between the two:

- The properties of Realm1 have been updated in the source policy store and consequently have different values from their counterparts in the target policy store.
- There is a Realm2 in Domain1 that does not exist in the target policy store.

To duplicate the contents of the source policy store in the target policy store, the command line on export would look like this:

```
XPSExport gran-add.xml -xo-replace CA.SM:
:Domain@03-0fb7bd02-6986-4bb9-b240-c232358958b1
```

After a successful import Domain1 in the target policy store is exactly the same as Domain1 in the source policy store, as shown in the figure following.



To specify a granular export of an explicitly specified object (domain) into the target policy store using the replace method, use the following command:

```
XPSExport –mr –xo <object_XID>
```

-mr

Replaces all the objects appearing after this parameter on the command line.

To specify a granular export of all the relevant objects of the explicitly specified object (domain) into the target policy store using the replace method, use the following command:

```
XPSExport –rr –xo <object_XID>
```

-rr

Replaces the relevant system objects of the objects appearing after this parameter on the command line.

Merge Policy Data

When you migrate a domain object from one policy store to another, only the explicitly specified object (domain) is migrated. All the relevant objects of the domain (for example, user directories, agents, agent types) are not migrated to the target policy store. Without the relevant system objects, you cannot import the domain to a policy store.

To specify a granular export of an explicitly specified object (domain) into the target policy store using the merge method, use the following command:

```
XPSExport –mm –xo <object_XID>>
```

-mm

Merges all the objects appearing after this parameter on the command line.

To specify a granular export of all the relevant objects of the explicitly specified object (domain) into the target policy store using the merge method, use the following command:

```
XPSExport –rm –xo <object_XID>
```

-rm

Merges the relevant system objects of the objects appearing after this parameter on the command line.

Note: The Merge option is an alternative to the Add, Replace, or Overlay options. The Merge option is similar to the add option, the only difference being that this option adds not only the missing objects but also adds the missing attributes of the existing objects.

XPSImport

The XPSImport tool supports the following tasks for migrating policy store data:

- Import the entire policy data.
- Import a portion of the policy data.
- Import configuration data.

Note: XPSImport does not import keys into the key store. You must use smkeyimport for this purpose.

Syntax

The syntax for XPSImport is:

```
XPSImport input_file [-pass <passphrase>] [-npass] [-validate] [-fo] [-vT] [-vI] [-vW] [-vE] [-vF]
[-e file_name] [-l log_path] [-?]
```

Parameters

input_file

Specifies the input XML file.

-q

(Optional) Suppresses progress messages.

-m <number>[%]

(Optional) Indicates that progress messages are output after every <number> of objects.

If the optional percent sign ("%") is included, then <number> is a percentage of the total objects, not a number of objects.

Default: 10%.

-pass <passphrase>

(Optional) Specifies the passphrase required for decryption of sensitive data. The phrase must be the same as the phrase specified during export, or the decryption will fail.

-npass

(Optional) Specifies that no passphrase is to be used.

Important! Sensitive data is imported as clear text.

-validateOnly

(Optional) Validates the input XML file without updating the database.

-schemaFile

Specifies the schema file to validate the input file. If this option is not specified then input file will not be validated.

-fo

Allows force overwrite of existing policy store date for a dump load.

-?

Displays command-line help.

-nb

(Optional) Averts the beeps on error.

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING (default).

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

-l log_file

(Optional) Outputs log to the specified file.

-e err_file

(Optional) Specifies the file to which errors and exceptions are logged. If omitted, stderr is used.

Example

```
XPSImport PolicyData.xml -e C:\\tmp\\ExceptionLog.txt
```

This example imports policy data objects as specified in the PolicyData.xml file. It is not immediately evident from the command line if the import is a dump load or a granular import. That information can however be retrieved by looking at the IsDumpExport attribute of <PolicyData> element in the input XML file. If this attribute is set to true, it indicates that the input XML file has to be used for dump load.

Troubleshooting Policy Data Transfer

The following factors might possibly be relevant when transferring policy store data:

- Errors are logged to the console (stdout/stderr) or directed to a file.
- The levels of logging are listed following:
  - Trace
  - Information
  - Warning
  - Error
  - Fatal
- An export fails if the file already exists.
- An import is rolled back if validation fails for an object in the XML file.
- Granular import fails if objects exported with Add type already exist in the target policy store.

smkeyexport

The smexportkey tool exports keys from the key store. The syntax for smkeyexport is following.

```
smkeyexport -dadminname -wadminpw [-ooutput_filename] [-f] [-c] [-cb] [-cf] [-l] [-v] [-t] [-?]
```

-d

Specifies the name of the SiteMinder administrator.

-w

Specifies the password of the SiteMinder administrator.

-o

(Optional). Specifies the output file; defaults to stdout.smdif.

-f

(Optional).Overwrites an existing output file.

-c

(Optional). Exports sensitive data unencrypted.

-cb

(Optional). Exports sensitive data encrypted with backward-compatible cryptography.

-cf

(Optional). Exports sensitive data encrypted with FIPS-compatible cryptography.

-l

(Optional). Creates and logs entries to the specified file (filename.log).

-v

(Optional). Specifies verbose messaging.

-t

(Optional). Enables tracing.

-?

(Optional). Displays command options.

CA SiteMinder® Key Tool

The CA SiteMinder® key tool utility (smkeytool):

- Lets you manage the 12.52 SP1 certificate data store.
- Gives you access to a legacy smkeydatabase during an upgrade to 12.52 SP1. You use the access legacy key store flag (-accessLegacyKS) to resolve all data collisions that can result in a failed migration to the certificate data store.
- Is installed to the following location:

  siteminder_home\bin

  siteminder_home

  Specifies the Policy Server installation path.

Follow these steps:

1. Open a command line or shell.
2. Run one of the following commands:
   - (Windows) smkeytool.bat -*option* [-*arguments*]
   - (UNIX) smkeytool.sh -*option* [-*arguments*]

Use smkeytool to:

- Add client certificate keys

  If you are using a root or chain Certificate Authority (CA) at the consuming authority that is not listed in the smkeydatabase, add it to the smkeydatabase.

  For example, a signed VeriSign CA server-side certificate is used to SSL-enable the producer-side web server that is installed with the Web Agent Option Pack. To use this certificate for Basic over SSL authentication, add the VeriSign certificate to the smkeydatabase at the consumer. The addition of the certificate helps ensure that the consumer is communicating with a producer with a server-side certificate. The presence of the certificate also helps ensure that a trusted CA verified the certificate.

Add a Private Key and Certificate Pair

Use the addPrivKey option to import only a private key/certificate pair into the certificate data store. Consider the following items:

- You can have multiple private key/certificate pairs in the store, but CA SiteMinder® supports only RSA keys in the store.
- Only private key/certificate pairs are stored in encrypted form.

- A Policy Server at a producing authority:
  - Uses a single private key/certificate pair to sign SAML assertions.
  - Uses the certificate to decrypt encrypted SAML assertions received from the consuming authority.

  Typically, the key is the first private key/certificate pair found in the certificate data store.
- Delete the certificate metadata from the certificate file before importing it. Import only the data starting with the --BEGIN CERTIFICATE-- marker and ending with the --END CERTIFICATE-- marker. Be sure to include the markers.

Arguments for this option include the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the 12.52 SP1 certificate data store.

-alias *alias*

Required. Assigns an alias to a private key/certificate pair in the database. The alias must be a unique string and can contain only alphanumeric characters.

-certfile *cert_file*

Specifies the full path to the location of the certificate that is associated with the private key/certificate pair. Required for keys in PKCS1, PKCS5, and PKCS8 format.

-keyfile *private_key_file*

Specifies the full path to the location of the private key file. Required for keys in PKCS1, PKCS5, and PKCS8 format.

-keycertfile *key_cert_file*

Specifies the full path to the location of the PKCS12 file that contains the private key/certificate pair data. Required for keys in PKCS12 format.

-password *password*

(Optional) Specifies the password that was used to encrypt the private key/certificate pair when the pair was created. Supply this password to decrypt the key/certificate pair before it gets written to the certificate data store.

Note: This password is not stored in the certificate data store.

After the key/certificate pair is decrypted and placed in the certificate data store, CA SiteMinder® encrypts the pair again using its own password.

Add a Certificate

Use the addCert option to add a public certificate or trusted CA certificate to the certificate data store.

Consider the following items:

- The certificate can be a certificate that is associated with a private key/certificate pair. However, only the certificate is added to the certificate data store.
- If you trust a certificate as a Certificate Authority, this certificate is always treated as a CA certificate.
- For X.509 certificate formats, CA SiteMinder® supports V1, V2, and V3 versions. For encoding formats, CA SiteMinder® supports DER and PEM formats.
- Restart the Web Agent when you add a Certificate Authority certificate.
- Delete the certificate metadata from the certificate file before importing it. Import only the data starting with the --BEGIN CERTIFICATE-- marker and ending with the --END CERTIFICATE-- marker. Be sure to include the markers.

Arguments for this option include the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the 12.52 SP1 certificate data store.

-alias *alias*

Required. Specifies the alias to the certificate associated with the private key in the certificate data store.

Limit: A unique string that contains only alphanumeric characters.

-infile *cert_file*

Required. Specifies the full path to the location of the newly added certificate.

-trustcacert

Optional. Checks that the user provider certificate being added is a CA certificate. The utility checks that the certificate has a digital signature extension and that the certificate has the same IssuerDN and Subject DN values.

-noprompt

(Optional) The user is not prompted to confirm the addition of the certificate.

Add Revocation Information

Use the addRevocationInfo option to specify the location of a CRL. The certificate data store references the location of the CRL.

Arguments for this option include the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the 12.52 SP1 certificate data store.

-issueralias *issuer_alias*

Required. Specifies the alias of the Certificate Authority who issues the CRL.

Example: -issueralias verisignCA

-type (*ldapcrl | filecrl*)

Required. Specifies if the CRL is LDAP–based or file–based.

-location *location*

Required. Specifies the location of the CRL.

- (File-based) The full path to the file.

  Example: -location c:\crls\siteminder_root_ca.crl

- (LDAP directory service) The full path to the LDAP server node.

  Example: -location "http://localhost:880/sn=siteminderroot, dc=crls,dc=com"

Delete Revocation Information

Use the deleteRevocationInfo option to delete a CRL from the certificate data store.

Arguments for this option include the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the 12.52 SP1 certificate data store.

-issueralias *issuer_alias*

(Required) Specifies the name of the Certificate Authority who issues the CRL.

-noprompt

(Optional) The user is not prompted to confirm that the CRL can be deleted.

Remove Certificate Data

Use the removeAllCertificateData option to remove all certificate data from the certificate data store.

The argument for this option is the following:

-noprompt

(Optional) The user is not prompted to confirm that the certificate data can be removed.

Delete a Certificate

Use the delete option to remove a certificate from the certificate data store. If the certificate has an associated private key, the key is also deleted.

Arguments for this option include the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the 12.52 SP1 certificate data store.

-alias *<alias>*

(Required) Specifies the alias of the certificate that the option is to remove.

-noprompt

(Optional) The user is not prompted to confirm that the certificate can be removed.

Export a Certificate or Private Key

Use the export option to export a certificate or private key to a file.

Consider the following items:

- Certificate data is exported using PEM encoding.
- Private key data is exported using DER encoded PKCS8 format.

Arguments for this option include the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the 12.52 SP1 certificate data store.

-alias *alias*

(Required) Identifies the certificate or key to be exported.

-outfile *out_file*

(Required) Specifies the full path to the file to which the data is exported.

-type (key|cert)

(Optional) Specifies whether a certificate or key is being exported.

Default: certificate.

-password *password*

Required only when exporting a private key. Specifies the password that is used to encrypt the private key when exported. You do not need a password to export the certificate holding the public key because certificates are exported in clear text.

To add this private key back to the certificate data store, use the addPrivKey option with this password.

Find an Alias

Use the findAlias option to find the alias that is associated with a certificate in the certificate data store.

Arguments for this option include the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the 12.52 SP1 certificate data store.

-infile *cert_file*

(Required) Specifies the full path to the certificate file associated with the alias you want.

-password *password*

Required only when a password–protected P12 file is specified as the certificate file.

Import Default CA Certificates

Use the importDefaultCACerts option to import all default trusted Certificate Authority certificates that are included with CA SiteMinder® to the certificate data store.

The argument for this option is the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the 12.52 SP1 certificate data store.

List Metadata for all Certificates

Use the listCerts option to list some metadata of all certificates stored in the certificate data store.

Arguments for this option include the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the 12.52 SP1 certificate data store.

-alias *alias*

(Optional) Lists the metadata details of the certificate and key that are associated with the alias specified.

This option supports an asterisk (*) as a wildcard character. Use the wildcard at the

- Beginning or end of an alias value.
- Beginning and end of an alias value.

Enclose the wildcard in quotes to prevent a command shell from interpreting the wildcard character.

List Revocation Information

Use the listRevocationInfo option to display a list of certificate revocation lists in the certificate data store. The following items are listed:

- The CRL name.
- Whether the CRL is file–based or LDAP–based.
- The CRL location.

Arguments for this option include the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the 12.52 SP1 certificate data store.

-issueralias *issuer_alias*

(Optional) Name of the Certificate Authority who issues the CRL.

This option supports an asterisk (*) as a wildcard character. Use the wildcard at the:

- Beginning or end of an alias value.
- Beginning and end of an alias value.

Enclose the wildcard in quotes to prevent a command shell from interpreting the wildcard character.

Display Certificate Metadata

Use the printCert option to display some metadata for a specified certificate. This command is useful on systems where viewing certificate properties is difficult.

Arguments for this option include the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the 12.52 SP1 certificate data store.

-infile ***cert_file***

Required. Location of the certificate file.

-password ***password***

The password is required only when a password-protected P12 file is specified as the certificate file.

Rename an Alias

Use the renameAlias option to rename an alias that is associated with a certificate.

Arguments for this option include the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the 12.52 SP1 certificate data store.

-alias ***current_alias***

(Required) Specifies the alias that is associated with a certificate.

-newalias ***new_alias***

(Required) Specifies the new alias name.

Limits: Must be a unique string that contains only alphanumeric characters.

Validate a Certificate

Use the validateCert option to determine if a certificate is revoked.

Arguments for this option include the following:

-accessLegacyKS

Specifies that the option applies to the legacy smkeydatabase. If you do not supply this argument, the option applies to the 12.52 SP1 certificate data store.

-alias *alias*

(Required) Specifies the alias to the certificate associated with the private key in the certificate data store

Limits: Must be a unique string that contains only alphanumeric characters.

-infile *crl_file*

(Optional) Specifies the CRL that you want the utility to look in for the certificate to validate it.

Load the the OCSP Configuration File

Use the loadOCSPConfigFile option to reload the OCSP configuration file into the certificate data store without restarting the Policy Server. When the file loads, any existing OCSP configuration is removed from the data store and the configuration is replaced with the contents of the file. The OCSPUpdater picks up the configuration changes the next time that it wakes.

The name of the OCSP configuration file is SMocsp.conf.

The command syntax for Windows is:
```
smkeytool.bat -loadOCSPConfigFile
```

The command syntax for UNIX is:
```
smkeytool.sh -loadOCSPConfigFile
```

smldapsetup

The smldapsetup utility allows you to manage an LDAP policy store from the command line. Using smldapsetup, you can configure an LDAP policy store, generate an LDIF file, and remove policy store data and schema.

To use smldapsetup, specify a mode, which determines the action that smldapsetup will perform, and arguments, which contain the values that are used to configure the LDAP server.

The following table contains the modes you can use with smldapsetup and the arguments each mode uses:

Modes	Arguments
reg	-h*host*, -p*portnumber*, -d*userdn*, -w*userpw*, -r*root*, -ssl*1*|*0*, -c*certdb*, -k1
ldgen	-h*host*, -p*portnumber*, -d*userdn*, -w*userpw*, -r*root*, -m*n*, -ssl*1*|*0*, -c*certdb* -f*ldif*, -t*tool*, -s*suffix*, -e, -k
ldmod	-h*host*, -p*portnumber*, -d*userdn*, -w*userpw*, -r*root*, -ssl*1*|*0*, -c*certdb*, -f*ldif*, -s*suffix*, -e, -k, -i
remove	-h*host*, -p*portnumber*, -d*userdn*, -w*userpw*, -r*root*, -ssl*1*|*0*, -c*certdb*, -k
switch	none
revert	-v
status	-v

To use smldapsetup

1. Navigate to one of the following locations:
   - (Windows) *siteminder_home*\bin
   - (UNIX) *siteminder_home*/bin

   siteminder_home

   Specifies the installed location of CA SiteMinder®.

2. Enter the following command:

   `smldapsetup mode arguments`

   Important! Before running a CA 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.

   Example: smldapsetup reg -hldapserver.mycompany.com -d"LDAP User" -wMyPassword123 -ro=security.com

   Note: When running smldapsetup, make sure that the LDAP user you specify has the appropriate administrator privileges to modify schema in the LDAP Directory Server. If this user does not have the proper privileges, then the LDAP server will not allow you to generate the policy store schema and to update or remove the policy store data. After running the smldapsetup command, this user appears in the Admin Username field on the Data tab of the Policy Server Management Console.

More Information:

Modes for smldapsetup (see page 228)

Modes for smldapsetup

The mode indicates the action that smldapsetup performs. You can specify a mode to connect to the LDAP server, generate an LDIF file, configure an LDAP policy store and remove policy data.

The modes for smldapsetup include:

reg

Tests the connection to the LDAP server. If the connection succeeds, smldapsetup configures the CA SiteMinder® LDAP server as its policy store using the -h*host*, -p*portnumber*, -*duserdn*, -w*userpw*, -r*root*, -ssl*1/0* and -c*certdb* arguments.

ldgen

Automatically detects supported LDAP servers and generates an LDIF file with the CA SiteMinder® schema. The generated file is used by smldapsetup ldmod to create the CA SiteMinder® schema. If the -e argument is specified, smldapsetup ldgen creates an LDIF file that can be used with ldmod to delete the CA SiteMinder® schema. Use the -m switch to skip automatic detection of LDAP servers. The ldgen mode requires the -f switch unless previously configured in reg mode.

ldmod

Connects to the LDAP server and the CA SiteMinder® schema without populating the policy store with any data. It requires the LDAP modify program and the LDIF file, specified with the *-fldif* argument. If you specify the -h*host*, -p*port_number*, -d*userdn*,-w*userpw*, -r*root*, -ssl*1/0* and -c*certdb* arguments, smldapsetup ldmod will modify the LDAP directory specified using these arguments. If you do not specify -h*host*, -p*portnumber*, -d*userdn*, *-wuserpw*, -r*root*, -ssl*1/0* and -c*certdb*, smldapsetup ldmod uses the LDAP directory previously defined using smldapsetup reg or the Policy Server Management Console.

remove

Connects to the LDAP server, then removes all policy data stored under the CA SiteMinder® LDAP node that corresponds to the current version of smldapsetup. If you specify the *-hhost*, -p*ort_number*, -d*userdn*,-w*userpw*, -r*root*, -ssl*1/0* and -c*certdb* arguments, smldapsetup remove will remove policy data from the LDAP directory specified by these arguments. If you do not specify -h*ost*, -p*port*, -d*userdn*, -w*userpw*, -r*root*, *-ssl1/0* and -c*certdb*, smldapsetup remove will remove the policy data from the LDAP directory previously defined using smldapsetup reg or the Policy Server Management Console.

switch

Reconfigures the Policy Server to use LDAP rather than ODBC. It does not prepare the LDAP store or the LDAP connection parameters before making the change.

revert

Reverts to ODBC policy store from LDAP. The only argument used with this mode is -v.

status

Verifies that the LDAP policy store connection parameters are configured correctly. It requires the -v argument. If you specify the -h*host*, -p*ort_number*, -d*userdn*, -w*userpw*, -r*root*, -ssl*1/0* and -c*certdb* arguments, smldapsetup status tests the connection to the LDAP directory specified using these arguments. If you do not specify -h*ost*, -p*ort_number*, *-duserdn*, -w*userpw*, -r*root*, -ssl*1/0* and -c*certdb*, smldapsetup status verifies the connection to the LDAP directory previously defined using smldapsetup reg or the Policy Server Management Console.

From the Data tab in the Policy Server Management Console, you can view or change the settings you configured with the reg, switch and revert functions using a GUI interface. You must use smldapsetup to perform the ldgen, ldmod, remove, and status functions.

Arguments for smldapsetup

Arguments allow you to specify the information used by the modes to manage the LDAP policy store. If you do not specify arguments, smldapsetup uses the values configured in the Policy Server Management Console.

Note: smldapsetup does not allow spaces between an argument and its value. For example, the -h argument should be specified as follows:
smldapsetup ldmod -hldapserver.mycompany.com

The arguments you can specify in an smldapsetup call are listed below:

-h*host*

Specifies the fully qualified name of the LDAP server; the relative name, if the machines are in the same domain (-hldapserver); or the IP address (-h123.12.12.12). If you do not specify a host, smldapsetup uses the previously configured value as the default.

Example: -hldapserver.mycompany.com

-p*port_number*

Specifies a non-standard LDAP port. The LDAP port must be specified if the LDAP server is using a non-standard port or if you are moving a server to a new server that uses a different port, such as moving from a server using SSL to one that is not. If a port is not specified, the previous configuration values are used. If no previous port configuration has been specified, smldapsetup uses the default ports 389, if SSL is not being used, or 636, if SSL is being used.

-d*userdn*

Specifies the LDAP user name of a user with the power to create new LDAP directory schema and entries. This is not necessarily the user name of the LDAP server administrator. If you do not specify a user name, smldapsetup uses the previously configured name as the default.

-w*userpw*

Specifies the password for the user identified in the -d argument. If you do not specify a password, smldapsetup uses the previously configuration value.

Example: -wMyPassword123

-r*root*

Specifies the distinguished name of the node in the LDAP tree where CA SiteMinder® will search for the policy store schema. If you do not specify a root, smldapsetup uses the previously configured root.

Example: -ro=security.com

-e

When specified with smldapsetup ldgen, generates an LDIF file that can delete the CA SiteMinder® schema. The generated file must be used with smldapsetup ldmod to remove the schema.

-m*n*

Skips automatic detection of LDAP servers and specify type of LDAP policy store where *n* is one of the following:

2

iPlanet v4 LDAP servers.

3

Active Directory LDAP servers.

4

Oracle Internet Directory.

5

iPlanet v5.

6

Sun Directory Servers.

9

Active Directory Application Mode (ADAM).

-f*ldif*

Specifies the absolute or relative path to an LDIF file from the directory in which smldapsetup is being executed.

Example: -f../siteminder/db/smldap.ldif

Default: if you do not specify a path, smldapsetup uses the current directory as the default.

-t*tool*

Specifies the absolute or relative path, including filename and extension, of the ldapmodify command line utility. Ldapmodify is used to configure the server schema using the LDIF format commands. LDAP servers and CA SiteMinder® provide a copy of ldapmodify. If the utility is not in the default location, use this argument to specify its location.

-ssl*1_or_0*

Specify -ssl1 to use an SSL-encrypted connection to the LDAP server, and -ssl0 to use a non-SSL connection. If you do not specify a value for -ssl, smldapsetup uses the previously configured value. If the LDAP connection has not been configured before, the initial default value is 0.

-c*cert*

This argument must be specified when using an SSL encrypted (-ssl1) LDAP connection. Specifies the path of the directory where the SSL client Netscape certificate database file, which is usually called cert8.db, exists.

Example: If cert8.db exists in /app/siteminder/ssl, specify -c/app /siteminder/ssl when running smldapsetup ldmod -f/app/siteminder/pstore.ldif -p81 -ssl1 -c/app/siteminder/ssl.

Note: For policy stores using an SSL-encrypted connection to Sun Java System LDAP, make sure the key3.db file exists in the same directory as cert8.db.

-k-k1

Enables you to use smldapsetup to set up or modify a key store if you are storing key information in a different LDAP directory. If you specify -k, smldapsetup checks to see if the Policy Server is pointing to the key store before performing any functions. If the Policy Server is not pointing to the key store, smldapsetup issues a warning. If you specify -k1, in conjunction with smldapsetup ldgen and the other arguments for a new policy store, smldapsetup creates a separate key store in the location you specify. If you do not specify -k or -k1, smldapsetup will modify the policy store.

-v

Enables verbose mode for troubleshooting. With -v, smldapsetup logs its command-line arguments and configuration entries as it performs each step in the LDAP migration.

-i*userDN*

Specifies the distinguished name of an account that should be used by CA SiteMinder® to make modifications to the policy store. This argument allows an administrator account to retain control of the CA SiteMinder® schema while enabling another account that will be used for day-to-day modifications of CA SiteMinder® data. When a change is made using the Administrative UI, the account specified by this argument is used. Be sure to enter the entire DN of an account when using this argument.

-q

Enables quiet mode for no questions to be asked.

-u

Creates a 6.x upgrade schema file (LDIF).

-x

Use the -x argument with ldmod to generate replication indexes for another 5.x Sun Java System Directory Server Enterprise Edition (formerly Sun ONE/iPlanet) LDAP directory server.

-ssuffix

This option allows you to specify a suffix other than the default parent suffix when configuring the 6.x Policy Server's schema in a Sun Java System Directory Server Enterprise Edition (formerly Sun ONE/iPlanet) LDAP directory server.

Example: assume the following:

ou=Apps,o=test.com is the Policy Store root.

o=test.com is the root suffix.

ou=netegrity,ou=Apps,o=test.com is the sub suffix.

If you do not use the -s parameter with smldapsetup, the Policy Server assigns ou=Apps,o=test.com as a parent suffix of ou=netegrity,ou=Apps,o=test.com. To change this and have the appropriate parent suffix set, run smldapsetup using the -s parameter while specifying o=test.com.

-?

Displays the help message.

Note: If the arguments contain spaces, you must enter double quotes around the entire argument. For example, if the name of the CA SiteMinder® administrator is LDAP user, the argument for smldapsetup would be: -d”LDAP user".

smldapsetup and Sun Java System Directory Server Enterprise Edition

In a Sun Java System Directory Server Enterprise Edition (formerly Sun ONE/iPlanet) directory server, smldapsetup creates the ou=Netegrity, *root* sub suffix and PolicySvr4 database.

root

The directory root you specified in the Root DN field on the Data tab of the Policy Server Management Console. This variable has to be either an existing root suffix or sub suffix.

Example: If your root suffix is dc=netegrity,dc=com then running smldapsetup produces the following in the directory server:

- A root suffix, dc=netegrity,dc=com, with the corresponding userRoot database.
- A sub suffix, ou=Netegrity,dc=netegrity,dc=com, with the corresponding PolicySvr4 database.

Example: If you want to place the policy store under ou=apps,dc=netegrity,dc=com, then ou=apps,dc=netegrity,dc=com has to be either a root or sub suffix of the root suffix dc=netegrity,dc=com.

If it is a sub suffix, then running smldapsetup produces the following:

- A root suffix, dc=netegrity,dc=com, with the corresponding userRoot database.
- A sub suffix, ou=apps,dc=netegrity,dc=com, with the corresponding Apps database.
- A sub suffix, ou=Netegrity,ou=apps,dc=netegrity,dc=com, with the corresponding PolicySvr4 database.

Note: For more information about root and sub suffixes, see the Sun Microsystems documentation.

Remove the SiteMinder Policy Store using smldapsetup

To remove the CA SiteMinder® policy store data and schema from an LDAP directory, you must first delete the data, then remove the schema.

Important!

- Before removing the CA SiteMinder® policy store data, be sure that the Policy Server is pointing to the policy store that contains the data you want to delete. smldapsetup will remove the data from the policy store to which the Policy Server is pointing. Additionally, export the policy store data to an output file and create a backup of the file before removing the data.
- If you are running a CA SiteMinder® utility or executable on Windows Server 2008, be sure to open the command–line window with Administrator permissions, even if you are logged into the system as an Administrator. For more information, see the release notes for your CA SiteMinder® component.

To remove the policy store using smldapsetup

1. Navigate to the following location:
   - (Windows) *siteminder_home*\bin
   - (UNIX) *siteminder_home*/bin

   siteminder_home

   Specifies the installed location of CA SiteMinder®.
2. Remove the policy store data by entering the following command:

   ```
   smldapsetup remove -hLDAP_IP_Address -pLDAP_Port
   -d LDAP_Admin -wLDAP_Admin_Password -rLDAP_Base_DN
   -v
   ```

   Example: smldapsetup remove -h192.169.125.32 -p552 -d"cn=directory manager" -wfirewall -rdc=ad,dc=test,dc=com -v

   Note: Removing the policy store data may take a few moments.

3. Generate the LDIF file you will use to delete the schema by entering the following:

   `smldapsetup ldgen -e -f`*`ldif`*

   ldif

   Specifies the name of the LDIF file you are generating.

   Example: smldapsetup ldgen -e -fdelete.ldif

4. Remove the CA SiteMinder® schema by executing the following command:

   `smldapsetup ldmod -f`*`ldif`*

   ldif

   Specifies the name of the LDIF file you generated using smldapsetup ldgen -e.

   Example: smldapsetup ldmod -fdelete.ldif

Delete SiteMinder Data in ODBC Databases

CA SiteMinder® provides SQL scripts that delete the CA SiteMinder® schema from ODBC databases. The following list describes each SQL script:

sm_oracle_ps_delete.sql

Removes the CA SiteMinder® policy store and data from an Oracle database.

sm_oracle_logs_delete.sql

If the database was created using sm_oracle_logs.sql, removes CA SiteMinder® logs stored in an Oracle database

sm_oracle_ss_delete.sql

Removes the CA SiteMinder® session store tables and data from an Oracle database.

sm_mssql_ps_delete.sql

Removes the CA SiteMinder® policy store and data from an SQL database.

sm_mssql_logs_delete.sql

If the database was created using sm_mssql_logs.sql, removes CA SiteMinder® logs stored in an SQL database

sm_mssql_ss_delete.sql

Removes the CA SiteMinder® session store tables and data from a SQL database.

sm_db2_ps_delete.sql

Removes the CA SiteMinder® policy store and data from a DB2 database.

sm_db2_logs_delete.sql

If the database was created using sm_db2_logs.sql, removes CA SiteMinder® logs stored in a DB2 database

sm_db2_ss_delete.sql

Removes the CA SiteMinder® session store tables and data from a DB2 database.

The ODBC database SQL scripts are in the following location:

- (Windows) *siteminder_home*\db

  siteminder_home

  Specifies the Policy Server installation path.

- (UNIX) *siteminder_home*/db

  siteminder_home

  Specifies the Policy Server installation path.

Delete the database objects by running the appropriate SQL script using DB2, SQL Plus for Oracle, or SQL Server Query Analyzer.

Note: For more information about running SQL scripts, see your database documentation.

smpatchcheck

The smpatchcheck tool lets you determine whether you have the Solaris patches required for the Policy Server and Web Agent installed on your system. Smpatchcheck can be run on the Solaris versions listed on the CA SiteMinder® Platform Matrix. To access this matrix, go to Technical Support and search for the CA SiteMinder® Platform Support Matrix.

To use smpatchcheck

1. Navigate to *siteminder_home*/bin

   siteminder_home

   Specifies the Policy Server installation path.

2. Enter smpatchcheck.

   Smpatchcheck looks for each required/recommended patch and then displays its status.

   For example:

```
Testing for Required Patches:
  Testing for Patch: 106327-09 ... NOT Installed
Testing for Recommended Patches:
  Testing for Patch: 106541-08 ... Installed
  Testing for Patch: 106980-00 ... Installed
SiteMinder Patch Check: Failed
```

Smpatchcheck returns one of the following messages:

Failed

One or more of the required patches is not installed.

Partially Failed

One or more of the recommended patches is not installed.

Success

All of the required and recommended patches are installed.

SiteMinder Test Tool

The CA SiteMinder® Test Tool is a utility that simulates the interaction between Agents and Policy Servers. It tests the functionality of the Policy Server. During testing, the Test Tool acts as the Agent, making the same requests to the Policy Server as a real Agent. This allows you to test your CA SiteMinder® configuration before deploying it.

Note: For further information about this tool, see the *Policy Server Configuration Guide*.

smreg

To change the super user password

1. Be sure that the Policy Server is running and pointed at a configured policy store.
2. Be sure that the smreg utility is located in *policy_server_home*\bin.

   policy_server_home

   Specifies the Policy Server installation path.

   Note: If the utility is not present, you can find it in the Policy Server installation media available on the Support site.

3. Run the following command:

   `smreg -su password`

   password

   Specifies the password for the CA SiteMinder® super user account.

   Note: Be sure that there is a space between -su and the password.

   The utility changes the super user account password.

4. Delete the smreg utility.

   Deleting the utility prevents anyone from changing the super user password.

XPSCounter

To comply with the terms of your CA SiteMinder® license, you can count the number of users in your CA SiteMinder® environment. The following process describes how to configure your directories and count the CA SiteMinder® users stored within them:

1. Make the following changes to each user directory you want to count:

   Note: For more information, see the *CA SiteMinder® Policy Server Configuration Guide*.

   - Require the use of Administrator Credentials by entering the user name and password of the directory administrator in the Administrative UI.
   - Define a Universal ID and other user attribute mappings using the Administrative UI.

2. For Microsoft Active Directory user stores, map the inetOrgPerson attribute using the Administrative UI.
3. Determine the number of users associated with CA SiteMinder® policies.

Map the Active Directory inetOrgPerson Attribute

If your CA SiteMinder® user stores are on Microsoft Active Directory servers, map the inetOrgPerson in each server before counting the CA SiteMinder® users.

Follow these steps:

1. Log in to the Administrative UI.
2. Click Infrastructure, Directory.
3. Click User Directories.
4. Search for the user directory you want and click the directory name.
5. Click Modify.

6. Click Create in the Attribute Mapping List section.
7. Select the option to create an object and click OK.
8. Type the following name:

   inetOrgPerson
9. Type the following description:

   Custom Mapping to Count Active Directory Users (with XPSCounter)
10. Do the following in the Properties section:
    a. Be sure that the Alias option is selected.
    b. Type the following definition:

       User
11. Click OK.
12. Click Submit.

    The inetOrgPerson attribute is mapped.

Determine the Number of Users Associated with CA SiteMinder® Policies

To comply with the CA SiteMinder® licensing terms, you can determine how many users in your organization are associated with CA SiteMinder® policies.

Note: If you do *not* have write access to the CA SiteMinder® binary files (XPS.dll, libXPS.so, libXPS.sl), an Administrator must grant you permission to use the related XPS command line tools using the Administrative UI or the XPSSecurity tool.

To determine the number of users

1. Open a command window on the Policy Server, and then enter the following command:

   ```
   XPSCounter
   ```

   The tool starts and displays the name of the log file for this session, and the License Parameters menu opens.
2. Enter 1.

   The Parameter menu appears.
3. Enter C.

   The Counter menu appears.
4. Enter I.
5. Enter ? to search for a user directory XID. Only those user directories that are defined in your policy store appear in the list.

6. Enter the number of the directory that contains the users you want to count.

   Note: This tool counts the number of user objects in each directory that you specify. It does not account for the same user object being listed in multiple directories or multiple user objects for the same user in a directory. You must consider this when interpreting the results provided by this tool.

7. (Optional) Enter a comment to describe the results.

   The users are counted and a confirmation message appears.

8. (Optional) Repeat Steps 5 through 8 to count the users in another directory.

9. Enter V.

   The following information appears for *each* directory counted:

   XID

   Displays the unique identifier for the specified user directory.

   Example: CA.SM::UserDirectory@0e-50ea30f0-b5c0-450c-a135-1e317dd25f11

   Name

   Displays the name of the specified user directory (as defined in the Administrative UI).

   : *count*

   Displays the most-recent user count of the specified user directory. You do *not* have to delete any previous values stored in the counter because this value is updated automatically every time the counter is run.

   Example: : 23

   Total

   Displays the total of number of users from all of the user directories you counted. For example, if you counted number of users for two different directories, and each directory has 23 users, the total shown will be 46.

XPSConfig

XPSConfig is an interactive command-line utility that allows administrators and members of operations to view product parameters and, if allowed, edit their settings. While you may have your own product-specific configuration tool using XPS programming interfaces, XPSConfig is available so that this is not a requirement.

For each vendor and installed product, XPSConfig manages the parameters or named settings that are defined in the product's Data Dictionary. Each product can read, write, and validate its own parameter settings.

To use XPSConfig, you must be an administrator with XPSConfig rights.

Parameters have the following attributes:

Name

Specifies the name of the parameter.

Limits:

- Names must start with a letter or underscore and contain only letters, numbers, and underscores.
- Names can be up to 32 characters in length.
- Names are not case-sensitive.

Type

Specifies the data type of the parameter value:

`Logical | Numeric | String`

Logical

Specifies a Boolean value: TRUE or FALSE.

Numeric

Specifies an integer.

String

Specifies a string of characters.

Scope

Specifies the value or scope of the parameter:

`Ask | Global | Local | Managed | Overrideable | Read Only`

Ask

Specifies that the value is managed by the product, not by XPS, and that the value is read only.

Global

Specifies that the value is stored in the policy store and accessible by all Policy Servers sharing that policy store.

Local

Specifies that each Policy Server stores its own value.

Managed

Specifies that the value is managed by the product, not by XPS, and that the value is read-write.

Overrideable

Specifies that a value stored locally on a Policy Server can override a value stored globally on a shared policy store.

Read Only

Specifies that the value is both the default value and read only.

Export

Specifies whether the parameter is included in exports of the policy store.

Type: Boolean

Report

Specifies whether the parameter is included in capabilities reporting for the Policy Server.

Type: Boolean

RemoteAccess

Specifies what type of access the remote API has to the parameter:

```
None | Read | ReadWrite
```

Description

Describes the purpose of the parameter.

LicenseType

Specifies the type of license limit:

```
None | SoftLimit | HardLimit | ExpDate
```

None

Specifies that the parameter is not a license limit.

SoftLimit

Specifies that the parameter is a soft or advisory license limit.

HardLimit

Specifies that the parameter is a hard or absolute license limit.

ExpDate

Specifies that the parameter is the date on which the license expires.

Default Value

Specifies a default value for use when the current value is undefined.

Note: If the default value is undefined, its value is specified according to its data type:

String

space

Number

zero

Boolean

FALSE

Visible

Specifies whether the parameter is visible to XPSConfig.

Type: Boolean

Syntax

XPSConfig has the following format:

```
XPSConfig [-vendor vendor] [-product product]
[-?] [-vT | -vI | -vW | -vE | -vF]
[-l log_path] [-e err_path] [-r rec_path]
```

Parameters

XPSConfig includes the following options:

-vendor

(Optional) Specifies the name of the vendor whose data you want to view.

-product

(Optional) Specifies the name of the product whose data you want to view.

-?

(Optional) Displays help information for this utility.

-vT | -vI | -vW | -vE | -vF

(Optional) Specifies when to log error information to the error file and how much information to log.

-vT

Logs detailed information so that you can TRACE errors.

-vI

Logs information in case there is an error.

-vW

Logs error information in the event of a WARNING, ERROR, or FATAL error.

-vE

Logs error information in the event of an ERROR or FATAL error.

-vF

Logs error information in the event of a FATAL error.

-l

(Optional) Outputs logging information to the specified location.

Default: stdout

-e

(Optional) Outputs error information to the specified location.

Default: stderr

-r

(Optional) Outputs a record of the session to the specified location.

XPSEvaluate

XPSEvaluate is an interactive command-line utility that allows administrators and application developers to evaluate expressions and test performance. To use XPSEvaluate, you must be an administrator with XPSEvaluate rights.

Syntax

XPSEvaluate has the following format:

```
XPSEvaluate [-np] [-trace] [-dbg debuglist]
[-f DB | formulapath] [-c contextpath] [-u userpath] [-step]
[-?] [-vT | -vI | -vW | -vE | -vF]
[-l log_path] [-e err_path] [-r rec_path]
```

Parameters

XPSEvaluate includes the following options:

-np

(Optional) Specifies no prompt.

-trace

(Optional) Turns on tracing.

-dbg

(Optional) Specifies the debug list.

-f

(Optional) Specifies the location of the named expressions.

Note: DB specifies the policy store.

-c

(Optional) Specifies the location of the context values.

-u

(Optional) Specifies the location of the user attributes.

-step

(Optional) Shows evaluation steps.

-?

(Optional) Displays help information for this utility.

-vT | -vI | -vW | -vE | -vF

(Optional) Specifies when to log error information to the error file and how much information to log.

-vT

Logs detailed information so that you can TRACE errors.

-vI

Logs information in case there is an error.

-vW

Logs error information in the event of a WARNING, ERROR, or FATAL error.

-vE

Logs error information in the event of an ERROR or FATAL error.

-vF

Logs error information in the event of a FATAL error.

-l

(Optional) Outputs logging information to the specified location.

Default: stdout

-e

(Optional) Outputs error information to the specified location.

Default: stderr

-r

(Optional) Outputs a record of the session to the specified location.

XPSExplorer

XPSExplorer is an interactive command-line utility that allows an administrator or application developer to view the data in a policy store. XPSExplorer has two uses:

- To determine the identifiers of objects for a granular export or import by exploring a list of domains or realms
- To repair the object store in the event that the store is damaged and must be repaired manually. This action should be performed only under the guidance of CA support.

To use XPSExplorer, you must be an administrator with XPSExplorer rights.

Syntax

XPSExplorer has the following format:

```
XPSExplorer [-?] [-vT | -vI | -vW | -vE | -vF]
[-l log_path] [-e err_path] [-r rec_path]
```

Parameters

XPSExplorer includes the following options:

-?

(Optional) Displays help information for this utility.

-vT | -vI | -vW | -vE | -vF

(Optional) Specifies when to log error information to the error file and how much information to log.

-vT

Logs detailed information so that you can TRACE errors.

-vI

Logs information in case there is an error.

-vW

Logs error information in the event of a WARNING, ERROR, or FATAL error.

-vE

Logs error information in the event of an ERROR or FATAL error.

-vF

Logs error information in the event of a FATAL error.

-l

(Optional) Outputs logging information to the specified location.

Default: stdout

-e

(Optional) Outputs error information to the specified location.

Default: stderr

-r

(Optional) Outputs a record of the session to the specified location.

Export a Subset of Policy Store Data

To export a subset of policy store data, you need the identifiers of the objects (XIDs) that you want to export. You can use XPSExplorer to locate object identifiers. To use XPSExplorer, you must be an administrator with XPSExplorer rights.

In this use case, you export the following accounting applications:

- Accounts Payable
- Accounts Receivable
- General Ledger
- Payroll

Export a subset of policy store data

1. Open a command prompt on the machine hosting the Policy Server.
2. Enter the following command:

   ```
   XPSExplorer
   ```

   The main menu opens and lists vendors, products, and classes.

   Note: Only objects in top-level classes can be exported. Top-level classes are marked with asterisks.
3. Enter the number corresponding to the class of objects that you want to export.

   The Class Menu opens.

   Example: If the number 15 corresponds to accounting, enter 15.
4. Enter S to view the objects in the class.

   The Search Menu opens and the objects in the class are listed.

   Example Search Results:

   1-CA.SM::Accounting@0e-08c6cadb-e30b-4e06-9e2e-b3d7a866fab8

   (I) Name : "Accounts Payable"

   (C) Desc : "accounts payable"

   2-CA.SM::Accounting@0e-3b0f4ccf-71f3-4968-b095-2b5a830c3244

   (I) Name : "Accounts Receivable"

   (C) Desc : "accounts receivable"

   3-CA.SM::Accounting@03-1c7ac22e-6646-4c61-8f2f-6261a0ef3a92

   (I) Name : "General Ledger"

   (C) Desc : "general ledger"

   4-CA.SM::Accounting@10-8d78bb81-ae15-11d1-9cdd-006008aac24b

   (I) Name : "Payroll"

   (C) Desc : "payroll"

   5-CA.SM::Accounting@@12-88f119a0-3fd1-46d0-b8ac-c1e83f00f97d

   (I) Name : "Job Costing"

   (C) Desc : "job costing"

   Example Object Identifiers (XIDs):

   CA.SM::Accounting@0e-08c6cadb-e30b-4e06-9e2e-b3d7a866fab8

   CA.SM::Accounting@0e-3b0f4ccf-71f3-4968-b095-2b5a830c3244

   CA.SM::Accounting@03-1c7ac22e-6646-4c61-8f2f-6261a0ef3a92

CA.SM::Accounting@10-8d78bb81-ae15-11d1-9cdd-006008aac24b

CA.SM::Accounting@@12-88f119a0-3fd1-46d0-b8ac-c1e83f00f97d

5. Enter Q three times to exit the Search, Class, and Main Menus and return to the command prompt.

6. Enter the following command at the command prompt:

```
XPSExport output_file -xo object_XID_1 -xo object_XID_2
-xo object_XID_3 -xo object_XID_4
```

output_file

Specifies the XML file to which the policy store data is exported.

-xo *object_XID*

Specifies the identifier of each object that you want to export.

Note: You can copy the object identifiers (XIDs) from the Search results and paste them in the command line.

Example:

```
XPSExport accounting.xml
-xo CA.SM::Accounting@0e-08c6cadb-e30b-4e06-9e2e-b3d7a866fab8
-xo CA.SM::Accounting@0e-3b0f4ccf-71f3-4968-b095-2b5a830c3244
-xo CA.SM::Accounting@03-1c7ac22e-6646-4c61-8f2f-6261a0ef3a92
-xo CA.SM::Accounting@10-8d78bb81-ae15-11d1-9cdd-006008aac24b
```

The policy store data for the specified accounting applications is exported to accounting.xml.

XCart Management

XPSExplorer includes the XCart feature. XCart allows you to collect the identifiers of the objects (XIDs) that you want to export and save them to a file for later use without manually copying and pasting each one. To use XPSExplorer, you must be an administrator with XPSExplorer rights.

To access XCart, enter X for XCart Management in the Main Menu of XPSExplorer. The XCart Menu opens and displays any objects that are in the XCart. The following options are context-sensitive and may or may not be displayed depending on the context:

C - Clear cart.

Empties the XCart.

L - Load cart from file.

- Initial load - Loads the XCart with the contents of the specified file and remembers the specified file name as the XCart file.
- Subsequent loads - Adds the contents of the specified file to the XCart.

  Note: The name of the XCart file does not change.

S - Save cart to file: xcart_file

Saves the contents of the XCart to the XCart file.

Important! The S command overwrites the contents of the XCart file without prompting first.

N - Save cart to new file.

Saves the contents of the XCart to the specified file and remembers the specified file name as the XCart file.

Note: The N Command prompts before overwriting the specified file.

Each object is tagged with an import mode that determines how it will be imported from the XPS file to the policy store:

A - Set import mode to ADD.

Adds new objects; does not replace existing objects.

O - Set import mode to OVERLAY.

Replaces existing objects; does not add new objects.

R - Set import mode to REPLACE.

Replaces existing objects and adds new objects.

D - Set import mode to default.

Specifies the default import mode.

Note: For each product class, there is a default import mode defined in the product's data dictionary.

Q - Quit

Exits the XCart Menu and returns to the Main Menu.

Export a Subset of Policy Store Data Using XCart

To export a subset of policy store data, you need the identifiers of the objects (XIDs) that you want to export. You can use the XCart feature of XPSExplorer to locate objects and save them in an XCart file for later use when you export. For example, an administrator can set up an XCart file for members of operations to use as needed. To use XPSExplorer, you must be an administrator with XPSExplorer rights.

In this use case, you save the following four accounting applications in a file for later use:

- Accounts Payable
- Accounts Receivable
- General Ledger
- Payroll

Export a subset of policy store data using XCart

1. Open a command prompt on the machine hosting the Policy Server.
2. Enter the following command:

   ```
   XPSExplorer
   ```

   The Main Menu opens and lists vendors, products, and classes.

   Note: Only objects in top-level classes can be exported. Top-level classes are marked with asterisks.
3. Enter X for XCart Management.

   The XCart Menu opens.
4. Create a text file.

   Example: C:\xcart\accounting.txt

   Note: This is where you want the contents of the XCart to be saved.
5. Enter L for Load cart from file.
6. Enter the path and name of the text file you created.

   The specified file name is remembered as the XCart file.

   Example: C:\xcart\accounting.txt

   Note: The file must exist. If not, L has no effect.
7. Enter Q to return to the Main Menu.
8. Enter the number corresponding to the class that you want to export.

   The Class Menu opens.

   Example: If the number 15 corresponds to Accounting, enter 15.
9. Enter S to view the objects in the class.

   The Search Menu opens and the objects in the class are listed.

   Example Search Results:

   1-CA.SM::Accounting@0e-08c6cadb-e30b-4e06-9e2e-b3d7a866fab8

   (I) Name : "Accounts Payable"

   (C) Desc : "accounts payable"

2-CA.SM::Accounting@0e-3b0f4ccf-71f3-4968-b095-2b5a830c3244

(I) Name : "Accounts Receivable"

(C) Desc : "accounts receivable"

3-CA.SM::Accounting@03-1c7ac22e-6646-4c61-8f2f-6261a0ef3a92

(I) Name : "General Ledger"

(C) Desc : "general ledger"

4-CA.SM::Accounting@10-8d78bb81-ae15-11d1-9cdd-006008aac24b

(I) Name : "Payroll"

(C) Desc : "payroll"

5-CA.SM::Accounting@@12-88f119a0-3fd1-46d0-b8ac-c1e83f00f97d

(I) Name : "Job Costing"

(C) Desc : "job costing"

10. For Accounting applications one through four:
    a. Enter the number corresponding to the application.
    b. Enter X for Add to XCart.
    c. Enter Q to exit the XCart Menu and return to the Search Menu.

    Note: An asterisk before an application indicates that it is in the XCart.
11. Enter Q twice to exit the Search and Class Menus and return to the Main Menu.
12. Enter X for XCart Management.
13. Enter S to Save the cart to the XCart file: C:\xcart\accounting.txt.
14. Enter Q twice to exit the XCart and Main Menus and return to the command prompt.
15. Enter the following command at the command prompt:

    `XPSExport output_file -xf xcart_file`

    output_file

    Specifies the XML file to which the policy store data is exported.

    -xf *xcart_file*

    Specifies the path and name of the XCart file containing the identifiers of the objects (XIDs) to export.

    Example:

    ```
    XPSExport accounting.xml C:\xcart\accounting.txt
    ```

    The policy store data for the accounting applications saved in the XCart file is exported to accounting.xml.

Add an Application to an XCart File

In this use case, you add a fifth accounting application, Job Costing, to the following four accounting applications already in the XCart file, accounting.txt, using the XCart feature of XPSExplorer:

- Accounts Payable
- Accounts Receivable
- General Ledger
- Payroll

Note: To use XPSExplorer, you must be an administrator with XPSExplorer rights.

Add an application to an XCart file

1. Open a command prompt on the machine hosting the Policy Server.
2. Enter the following command:

   `XPSExplorer`

   The Main Menu opens and lists vendors, products, and classes.

   Note: Only objects in top-level classes can be exported. Top-level classes are marked with asterisks.
3. Enter X for XCart Management.

   The XCart Menu opens.
4. Enter L for Load cart from file.
5. Enter the path and name of the existing text file containing the four accounting applications.

   The specified file name is remembered as the XCart file.

   Example: C:\xcart\accounting.txt
6. Enter Q to return to the Main Menu.
7. Enter the number corresponding to the class that you want added to the XCart file.

   The Class Menu opens.

   Example: If the number 15 corresponds to accounting, enter 15.
8. Enter S to view the objects in the class.

   The Search Menu opens and the objects in the class are listed.

   Example Search Results:

   1-CA.SM::Accounting@0e-08c6cadb-e30b-4e06-9e2e-b3d7a866fab8

   (I) Name : "Accounts Payable"

   (C) Desc : "accounts payable"

2-CA.SM::Accounting@0e-3b0f4ccf-71f3-4968-b095-2b5a830c3244

(I) Name : "Accounts Receivable"

(C) Desc : "accounts receivable"

3-CA.SM::Accounting@03-1c7ac22e-6646-4c61-8f2f-6261a0ef3a92

(I) Name : "General Ledger"

(C) Desc : "general ledger"

4-CA.SM::Accounting@10-8d78bb81-ae15-11d1-9cdd-006008aac24b

(I) Name : "Payroll"

(C) Desc : "payroll"

5-CA.SM::Accounting@@12-88f119a0-3fd1-46d0-b8ac-c1e83f00f97d

(I) Name : "Job Costing"

(C) Desc : "job costing"

Note: An asterisk before an application indicates that it is in the XCart.

9. To add Job Costing to the XCart file:
   a. Enter 5 for the Job Costing application.
   b. Enter X for Add to XCart.
   c. Enter Q to exit the XCart menu and return to the Search Menu.

      The asterisk before the application indicates that it is in the XCart.
   d. Enter Q twice to exit the Search and Class Menus and return to the Main Menu.
   e. Enter X for XCart Management.
   f. Enter S to Save the XCart to the XCart file: C:\xcart\accounting.txt.

      Job Costing is added to accounting.txt.
10. Enter Q twice to exit the XCart and Main Menus and return to the command prompt.

XPSSecurity

XPSSecurity is an interactive command-line utility that allows administrators and members of operations to create and delete administrators and edit their rights. To use XPSSecurity, you must be an administrator with XPSSecurity rights.

Syntax

XPSSecurity has the following format:

```
XPSSecurity [-?] [-vT | -vI | -vW | -vE | -vF]
[-l log_path] [-e err_path] [-r rec_path]
```

Parameters

XPSSecurity includes the following options:

-?

(Optional) Displays help information for this utility.

-vT | -vI | -vW | -vE | -vF

(Optional) Specifies when to log error information to the error file and how much information to log.

-vT

Logs detailed information so that you can TRACE errors.

-vI

Logs information in case there is an error.

-vW

Logs error information in the event of a WARNING, ERROR, or FATAL error.

-vE

Logs error information in the event of an ERROR or FATAL error.

-vF

Logs error information in the event of a FATAL error.

-l

(Optional) Outputs logging information to the specified location.

Default: stdout

-e

(Optional) Outputs error information to the specified location.

Default: stderr

-r

(Optional) Outputs a record of the session to the specified location.

Make an Administrator a Super User

A super user is defined when the connection to the external administrator store is configured. The super user is used to create and manage all other administrator accounts. If the super user is unavailable, use XPSSecurity to make any user in the external store a super user.

To make an administrator a super user

1. Log into the Policy Server host system with a CA SiteMinder® administrator account that has XPSSecurity rights.

   Note: If an administrator with XPSSecurity rights is not available, you can log in as one the following:

   - (Windows) the system administrator
   - (UNIX) root
   - the user who installed the Policy Server

2. Be sure that the XPSSecurity utility is located in *policy_server_home*/bin.

   policy_server_home

   Specifies the Policy Server installation path.

   Note: If the utility is not present, you can find it in the Policy Server installation media available on the Support site.

3. Open a command window and run the following command:

   ```
   XPSSecurity
   ```

   The main menu appears.

4. Type A and press Enter.

   The administrator menu lists the CA SiteMinder® administrators in the external store. Each administrator is prefixed with a number.

5. Type the number of the administrator and press Enter.

   The administrator menu displays attributes specific to the administrator you chose. Each attribute is prefixed with a number.

6. Type 2 and press Enter.

   The administrator menu updates with flag settings.

7. Type a question mark (?) and press Enter.

   The Disabled and Super User flags appear. Each flag is prefixed with a number.

8. Type 2 and press Enter.

   The Super User flag is selected.

9. Type Q and press Enter.

   The administrator menu displays attributes specific to the administrator. The Flags attribute is set to Super User.

10. Type U and press Enter.

    The administrator record is updated.

11. Type Q and press Enter.

    The administrator menu lists the CA SiteMinder® administrators in the external store. The administrator you chose appears as a super user.

12. Type Q and press Enter for the next two prompts to exit the utility.

    The administrator you chose is a super user. Use this administrator to restore modified or deleted permissions.

-XPSSweeper

XPSSweeper is a command-line utility that can also be run as a batch job. You can use XPSSweeper to synchronize XPS and SiteMinder policy stores. Usually, XPS synchronizes the different policy stores. However, when legacy tools are used, the policy stores may need to be resynchronized using XPSSweeper. In any case, XPSSweeper does not harm the policy stores and can be run as a precaution.

Syntax

XPSSweeper has the following format:

```
XPSSweeper [-f] [-s seconds] [-m entries]
[-?] [-vT | -vI | -vW | -vE | -vF]
[-l log_path] [-e err_path]
```

Parameters

XPSSweeper includes the following options:

-f

(Optional) Runs XPSSweeper in a loop forever.

Note: Use Control-C to exit.

-s

(Optional) Sleeps for the specified number of seconds between iterations of XPSSweeper.

-m

(Optional) Outputs a milestone message every time the specified number of entries has been logged.

-?

(Optional) Displays help information for this utility.

-vT | -vI | -vW | -vE | -vF

(Optional) Specifies when to log error information to the error file and how much information to log.

-vT

Logs detailed information so that you can TRACE errors.

-vI

Logs INFOrmation in case there is an error.

-vW

Logs error information in the event of a WARNING, ERROR, or FATAL error.

-vE

Logs error information in the event of an ERROR or FATAL error.

-vF

Logs error information in the event of a FATAL error.

-l

(Optional) Outputs logging information to the specified location.

Default: stdout

-e

(Optional) Outputs error information to the specified location.

Default: stderr

Run XPSSweeper as a Batch Job

You can run XPSSweeper as a batch job by setting the following two XPS configuration parameters using XPSConfig:

CA.XPS::$Autosweep

Specifies whether to run XPSweeper according to the Autosweep schedule or not to run XPSSweeper at all.

Type: Boolean

CA.XPS::$AutosweepSchedule

Specifies the Autosweep schedule in GMT using the following format:

```
DDD@{HH:MM}[,DDD@{HH:MM}] ... [,DDD@{HH:MM}]
```

DDD

(Optional) Specifies the day of the week:

```
Sun | Mon | Tue | Wed | Thu | Fri | Sat
```

HH

Specifies the hour.

Range: 00-23

MM

Specifies the number of minutes past the hour.

Range: 00-59

Examples:

Sun@08:30

Every Sunday at 8:30am GMT

Tue@14:00

Every Tuesday at 2:00pm GMT

15:15

Everyday at 3:15pm GMT

Sun@08:30,Tue@14:00,15:15

Every Sunday at 8:30am, every Tuesday at 2:00pm, and everyday at 3:15pm except Tuesday

Note: Multiple Autosweep times can be separated by commas, spaces, or semicolons.

Policy Servers manage XPSSweeper Autosweep times as follows:

- XPSSweeper may run a few minutes off schedule because the cache check frequency is every several minutes.
- If XPSSweeper is already running when it is scheduled to run, it is not stopped and restarted, but allowed to finish the sweep process.
- XPSSweeper is not run more frequently than every two hours, even when scheduled.

  Example: If XPSSweeper is scheduled to run at 2:00pm on Tuesday and daily at 3:15pm, the latter sweep is not run on Tuesdays.

Configure Autosweep to Run Every 24 Hours Using XPSConfig

We recommend configuring the XPSSweeper utility to run once every 24 hours. If the XPSSweeper utility does *not* run often enough, the Policy Server could have trouble starting. Too many tombstone objects in the policy store produce the following error:

```
LDAP_SIZELIMIT_EXCEEDED
```

Setting the XPSSweeper utility to run automatically uses the following XPS configuration parameters:

- CA.XPS::$Autosweep
- CA.XPS::$AutosweepSchedule

Follow these steps:

1. Open a command-line window on the computer hosting the Policy Server.
2. Enter the following command:

   ```
   XPSConfig
   ```

   The Products Menu opens and lists the products.
3. Enter XPS for Extensible Policy Store.

   The Parameters Menu opens and lists the XPS parameters.
4. Enter 7 for Autosweep.

   The Autosweep Parameter Menu opens.
5. Verify that the Autosweep value is set to TRUE or enter C to Change the value to TRUE.

   Note: This step specifies running XPSSweeper according to the Autosweep Schedule.
6. Enter Q to exit the Autosweep Menu and return to the Parameters Menu.

7. Enter 8 for AutosweepSchedule.

   The AutosweepSchedule Parameter Menu opens.

8. Enter C to Change the value of the AutosweepSchedule parameter.
9. Enter the time that you want for the New Value.
10. Enter Q three times.

    The command prompt appears.

Chapter 21: Policy Server Configuration Files

This section contains the following topics:

CA Compliance Security Manager Configuration File

CA SiteMinder® has a command line tool, smcompliance, which creates compliance reports that you manually import into CA Security Compliance Manager.The CA Compliance Security Manager configuration file (compliance.conf) lets you modify the contents of the compliance reports.

Location: *siteminder_home*\compliance\config

siteminder_home

Specifies the Policy Server installation path.

More information:

Change the Content of the Existing Compliance Reports (see page 271)
Add a New Compliance Report (see page 270)

Connection API Configuration File

The Connection API file (conapi.conf) is used to configure services through the Connection API. These services include the OneView Monitor.

Location: *siteminder_home*\config

siteminder_home

Specifies the Policy Server installation path.

More information:

Configure OneView Monitor Port Numbers (see page 173)

OneView Monitor Configuration File

The CA SiteMinder® OneView Monitor:

- Identifies performance bottlenecks and provides information about resource usage in a CA SiteMinder® deployment.
- Displays alerts when certain events, such as component failure, occur.

The OneView Monitor configuration file (mon.conf) is used to specify:

- The frequency at which the OneView Monitor requests data from registered components.
- The frequency at which registered components send a heart beat event to the OneView Monitor.
- If the Policy Server component index is constant.

Location: *siteminder_home*\monitor

siteminder_home

Specifies the Policy Server installation path.

More information:

Setting The OneView Data Refresh Rate and Heartbeat (see page 172)

CA SiteMinder® Configuration File

The CA SiteMinder® configuration file (siteminder.conf) is used to:

- Start and stop the Policy Server processes
- Configure, disable, and enable executives

One or more executive applications monitor the status of Policy Server processes and automatically restart any processes that fail.

Location: *siteminder_home*\config

siteminder_home

Specifies the Policy Server installation path.

More information:

Configure the UNIX Executive (see page 26)
Configure Windows Executives (see page 26)

SNMP Configuration File

SNMP–compliant network management applications can monitor many operational aspects of a CA SiteMinder® environment. The CA SiteMinder® SNMP module allows for the exchange of information with these applications.

The SNMP configuration file (snmp.conf) provides settings for the CA SiteMinder® SNMP module.

Location: *siteminder_home*\config

siteminder_home

Specifies the Policy Server installation path.

Note: For more information about using this file, see Configure the SNMP Agent on Windows in the *Policy Server Installation Guide*.

SNMP Event Trapping Configuration File

The SNMP event trapping configuration file (snmptrap.conf) provides settings for the following:

- The system events that you want mapped to SNMP traps.
- The addresses of the Network Management Systems to which the traps are sent.

Location: *siteminder_home*\config

siteminder_home

Specifies the Policy Server installation path.

Note: For tasks that are related to this file, see How to Configure SNMP Trapping Events on Windows and How to Configure SNMP Trapping Events on UNIX in the *Policy Server Installation Guide*.

More information:

Event Data (see page 189)
CA SiteMinder® MIB (see page 182)

Policy Server Registry Keys

The Policy Server registry keys are located at one of the following:

- (Windows) HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\PolicyServer.
- (UNIX) The sm.registry file.

  The default location of this file is *siteminder_home*/registry.

  siteminder_home

  Specifies the Policy Server installation path.

Consider the following:

- Specific circumstances can require that you do one of the following:
  - Modify an existing registry key.
  - Create a registry key and assign a value.

  In these cases, the CA SiteMinder® documentation details the required steps.
- In all other cases, we recommend that you modify Policy Server settings using the Administrative UI or the Policy Server Management Console, as detailed in the CA SiteMinder® documentation. Do not modify Policy Server settings using the registry keys, unless instructed by CA SiteMinder® Support or the documentation.

Appendix A: CA SiteMinder® and CA Security Compliance Manager

This section contains the following topics:

How CA SiteMinder® and CA Security Compliance Manager Integration Works

CA CA SiteMinder® offers a command line tool, smcompliance, which creates compliance reports that you can manually import into CA Security Compliance Manager. The smcompliance tool generates the following types of reports by default:

Policies

Lists all of the policies stored in the CA SiteMinder® Policy Server from which the command was run.

User Directory

Lists all of the user directories in the policy store that is associated with the Policy Server.

User Resources

Lists the users, their respective user directories and any associated policies.

To export CA SiteMinder® compliance data to CA Security Compliance Manager, use the following process:

1. (Optional) Update the configuration file for the compliance tool if you want to do any of the following:
   - Change the report name or field names in an existing report.
   - Add a new report.
   - Delete a report.
2. Generate the reports by running the compliance tool on the Policy Server.
3. Send the generated reports to the CA Security Compliance Manager administrator in your organization.

Generate the Compliance Reports

The CA SiteMinder® compliance reports for CA Security Compliance Manager are generated with a command line tool. After the reports are generated, you must send them to the CA Security Compliance Manager administrator in your organization so they can be imported into CA Security Compliance Manager.

To generate the compliance reports

1. Open a command line window on the machine which hosts the Policy Server.
2. Run the smcompliance command with any of the following options:

   -dir *directory_name*

   Specifies the full path to an output directory where the generated reports will be saved. If this directory already exists, the tool renames the existing directory as a backup.

   Default: *siteminder_home*/compliance/output

   -conf *configuration_file*

   Specifies the full path to the configuration file that determines the content and format of the reports. The default configuration file has the content for CA Security Compliance Manager, but you can customize a configuration file to meet your needs.

   Default: *siteminder_home*/compliance/config

   -log *log_file*

   Specifies the full path to a log file.

   Default: *siteminder_home*/compliance/output

   -format *format_type*

   Specifies one of the following file types for the reports:

   - CSV (comma-separated value) file.
   - XML file

   Default: csv

   The reports and log file are generated. The files are ready to send to the CA Security Compliance Manager administrator.

Display List of Available Compliance Reports Or Their Fields

The CA SiteMinder® compliance-report tool, smcompliance, can generate other types of reports in addition to those reports produced by default.

To display a list of available compliance reports

1. Open a command prompt on the Policy Server.
2. Enter the following command:

   ```
   smcompliance -help reports
   ```

   A list of report names appears.
3. (Optional) To see what fields a report contains, enter the following command:

   ```
   smcompliance -generate report_name
   ```

   The *report_name* must match a name from the list in Step 2. For example, to see what fields the agents report contains, enter the following:

   smcompliance -generate agents

   A list of fields for the report appears in XML format. You can add the XML to a configuration file to produce a new report.

Add a New Compliance Report

You can generate other types of compliance reports by adding new reports to the configuration file used by the smcompliance tool.

To add a new compliance report

1. Verify the name of the report you want to add displaying a list of available compliance reports with the smcompliance tool.
2. Display the fields of the report you want to add, then copy the xml-formatted text from the screen.
3. Navigate to the following directory on the Policy Server.

   siteminder_home\compliance\config
4. Open the default configuration file, compliance.conf, with a text editor.
5. Save a copy of the default file using a different name.
6. Copy an existing <report> section and paste it above the </reports> tag at the bottom of the configuration file.
7. Remove the existing text between the <columns> tags.
8. Add the text from Step 2 between the <columns> tags.
9. Replace the value of the name attribute in the <report> tag with the name of the report from Step 1.
10. Change the value of the name attribute in the <table> tag to describe the new report. The generated report file uses this name.
11. Save your changes and close the new configuration file.

    The new report is added.
12. Run the smcompliance command and specify the new configuration file.

Change the Content of the Existing Compliance Reports

The reports generated by the default configuration file provide the typical compliance information that CA Security Compliance Manager needs. If your organization has different needs, you can create your own custom configuration file to generate reports with the information you want.

1. Navigate to the following directory on the Policy Server.

   siteminder_home\compliance\config

2. Open the default configuration file, compliance.conf, with a text editor.
3. Save a copy of the default file using a different name.
4. Make the any of the following changes to the new copy of the configuration file:
   - To remove a report, look between the <report> and </report> tags for the report that you want to remove, and then delete the section and the tags.
   - To change the name of a report, modify the value of the name attribute in the <table> tag.
   - To change the name of a field in a report (*not* the information it contains), modify the value of the name attribute in the <column> tag.
   - Move any columns you want to add from <comment> section in the configuration file to the <columns> section.

Appendix B: General CA SiteMinder® Troubleshooting

Resolve LDAP search timeout issues

Symptom:

My smps.log shows that my LDAP server is timing out before it returns any search results. How can I increase the time out interval?

Solution:

Change the value of the following registry setting (see page 37):

`SearchTimeout`

Administrative UI Becomes Unresponsive

Symptom:

On a stand–alone Administrative UI installation (with an embedded JBoss application server), the Administrative UI becomes unresponsive. That is, the Administrative UI service does not start or you cannot log in after a period of normal operation.

Solution:

1. Stop the Administrative UI application server.
2. When the application server is down, rename or delete the data directory in the following location:

   `\adminui\server\default`
3. Restart the application server.
4. Run the following command on the Policy Server:

   `XPSRegClient` *`client_name`*`[:`*`passphrase`*`] -adminui -t` *`timeout`* `-r` *`retries`* `-c` *`comment`*
   `-cp -l` *`log_path`* `-e` *`error_path`*
   `-vT -vI -vW -vE -vF`

   Note: Inserting a space between *client_name* and [:*passphrase*] results in an error.

client_name

Identifies the Administrative UI being registered.

Limit: This value must be unique. For example, if you have previously used smui1 to register an Administrative UI, enter smui2.

Note: Record this value. This value is to complete the registration process from the Administrative UI.

passphrase

Specifies the password that is required to complete the registration of the Administrative UI.

Limits:

- The passphrase must contain at least six (6) characters.
- The passphrase cannot include an ampersand (&) or an asterisk (*).
- If the passphrase contains a space, it must be enclosed in quotation marks.
- If you are registering the Administrative UI as part of an upgrade, you can reuse a previous passphrase.

Note: If you do not specify the passphrase in this step, XPSRegClient prompts you to enter and confirm one.

Important! Record the passphrase, so that you can refer to it later.

-adminui

Specifies that an Administrative UI is being registered.

-t *timeout*

(Optional) Specifies how long you have to complete the registration process from the Administrative UI. The Policy Server denies the registration request when the timeout value is reached.

Unit of measurement: minutes

Default: 240 (four hours)

Minimum Limit: 1

Maximum Limit: 1440 (one day)

-r *retries*

(Optional) Specifies how many failed attempts are allowed when you complete the registration process from the Administrative UI. A failed attempt can result from an incorrect client name or passphrase submitted to the Policy Server during the registration process.

Default: 1

Maximum Limit: 5

-c *comment*

(Optional) Inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-cp

(Optional) Specifies that registration log file can contain multiple lines of comments. The registration tool prompts for multiple lines of comments and inserts the specified comments into the registration log file for informational purposes.

Note: Surround comments with quotes.

-l *log_path*

(Optional) Specifies where to export the registration log file.

Default: *siteminder_home*\log

siteminder_home

Specifies the Policy Server installation path.

-e *error_path*

(Optional) Sends exceptions to the specified path.

Default: stderr

-vT

(Optional) Sets the verbosity level to TRACE.

-vI

(Optional) Sets the verbosity level to INFO.

-vW

(Optional) Sets the verbosity level to WARNING.

-vE

(Optional) Sets the verbosity level to ERROR.

-vF

(Optional) Sets the verbosity level to FATAL.

The registration tool lists the name of the registration log file and prompts for a passphrase.

5. Press Enter.

   The registration tool creates the client name and passphrase pairing.

6. To register the Administrative UI with a Policy Server, complete one of the following steps on the Administrative UI host:

   - Windows:
     - (Recommended) Use the Administrative UI shortcut to open the Administrative UI. Using the shortcut registers the Administrative UI over SSL. If you do not have access to the shortcut, open a web browser and go to the following location:

       https://*host*:8443/iam/siteminder/adminui

       Note: A self–signed certificate that is valid for ten years is created and used for the connection. The certificate is created with an RSA 2048 key strength.
     - Open a web browser and go to the following location:

       http://host:8080/iam/siteminder/adminui
   - UNIX:
     - (Recommended) Open a web browser and go to the following location to register the Administrative UI over SSL:

       https://host:8443/iam/siteminder/adminui
     - Open a browser and go to the following location:

       http://*host*:8080/iam/siteminder/adminui

       Note: If the host system does not have a web browser, you can remotely access the login screen.

     host

     Specifies the fully qualified Administrative UI host system name.

     The CA SiteMinder® Administrative UI login screen appears.

7. Enter the following value in the User Name field:

   `siteminder`

8. Type the CA SiteMinder® superuser account password in the Password field.

Resolve MySQL Session Store Timeout Errors

Symptom:

When a MySQL database is configured as the session store, the following timeout message appears periodically in the Policy Server logs:

```
[ERROR][sm-Server-07011] failed.Exception : State = HYT00 Internal
Code = 0 - [DataDirect][ODBC MySQL Wire Protocol driver]Timeout
expired.. Error code -4007
```

Solution:

Increase the session server maintenance query timeout by modifying the value of the MaintenanceQueryTimeout registry key in the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Se
ssionServer
```

We recommend the following value:

```
MaintenanceQueryTimeout=0x12c
```

Policy Server Exits with LDAP Admin Limit Exceeded Error

Symptom:

The Policy Server gracefully exits when LDAP search to Policy Store/Key Store fails with the following error:

```
LDAP_ADMINLIMIT_EXCEEDED (error code 11)
```

Solution:

Enable the following optional registry key:

`EnableRetryOnAdminLimitExceededFailure`

Allows the Policy Server to retry the search once before giving up.

Values: 0 (disabled) or 1 (enabled).

Default: 0

Windows

Follow these steps:

1. From the Windows Start menu, select Run.
2. Enter regedit in the Run dialog box and click OK.

3. In the Registry Editor, navigate to the following location:

   `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Netegrity\SiteMinder\CurrentVersion\ObjectStore`

4. Modify the value of the following registry key:

   `EnableRetryOnAdminLimitExceededFailure`

5. Restart the Policy Server.

UNIX

Follow these steps:

1. Navigate to the following location:

   install_directory/siteminder/registry

2. Open sm.registry in a text editor.

3. Locate the following text in the file:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\ObjectStore`

4. Modify the value of the following registry key:

   `EnableRetryOnAdminLimitExceededFailure`

5. Restart the Policy Server.

Command Line Troubleshooting of the Policy Server

You can run the Policy Server process interactively in a separate window with debugging options turned on to troubleshoot problems. The following server executable may be run from the command line:

install_dir/siteminder/bin/smpolicysrv

Note: On Windows systems, do *not* run the smpolicysrv commands from a remote desktop or Terminal Services window. The smpolicysrv command depends on inter-process communications that do not work if you run the smpolicysrv process from a remote desktop or Terminal Services window.

Use the following options with the smpolicysrv command:

-t*port_number*

This option is used to modify the TCP port that the server binds to for Agent connections. If this switch is not used, the server defaults to the TCP port specified through the Policy Server Management Console.

-u*port_number*

This option is used to modify the UDP port that the server binds to for RADIUS connections. If this switch is not used, the server defaults to the UDP port specified through the Policy Server Management Console. This switch is applicable to the authentication and accounting servers only.

-stop

This switch stops the server in the most graceful manner possible. All database and network connections are closed properly using this method.

-abort

This switch stops the server immediately, without first closing database and network connections.

-stats

This switch produces current server runtime statistics such as thread pool limit, thread pool message, and the number of connections.

-resetstats

This switch resets the current server runtime statistics without restarting the Policy Server. This switch resets the following counters:

- Max Threads is reset to the Current Threads value.
- Max Depth of the message queue is reset to the Current Depth of the message queue.
- Max Connections is reset to Current Connections.
- Msgs, Waits, Misses, and Exceeded limit are reset to zero.

This switch does not reset the following counters:

- Thread pool limit
- Current Threads
- Current Depth of the message queue
- Current Connections
- Connections Limit

-publish

Publishes information about the Policy Server.

-tadm*port_number*

Sets the TCP port for the administration service.

-uac*port_number*

Sets the UDP port for Radius accounting.

-uadm*port_number*

Sets the UDP port for the administration service.

-uauth*port_number*

Sets the UDP port for Radius authentication.

-ac

Enables the servicing of Agent API requests.

-noac

Disables the servicing of Agent API requests.

-adm

Enables the servicing of administration requests.

-noadm

Disables the servicing of administration requests.

-radius

Enables the servicing of RADIUS requests.

-noradius

Disables the servicing of RADIUS requests.

-onlyadm

Combines the following options into a single option:

- -adm
- -noac
- -noradius

–starttrace

The command:

- starts logging to a trace file and does not affect trace logging to the console.
- issues an error if the Policy Server is not running.

If the Policy Server is already logging trace data, running the –starttrace command causes the Policy server to:

- rename the current trace file with a time stamp appended to the name in the form: *file_name*.YYYYMMDD_HHmmss.*extension*

- create a new trace file with the original name

  For example, if the trace file name in Policy Server Management Console's Profiler tab is C:\temp\smtrace.log, the Policy Server generates a new file and saves the old one as c:\temp\smtrace.20051007_121807.log. The time stamp indicates that the Policy Server created the file on October 7, 2005 at 12:18 pm. If you have not enabled the tracing of a file feature using the Policy Server Management Console's Profiler tab, running this command does not do anything.

-stoptrace

The command:

- stops logging to a file and does not affect trace logging to the console.
- issues an error if the Policy Server is not running.

You can use two smpolicysrv command line options, -dumprequests and -flushrequests, to troubleshoot and recover more quickly from an overfull Policy Server message queue. Only use these options in the following case:

1. Agent requests waiting in the Policy Server message queue time out.
2. One or more Agents resend the timed-out requests, overfilling the message queue.

!Important Do not use -dumprequests and -flushrequests in normal operating conditions.

-dumprequests

Outputs a summary of each request in the Policy Server message queue to the audit log.

-flushrequests

Flushes the entire Policy Server message queue, so that no requests remain.

Start or Stop Debugging Dynamically

You can start or stop the debugging function of certain components at any time *without* restarting the Policy Server.

Note: We recommend using this feature only when directed to do so by CA Technologies technical support personnel.

Follow these steps:

1. Open a command window on the machine hosting the Policy Server.
2. Type the following command:

   ```
   SmCommand -i SiteMinder
   ```

   A list of options appears.
3. Select one of the following debugging options according to the instructions that your CA support representative provides.

   CA.EPM::EPMObjects_Debug

   Toggles the debugging state of the CA SiteMinder® EPM component.

   CA.XPS::Debug

   Toggles the debugging state of the CA SiteMinder® XPS component.

   CA.XPS::XPSEval_Debug

   Toggles the debugging state of the CA SiteMinder® XPSEvaluate component.

Start or Stop Tracing Dynamically

You can start or stop the tracing functions of certain components at any time *without* restarting the Policy Server.

Follow these steps:

1. Open a command window on the machine hosting the Policy Server.
2. Type the following command:

   ```
   SmCommand -i SiteMinder
   ```

3. A list of options appears. The tracing options display the *opposite* of their current states. For example, if tracing for CA XPS is currently disabled, the option to turn it on appears as follows:

   item_number - CA.XPS::TraceOn

4. Select one of the following options by typing the number of the option you want:

   CA.EPM::EPMObjects_Trace*State*

   Toggles tracing for the EPM Objects components on or off.

   CA.XPS::Trace*State*

   Toggles tracing for the XPS components on or off.

   CA.XPS::XPSEval_Trace*State*

   Toggles tracing for the XPS Expression Evaluator components on or off.

   A confirmation message appears. The list of options is redisplayed with your changes.

5. (Optional) Repeat Step 4 to start or stop tracing on another component.
6. Type Q to quit.

   Tracing has been changed dynamically.

Policy Server Hangs after Web Agent Communication Failure

Symptom:

If a Web Agent goes offline during a Policy Server request, for example, during a network outage, and does not notify the Policy Server of the communication failure, the Policy Server continues to wait for the Web Agent data. The Policy Server continues to wait, even after the Web Agent regains network functionality and closes the connection to the Policy Server.

If many requests from one or more Web Agents are lost in this manner, the Policy Server can become unresponsive because the worker threads handling the requests are not released.

Solution:

Creating and enabling the SiteMinder Enable TCP Keep Alive (SM_ENABLE_TCP_KEEPALIVE) environment variable configures the Policy Server to send KeepAlive packets to idle Web Agent connections. The interval at which the Policy Server sends the packets is based on OS–specific TCP/IP parameters.

You can also set this variable at the locations for the Web Agent, an Application Server Agent (ASA), the Administrative UI, or a custom agent created by the SDK.

Consider the following when configuring the parameters:

- When the Policy Server must start to send the packets.
- The interval at which the Policy Server sends the packets.
- The number of times the Policy Server sends the packets before determining that the Web Agent connection is lost.

  Note: For more information about configuring TCP/IP parameters, see your OS–specific documentation.

To configure the Policy Server to send KeepAlive packets to idle Web Agent connections

1. Log into the Policy Server host system.
2. Do one of the following:
   - (Windows) Create the following system environment variable with a value of 1:

     SM_ENABLE_TCP_KEEPALIVE
   - (UNIX)
     a. Create the following system environment variable:

        SM_ENABLE_TCP_KEEPALIVE=1

     b. Export the environment variable.

   Note: The value must be 0 (disabled) or 1 (enabled). If a value other than 0 or 1 is configured, the environment variable is disabled. If the environment variable is disabled, the Policy Server does not send KeepAlive packets to idle Web Agent connections.

Check the Installed JDK Version

If a Policy Server fails to start, check that the correct version of the JDK is installed.

Override the Local Time Setting for the Policy Server Log

The Policy Server log file, *install_dir*/siteminder/log/smps.log, displays time in local timezone as identified by the operating system of the machine on which the Policy Server is installed.

To display the time in this log file in GMT time:

1. Locate the following registry setting:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\
   CurrentVersion\LogConfig\LogLocalTime
   ```

2. Change the value from 1 (which is the default) to 0.

Review System Application Logs

If the Policy Server fails to start, review the event log (on Windows) or the syslog (on UNIX) for information about the Policy Server.

- On Windows, view the event log using the Event Viewer. From the Log menu of the Event Viewer, select Application.
- On UNIX, view the syslog using a text editor.

LDAP Referrals Handled by the LDAP SDK Layer

Enhancements have been made to CA SiteMinder®'s LDAP referral handling to improve performance and redundancy. Previous versions of CA SiteMinder® supported automatic LDAP referral handling through the LDAP SDK layer. When an LDAP referral occurred, the LDAP SDK layer handled the execution of the request on the referred server without any interaction with the Policy Server.

CA SiteMinder® now includes support for non-automatic (enhanced) LDAP referral handling. With non-automatic referral handling, an LDAP referral is returned to the Policy Server rather than the LDAP SDK layer. The referral contains all of the information necessary to process the referral. The Policy Server can detect whether the LDAP directory specified in the referral is operational, and can terminate a request if the appropriate LDAP directory is not functioning. This feature addresses performance issues that arise when an LDAP referral to an offline system causes a constant increase in request latency. Such an increase can cause CA SiteMinder® to become saturated with requests.

Disable LDAP Referrals

If LDAP referrals are causing errors, you can disable all LDAP referrals. Note that disabling LDAP referrals will cause any referrals in your directory to return errors.

To disable LDAP referral handling for Policy Servers on Windows

1. From the Windows Start menu, select Run.
2. Enter regedit in the Run dialog box and click OK.
3. In the Registry Editor, navigate to:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Ds\LDAPProvider`
4. Modify the following registry value:

   Note: The value is shown in hexadecimal notation.

   `"EnableReferrals"=dword:00000001`

   Determines if any LDAP referrals are handled by the Policy Server. If set to 0, no LDAP referrals will be accepted by the Policy Server. If set to 1, the Policy Server accepts LDAP referrals.

   LDAP referrals are enabled by default. This setting may only be modified by editing the Registry.
5. Restart the Policy Server.

To disable LDAP referral handling for a Policy Server on Solaris

1. Navigate to:

   install_dir`/siteminder/registry`
2. Open sm.registry in a text editor.
3. Locate the following text in the file:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Ds\LDAPProvider`
4. Locate the line that follows the line from step 3 and begins with:

   `EnableReferrals`
5. Modify the value that comes just before the semicolon as follows.

   Note: The value must be converted to hexadecimal notation.

   Determines if any LDAP referrals are handled by the Policy Server. If set to 0, no LDAP referrals will be accepted by the Policy Server. If set to 1, the Policy Server accepts LDAP referrals.
6. Restart the Policy Server.

Handle LDAP Referrals on Bind Operations

To configure LDAP referrals on bind operations for Policy Servers on Windows

1. From the Windows Start menu, select Run.
2. Enter regedit in the Run dialog box and click OK.
3. In the Registry Editor, navigate to:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\
   CurrentVersion\Ds\LDAPProvider
   ```

4. Modify the following registry value:

   Note: The value is shown in hexadecimal notation.

   ```
   "ChaseReferralsOnBind"=dword:00000001
   ```

   Determines if LDAP referrals on a bind operation should be chased. Most LDAP directory servers handle LDAP referrals on binds. If your directory server handles referrals on binds, ChaseReferralsOnBind has no effect. However, if your directory does not, this setting allows the Policy Server to handle bind referrals.

   If your server does handle referrals on bind operations you can change this setting to 0, disabling the Policy Server's ability to handle bind referrals.

   Referral chasing on binds is enabled by default. This setting may only be modified by editing the Registry.

5. Restart the Policy Server.

To configure LDAP referrals on bind operations for a Policy Server on Solaris

1. Navigate to:

   install_dir/siteminder/registry

2. Open sm.registry in a text editor.
3. Locate the following text in the file:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\
   CurrentVersion\Ds\LDAPProvider
   ```

4. Locate the line that follows the line from step 3 and begins with:

   ```
   ChaseReferralsOnBind
   ```

5. Modify the value that comes just before the semicolon as follows.

   Note: The value must be converted to hexadecimal notation.

   Determines if LDAP referrals on a bind operation should be chased. Most LDAP directory servers handle LDAP referrals on binds. If your directory server handles referrals on binds, ChaseReferralsOnBind has no effect. However, if your directory does not, this setting allows the Policy Server to handle bind referrals.

If your server does handle referrals on bind operations you can change this setting to 0, disabling the Policy Server's ability to handle bind referrals.

6. Restart the Policy Server.

Idle Timeouts and Stateful Inspection Devices

Stateful inspection devices, such as firewalls, generally have an idle timeout setting. CA SiteMinder® connections from Policy Servers to Agents also have idle timeout settings.

The Policy Server polls the services at a regular interval. The polling interval has a 5-minute cap. This means the idle connections will time out within 5 minutes of the configured value. For example, if the value 55 minutes is specified as the timeout, then the connections will time out between 55 and 60 minutes.

By default, connections created between a Policy Server and a Web Agent expire after 10 minutes of inactivity. If a firewall or other stateful network device exists between a Policy Server and a Web Agent and connections are idle for longer that the device's idle timeout, then the device ends those connections without notifying either the Policy Server or the Web Agent.

When the Web Agent attempts to use a connection that has been terminated by a network device, it receives a network error, resets the connection, and reports a 500 error (20-0003) to the browser. The Agent also closes all other connections in the connection pool that are the same age or older than the one that received the error. On the Policy Server side, however, the sockets for those connections remain established. Depending on the load patterns for the site, connection growth can occur to a point that it interferes with the proper operation of the Policy Server.

To prevent a firewall or other stateful network device from terminating Policy Server – Web Agent connections, you must configure an idle timeout for Policy Server. When the Policy Server closes a TCP/IP connection, it will wait for a specified period of inactivity and then send RESET, closing the server and client ends of the connection cleanly. The period of inactivity is specified in the Idle Timeout (minutes) field on the Settings tab of the Policy Server Management Console.

Note: The Idle Timeout (minutes) field can also be used to limit the amount of time an administrator may be connected.

At installation, the Idle Timeout value is set to 10 minutes. To work with a stateful network device, set the value to a shorter time period than the TCP/IP idle timeout of the device that is located between the web agent and the policy server. It is recommended that the TCP Idle Session Timeout be set to 60% of the idle timeout of any stateful device(s) to ensure that the Policy Server's timeout occurs first.

Error -- Optional Feature Not Implemented

When the Policy Server attempts to use an ODBC data source, but cannot connect to the database, the following error message may appear:

```
Optional feature not implemented.. Error code -1
```

Often this message indicates a component mismatch, a misconfiguration or invalid credentials.

Note: CA's configuration of the Intersolv or Merant drivers differs from the default configuration.

If you receive the above message, and you are using an ODBC data source as your policy store, or for logging, see the sections that describe the configuration of ODBC data sources in the *Policy Server Installation Guide*.

Errors or Performance Issues When Logging Administrator Activity

On the Audit tab of the Policy Server Management Console, if you have set Administrator Changes to Policy Store Objects to Log All Events, and you are logging to an ODBC data source, you may encounter one of the following:

- Substantial delays when saving objects in the Administrative UI
- The error message:

  ```
  Exception occurred while executing audit log insert.
  ```

If either of these conditions occur, log to a text file instead.

Policy Servers Sharing Policy Store Not Updated Consistently

Symptom:

If multiple Policy Servers share a single policy store, the data inside the policy store could possibly be out of synchronization. Synchronization issues can occur under the following conditions:

- The system times on the Policy Servers differ.
- Network latency.

For example, suppose the system time on Policy Server A is 10:00, and the system time on Policy Server B is 10:05. Policy Server A sends its data to the policy store at 10:00. Policy Server B does *not* record any changes in the data timestamped *before* 10:05 because those events appear to have occurred earlier.

Solution:

To accommodate different system times or network latency issues:

1. Create the following DWORD registry setting:

   ```
   SiteMinder\CurrentVersion\ObjectStore
   Key: ServerCommandTimeDelay
   ```

2. Set the value of the key to the number of seconds that corresponds to the time difference. For example, for a five-minute time difference, set the value of the key to 300.

Cache Failure Timeout

The Policy Server can sometimes fail to process events after deleting the following objects:

- Policies
- Rules
- Realms
- Policy domains

Cache failure timeout functionality addresses this issue.

When the secondary cache buildup is not successful, the policy server aborts after a timeout period. You specify the timeout period using the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\ObjectStore\CacheFailureTimeout
```

The value of this key is in seconds. The default is 0, which implies no timeout.

After the policy server shuts down, the smexec brings up the next process event request immediately.

Key Rollover Log Messages

When the Policy Server issues key rollover commands to Web agents, they can process the commands successfully some of the time, but other times, the commands fail. To facilitate troubleshooting in this situation, the Policy Server logs three types of messages to SMPS.log.

[INFO] Key Rollover Request has been initiated manually

This message is logged when an administrator manually initiates a key rollover.

[INFO] Key Rollover Request has been initiated automatically by Policy Server

This message is logged when the Policy Server initiates a key rollover automatically.

[INFO] Key distribution has been initiated by Policy Server

This message is logged when a key rollover request has been initiated, either automatically or manually.

Cache Update Log Messages

You can enable and disable cache flushing or updates through the Administrative UI or the Command Line Interface. To facilitate troubleshooting, the Policy Server logs two types of messages to SMPS.log.

[INFO] Server 'enablecacheupdates' command received.

This message is logged when cache flushing is enabled, either through the Administrative UI or the Command Line Interface.

[INFO] Server 'disablecacheupdates' command received.

This message is logged when cache flushing is disabled, either through the Administrative UI or the Command Line Interface.

Event Handlers List Settings Warning when Opening Policy Server Management Console

Symptom:

When I log into the Policy Server Management Console for the first time after upgrading to CA SiteMinder® 12.52 SP1, a warning message appears saying that the event handlers list should be set to XPSAudit.

Solution:

For CA SiteMinder® 12.52 SP1, you can no longer add custom event handler libraries using the Policy Server Management Console. Use the XPSConfig command-line tool to add any custom event-handler libraries.

More information:

Add Event Handler Libraries (see page 130)

CA SiteMinder® Policy Server Startup Event Log

Symptom:

My Policy Server crashed while it was starting up. I want to know what CA SiteMinder® startup events occurred before the Policy Server crashed.

Solution:

If the Policy Server crashes on startup, a log of the startup events is stored in the following file:

policy_server_home/audit/SmStartupEvents.audit

VLV Indexing on Some LDAP User Directories Causes SiteMinder Agent Group Lookups to Fail (174279)

Symptom:

Flaws in the Virtual List View (VLV) implementation on some LDAP user directories can cause SiteMinder Agent group lookups to fail, returning zero entries and raising a “directory unwilling to perform" error.

Solution:

If you experience SiteMinder Agent group lookup failures as described, disable VLV lookups on the Policy Server.

Create the registry key EnableVLV of type DWORD at the following location:

`HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\Siteminder\CurrentVersion\DS\LDAPProvider`

EnableVLV

Disables or enables VLV for LDAP directory lookups. To disable VLV, set EnableVLV to 0. To enable VLV, set EnableVLV to 1.

Values: 0 (disabled) or 1 (enabled).

Default: 1 (enabled).

STAR issue: 20397633-1

Appendix C: Log File Descriptions

smaccesslog4

The following table describes the logging that appears in smaccesslog4, which logs authentication and authorization activity.

Field Name	Description	Null?	Field Type
sm_timestamp	This marks the time at which the entry was made to the database.	NOT NULL	DATE
sm_categoryid	The identifier for the type of logging. It may be one of the following ■ 1 = Auth ■ 2 = Az ■ 3 = Admin ■ 4 = Affiliate	NOT NULL	NUMBER(38)
sm_eventid	This marks the particular event that caused the logging to occur. It may be one of the following: ■ 1 = AuthAccept ■ 2 = AuthReject ■ 3 = AuthAttempt ■ 4 = AuthChallenge ■ 5 = AzAccept ■ 6 = AzReject ■ 7 = AdminLogin ■ 8 = AdminLogout ■ 9 = AdminReject ■ 10 = AuthLogout ■ 11 = ValidateAccept ■ 12 = ValidateReject ■ 13 = Visit	NOT NULL	NUMBER(38)
sm_hostname	The machine on which the server is running.		VARCHAR2(255)

Field Name	Description	Null?	Field Type
sm_sessionid	This is the session identifier for this user's activity.		VARCHAR2(255)
sm_username	The username for the user currently logged in with this session.		VARCHAR2(512)
sm_agentname	The name associated with the agent that is being used in conjunction with the policy server.		VARCHAR2(255)
sm_realmname	This is the current realm in which the resource that the user wants resides.		VARCHAR2(255)
sm_realmoid	This is the unique identifier for the realm.		VARCHAR2(64)
sm_clientip	This is the IP address for the client machine that is trying to utilize a protected resource.		VARCHAR2(255)
sm_domainoid	This is the unique identifier for the domain in which the realm and resource the user is accessing exist.		VARCHAR2(64)
sm_authdirname	This not used by the reports generator.		VARCHAR2(255)
sm_authdirserver	This not used by the reports generator.		VARCHAR2(512)
sm_authdir-namespace	This not used by the reports generator.		VARCHAR2(255)
sm_resource	This is the resource, for example a web page, that the user is requesting.		VARCHAR2(512)
sm_action	This is the HTTP action. Get, Post, and Put.		VARCHAR2(255)
sm_status	This is some descriptive text about the action.		VARCHAR2(1024)

Field Name	Description	Null?	Field Type
sm_reason	These are the motivations for logging. 32000 and above are user defined. They are as follows: ■ 0 = None ■ 1 = PwMustChange ■ 2 = InvalidSession ■ 3 = RevokedSession ■ 4 = ExpiredSession ■ 5 = AuthLevelTooLow ■ 6 = UnknownUser ■ 7 = UserDisabled ■ 8 = InvalidSessionId ■ 9 = InvalidSessionIp ■ 10 = CertificateRevoked ■ 11 = CRLOutOfDate ■ 12 = CertRevokedKeyCompromised ■ 13 = CertRevokedAffiliationChange ■ 14 = CertOnHold ■ 15 = TokenCardChallenge ■ 16 = ImpersonatedUserNotInDi ■ 17 = Anonymous ■ 18 = PwWillExpire ■ 19 = PwExpired ■ 20 = ImmedPWChangeRequired ■ 21 = PWChangeFailed ■ 22 = BadPWChange ■ 23 = PWChangeAccepted ■ 24 = ExcessiveFailedLoginAttempts ■ 25 = AccountInactivity ■ 26 = NoRedirectConfigured ■ 27 = ErrorMessageIsRedirect	NOT NULL	NUMBER(38)

Field Name	Description	Null?	Field Type
sm_reason (continued)	■ 28 = Tokencode ■ 29 = New_PIN_Select ■ 30 = New_PIN_Sys_Tokencode ■ 31 = New_User_PIN_Tokencode ■ 32 = New_PIN_Accepted ■ 33 = Guest ■ 34 = PWSelfChange ■ 35 = ServerException ■ 36 = UnknownScheme ■ 37 = UnsupportedScheme ■ 38 = Misconfigured ■ 39 = BufferOverflow		
sm_transactionid	This is not used by the reports generator.		VARCHAR2(255)
sm_domainname	This is the name of the domain in which the realm and resource the user is accessing exist.	NULL	VARCHAR2(255)
sm_impersonator-name	This is the login name of the administrator that is acting as the impersonator in an impersonated session.	NULL	VARCHAR2(512)
sm_impersonator-dirname	This is the name of the directory object that contains the impersonator.	NULL	VARCHAR2(255)

smobjlog4

The following table describes the logging that appears in smobjlog4, which logs administrative events.

Field Name	Description	Null?	Type
sm_timestamp	This marks the time at which the entry was made to the database.	NOT NULL	DATE

Field Name	Description	Null?	Type
sm_categoryid	The identifier for the type of logging. It may be one of the following: ■ 1 = Auth ■ 2 = Agent ■ 3 = AgentGroup ■ 4 = Domain ■ 5 = Policy ■ 6 = PolicyLink ■ 7 = Realm ■ 8 = Response ■ 9 = ResponseAttr ■ 10 = ResponseGroup ■ 11 = Root ■ 12 = Rule ■ 13 = RuleGroup ■ 14 = Scheme ■ 15 = UserDirectory ■ 16 = UserPolicy ■ 17 = Vendor ■ 18 = VendorAttr ■ 19 = Admin ■ 20 = AuthAzMap ■ 21 = CertMap ■ 22 = ODBCQuery ■ 23 = SelfReg ■ 24 = PasswordPolicy ■ 25 = KeyManagement ■ 26 = AgentKey ■ 27 = ManagementCommand ■ 28 = RootConfig	NOT NULL	NUMBER(38)

Field Name	Description	Null?	Type
sm_categoryid (continued)	■ 29 = Variable ■ 30 = VariableType ■ 31 = ActiveExpr ■ 32 = PropertyCollection ■ 33 = PropertySection ■ 34 = Property ■ 35 = TaggedString ■ 36 = TrustedHost ■ 37 = SharedSecretPolicy	NOT NULL	NUMBER(38)
sm_eventid	This marks the particular event that caused the logging to occur. It may be one of the following: ■ 1 = Create ■ 2 = Update ■ 3 = UpdateField ■ 4 = Delete ■ 5 = Login ■ 6 = Logout ■ 7 = LoginReject ■ 8 = FlushAll ■ 9 = FlushUser ■ 10 = FlushUsers ■ 11 = FlushRealms ■ 12 = ChangeDynamicKeys ■ 13 = ChangePersistentKey ■ 14 = ChangeDisabledUserState ■ 15 = ChangeUserPassword ■ 16 = FailedLoginAttemptsCount ■ 17 = ChangeSessionKey	NOT NULL	NUMBER(38)
sm_hostname	This is not used by the reports generator for administrative logging.		VARCHAR2(255)
sm_sessionid	This is the session identifier for this user's activity.		VARCHAR2(255)

Field Name	Description	Null?	Type
sm_username	The username for this administrator.		VARCHAR2(512)
sm_objname	This is the object in the administrator that is being accessed.		VARCHAR2(512)
sm_objoid	This is the unique identifier for the object being accessed in the administrator. This is not used by the reports generator.		VARCHAR2(64)
sm_fielddesc	This is some descriptive text for the action being taken by the administrator.		VARCHAR2(1024)
sm_domainoid	This is the unique identifier for the domain that has an object being modified in the administrator. This is not used by the reports generator.		VARCHAR2(64)
sm_status	This is some descriptive text about the action. This is not used by the reports generator.		VARCHAR2(1024)

Appendix D: Publishing Diagnostic Information

Diagnostic Information Overview

The Policy Server includes a command line tool for publishing diagnostic information about a CA SiteMinder® deployment. Using the tool, you can publish information about Policy Servers, policy stores, user directories, Agents, and custom modules.

Use the Command Line Interface

The Policy Server includes a command that can be executed at the command line to publish information. The command is located in the *installation_dir*/siteminder/bin directory.

To publish information, use smpolicysrv command, followed by the -publish switch. For example:

```
smpolicysrv -publish <optional file_name>
```

Note: On Windows systems, do *not* run the smpolicysrv command from a remote desktop or Terminal Services window. The smpolicysrv command depends on inter-process communications that do not work if you run the smpolicysrv process from a remote desktop or Terminal Services window.

Important! Before running a CA 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.

Specify a Location for Published Information

Published information is written in XML format to a specified file. The specified file name is saved in the following registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\
Publish
```

This key is located in the system registry on Windows systems, and in the *install_dir*/registry/sm.registry file on UNIX. The default value of the registry setting is:

policy_server_install_dir>\log\smpublish.xml

If you execute **smpolicysrv -publish** from a command line, and you do not supply a path and file name, the value of the registry setting determines the location of the published XML file.

Note: On Windows systems, do *not* run the smpolicysrv command from a remote desktop or Terminal Services window. The smpolicysrv command depends on inter-process communications that do not work if you run the smpolicysrv process from a remote desktop or Terminal Services window.

Important! Before running a CA 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.

To specify a location and generate output in an XML file

1. From a command line, navigate to:

   `installation_dir/siteminder/bin`

2. Type the following command:

   `smpolicysrv -publish path_and_file_name`

   For example, on Windows:

   ```
   smpolicysrv -publish c:\netegrity\siteminder\published-data.txt
   ```

   For example, on UNIX:

   ```
   smpolicysrv -publish /netegrity/siteminder/published-data.txt
   ```

   The Policy Server generates XML output in the specified location and updates the value of the HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Publish registry key to match the location you specified.

Published Data

This section outlines the information that may be published for the following:

- Policy Servers
- Policy/Key Stores
- User Directories
- Agents
- Custom Modules

Published Policy Server Information

The Policy Server information includes the server name, platform, configuration, and server versions information. In addition, any registry settings used to configure the Policy Server may be published.

Published Policy Server information includes:

- Basic Information:
  - Name
  - Versioning
  - Platform
  - Thread Pool statistics
- Server Configuration (those values set in the Policy Server Management Console):
  - Key Management
  - Journaling
  - Caching
  - Event Handlers
  - Trace Logging
  - Audit Logging

Published Policy Server XML Output Format

The following example shows how Policy Server information is formatted:

```
<SERVER>
     < SHORT_NAME>   smpolicysrv </SHORT_NAME>
     <FULL_NAME>    SiteMinder Policy Server </FULL_NAME>
     <PRODUCT_NAME> SiteMinder(tm) </PRODUCT_NAME>
     <VERSION>  6.0 </VERSION>
     <UPDATE>   01 </UPDATE>
     <LABEL>    283 </LABEL>
     <PLATFORM> Windows (Build 3790)
    </PLATFORM>
     <SERVER_PORT>     44442 </SERVER_PORT>
     <RADIUS_PORT> 0 </RADIUS_PORT>
     <THREADPOOL>
         <MSG_TOTALS>    15011 </MSG_TOTALS>
         <MSG_DEPTH>     2 </MSG_DEPTH>
         <THREADS_LIMIT> 8 </THREADS_LIMIT>
         <THREADS_MAX>   3 </THREADS_MAX>
         <THREADS_CURRENT> 3 </THREADS_CURRENT>
     </THREADPOOL>
     <CRYPTO> 128 </CRYPTO>
     <KEYMGT>
         <GENERATION> enabled </GENERATION>
         <UPDATE>     disabled </UPDATE>
     </KEYMGT>
     <JOURNAL>
         <REFRESH> 60 </REFRESH>
         <FLUSH>   60 </FLUSH>
     </JOURNAL>
     <PSCACHE>
         <STATE>          enabled </STATE>
         <PRELOAD>        enabled </PRELOAD>
     </PSCACHE>
     <USERAZCACHE>
         <STATE>    enabled </STATE>
         <MAX>      10 </MAX>
         <LIFETIME> 3600 </LIFETIME>
     </USERAZCACHE>
</SERVER>
```

The following table defines the Policy Server information that is published.

TAG	Contains	Description	Parent Tag	Required
SERVER	Elements	Denotes server information	SMPUBLSIH	Required
SHORT_NAME	Text	Abbreviated name of the server	SERVER	Required
FULL_NAME	Text	Full name of the running server	SERVER	Required
PRODUCT_NAME	Text	Name of the Product	SERVER	Required
VERSION	Text	Version of the server	SERVER	Required
UPDATE	Text	Service Pack version	SERVER	Required
LABEL	Text	Build or CR number	SERVER	Required
PLATFORM	Text	OS platform identifying data	SERVER	Required
THREAD_POOL	Elements	Information about the thread pool	SERVER	Required
MSG_TOTAL	Int	Number of thread pool messages handled	THREAD_POOL	Required
MSG_DEPTH	Int	Max number of messages in thread pool	THREAD_POOL	Required
THREADS_LIMIT	Int	Ceiling on number of threads	THREAD_POOL	Required
THREADS_MAX	Int	Max number of threads used	THREAD_POOL	Required
THREADS_CURRENT	Int	Current number of threads used	THREAD_POOL	Required
PSCACHE	Elements	Denotes information on policy server cache settings	SERVER	Required
PRELOAD	Text	Indicates if enabled/disabled	PSCACHE	Required
JOURNAL	Empty,	Indicates the journaling settings, refresh rate and time values to flush	SERVER	Required
FLUSH	Int	Value at which to flush	JOURNAL	Required
REFRESH	Int	Refresh rate	JOURNAL	Required

TAG	Contains	Description	Parent Tag	Required
KEYMGT	Empty,	Indicates Key Management settings (Generation: if automatic key generations is enable) (Update: if automatic updating of agent keys is done.)	SERVER	Required
GENERATION	Enabled or disabled	Enabled or disabled indicates the automatic key generation is enabled	KEYMGT	Required
UPDATE	Enabled or disabled	Indicates that automatic update of agent keys is enabled	KEYMGT	Required
USERAZCACHE	Elements	Information about the User AZ cache settings	SERVER	Required
MAX	Int	Maximum number of cache entries	USERAZCACHE	Required
LIFETIME	int	Life time of cached object	USERAZCACHE	Required
PORT	Int	Port Number	SERVER	Required
RADIUS_PORT	Int	Radius Port number (if enabled)	SERVER	Required
STATE	text, enabled or disabled	Indicates if something is enabled or disabled	Many tags	Various

Published Object Store Information

The Policy Server can store information in the following types of object stores:

- policy store
- key store
- audit log store
- session store

Published object store information includes the type of object store that is being used, back–end database information, configuration, and connection information.

Published Policy/Key Store XML Output Format

The following example shows how policy/key store information is formatted:

```
<POLICY_STORE>

   <DATASTORE>
      <NAME> Policy Store   </NAME>
      <USE_DEFAULT_STORE>  false </USE_DEFAULT_STORE>
      <LOADED> true </LOADED>
      <SERVER_LIST>
         <CONNECTION_INFO>
            <TYPE> ODBC</TYPE>
            <SERVICE_NAME> sm </SERVICE_NAME>
            <USER_NAME> sa </USER_NAME>
            <DBMS_NAME> Microsoft SQL Server </DBMS_NAME>
            <DRIVER_NAME> Microsoft SQL Server </DRIVER_NAME>
            <DBMS_VERSION> 08.00.0760 </DBMS_VERSION>
         </CONNECTION_INFO>
     </SERVER_LIST>
   </DATASTORE>

   <DATASTORE>
      <NAME>  Key Store </NAME>
      <USE_DEFAULT_STORE> true </USE_DEFAULT_STORE>
      <LOADED> true </LOADED>
   </DATASTORE>

   <DATASTORE>
      <NAME> Audit Log Store </NAME>
      <USE_DEFAULT_STORE> true </USE_DEFAULT_STORE>
      <LOADED> true </LOADED>
   </DATASTORE>

   <DATASTORE>
      <NAME> Session Server Store </NAME>
      <USE_DEFAULT_STORE>  false </USE_DEFAULT_STORE>
      <LOADED> false </LOADED>
   </DATASTORE>

</POLICY_STORE>
```

The following table defines the policy/key store information that is published.

TAG	Contains	Description	Parent Tag	Required
POLICY_STORE	Elements	Denotes all the Data Store information	SMPUBLISH	Required
DATASTORE	Elements	Denotes information about a particular Object Store. ■ Type is the type of data store. ■ Use defaults indicates if default objectstore is being used for that type. ■ Loaded indicates if that type is loaded.	POLICY_STORE	Required
NAME	Text	Name/Type of Data Store	DATASTORE	Required
USE_DEFAULT_STORE	Text	Indicates (True/false) if storage is within the default 'Policy Store'	DATASTORE	Required
LOADED	Text	Indicates (true/false) if the data store has been loaded and initialized	DATASTORE	Required
TYPE	Text	Type of policy store, that is, ODBC/LDAP	DATASTORE	Required
SERVER_ LIST	Elements	List of fail over servers used for data store (ODBC)	DATASTORE	Optional
CONNECTION_INFO	Elements	Type of Server Connection	SERVER_LIST	Optional
DRIVER_NAME	Text	Name of the ODBC driver name	CONNECTION	Optional
IP	Text	IP address	DATASTORE	Optional
LDAP_VERSION	Text	LDAP version	DATASTORE	Optional
API_VERSION	Text	LDAP API version	DATASTORE	Optional
PROTOCOL_VERSION	Text	LDAP protocol version	DATASTORE	Optional
API_VENDOR	Text	API Vendor	DATASTORE	Optional

TAG	Contains	Description	Parent Tag	Required
VENDOR_VERSION	Text	Vendor version	DATASTORE	Optional

Published User Directory Information

For each user directory that has been loaded and accessed by the Policy Server, the following information can be published:

- Configuration
- Connection
- Versioning

Published User Directory XML Output Format

The user directory information will be formatted like the following example:

Note: The published information will vary depending on the type of user directory.

```
< USER_DIRECTORIES>

   <DIRECTORY_STORE >
      <TYPE> ODBC </TYPE>
      <NAME> sql5.5sample </NAME>
      <MAX_CONNECTIONS> 15 </MAX_CONNECTIONS>
         <SERVER_LIST>
            <CONNECTION_INFO>
               <TYPE> ODBC</TYPE>
               <SERVICE_NAME> sql5.5sample </SERVICE_NAME>
               <USER_NAME> sa </USER_NAME>
               <DBMS_NAME> Microsoft SQL Server </DBMS_NAME>
               <DRIVER_NAME> Microsoft SQL Server </DRIVER_NAME>
               <DBMS_VERSION> 08.00.0760 </DBMS_VERSION>
            </CONNECTION_INFO>
         </SERVER_LIST>
   </DIRECTORY_STORE >
   <DIRECTORY_STORE>
      <TYPE> LDAP:  </TYPE>
      <NAME> LDAPsample </NAME>
      <FAILOVER_LIST> 172.26.14.101:12002 </FAILOVER_LIST>
      <VENDOR_NAME> Netscape-Directory/4.12 B00.193.0237
      </VENDOR_NAME>
      <SECURE_CONNECTION> disabled </SECURE_CONNECTION>
      <CREDENTIALS>       required </CREDENTIALS>
      <CONNECTION_INFO>
         <PORT_NUMBER> 12002 </PORT_NUMBER>
         <DIR_CONNECTION> 172.26.14.101:12002 </DIR_CONNECTION>
         <USER_CONNECTION> 172.26.14.101:12002 </USER_CONNECTION>
      </CONNECTION_INFO>
      <LDAP_VERSION>     1 </LDAP_VERSION>
      <API_VERSION>      2005 </API_VERSION>
      <PROTOCOL_VERSION> 3 </PROTOCOL_VERSION>
      <API_VENDOR>       mozilla.org </API_VENDOR>
      <VENDOR_VERSION>   500 </VENDOR_VERSION>
   </DIRECTORY_STORE>
</USER_DIRECTORIES>
```

The following table defines the user directory information that will be published.

TAG	Contains	Description	Parent Tag	Required
USER_DIRECTORIES	Elements	Denotes a collection of loaded directory stores	SMPUBLISH	Required
DIRECTORY_STORE	Elements	Denotes a particular directory store.	USER_DIRECTORIES	Optional
TYPE	Text	Type of Directory Store	DIRECTORY_STORE	Required
NAME	Text	Defined name of the Directory store	DIRECTORY_STORE	Required
MAX_CONNECTIONS	Int	Maximum number of connections defined	DIRECTORY_STORE	Optional
SERVER_LIST	Elements	Collection of servers (ODBC)	DIRECTORY_STORE	Optional
FAILOVER_LIST	Text			

Published Agent Information

Published Agent information lists the agents currently connected to policy server, including their IP address and name.

Published Agent XML Output Format

The Agent information will be formatted as in the following example:

```
< AGENT_CONNECTION_MANAGER>
   <CURRENT>      4 </CURRENT>
   <MAX>          4 </MAX>
   <DROPPED>      0 </DROPPED>
   <IDLE_TIMEOUT> 0 </IDLE_TIMEOUT>
   <ACCEPT_TIMEOUT> 10 </ACCEPT_TIMEOUT>

   <AGENT_CONNECTION>
      <NAME> agent1 </NAME>
      <IP>   172.26.6.43 </IP>
      <API_VERSION> 1024 </API_VERSION>
      <LAST_MESSAGE_TIME> 0x05705E0C </LAST_MESSAGE_TIME>
   </AGENT_CONNECTION>
   <AGENT_CONNECTION>
      <NAME> agent1 </NAME>
      <IP>   172.26.6.43 </IP>
      <API_VERSION> 1024 </API_VERSION>
      <LAST_MESSAGE_TIME> 0x05705E0C </LAST_MESSAGE_TIME>
   </AGENT_CONNECTION>
   <AGENT_CONNECTION>
      <NAME> agent1 </NAME>
      <IP>   172.26.6.43 </IP>
      <API_VERSION> 1024 </API_VERSION>
      <LAST_MESSAGE_TIME> 0x05705E0C </LAST_MESSAGE_TIME>
   </AGENT_CONNECTION>
   <AGENT_CONNECTION>
      <NAME> 940c0728-d405-489c-9a0e-b2f831f78c56 </NAME>
      <IP>   172.26.6.43 </IP>
      <API_VERSION> 1482282902 </API_VERSION>
      <LAST_MESSAGE_TIME> 0x05705E0C </LAST_MESSAGE_TIME>
   </AGENT_CONNECTION>
</AGENT_CONNECTION_MANAGER>
```

Note: The Agent connections information is contained within the <AGENT_CONNECTION_MANAGER>tag.

The following table defines the Agent information that will be published.

TAG	Contains	Description	Parent Tag	Required
AGENT_CONNECTION-_MANAGER	Elements	Defines data for the agent connections	SM_PUBLISH	Required
CURRENT	Int	Number of current connections	AGENT_CONNECTION-_MANAGER	Required
MAX	Int	Maximum number of connections	AGENT_CONNECTION-_MANAGER	Required
DROPPED	Int	Maximum number of connections	AGENT_CONNECTION-_MANAGER	Required
IDLE_TIMEOUT	Int	Time after which an idle connection is timed out.	AGENT_CONNECTION-_MANAGER	Required
ACCEPT_TIMEOUT	Int	Time after which an attempted connection is timed out	AGENT_CONNECTION-_MANAGER	Required
AGENT_CONNECTION	Elements	Denotes data about an active agent connection	AGENT_CONNECTION-_MANAGER	Optional
IP	Text	IP address of agent	AGENT_CONNECTION	Required
API_VERSION	Int	Version of the API used by the connected agent	AGENT_CONNECTION	Required
NAME	Text	Name of the agent	AGENT_CONNECTION	Required
LAST_MESSAGE_TIME	Int	Time since last message from agent	AGENT_CONNECTION	Required
AGENT_CONNECTION-_MANAGER	Elements	Defines data for the agent connections	SM_PUBLISH	Required

Published Custom Modules Information

Custom modules are DLLs or libraries that can be create to extend functionality of an existing Policy Server. These come in several types: event handlers, authentication modules, authorization modules, directory modules, and tunneling modules. Authentication modules are generally referred to as custom Authentication schemes and the Authorization modules are known as Active Policies. Tunnel modules are used to define a secure communication with an Agent. Event modules provide a mechanism for receiving event notifications. Information about which custom modules have been loaded by a Policy Server can be published. Each type of custom module is defined in its own XML Tag

Published Custom Modules XML Output Format

The following table defines the custom module information that will be published.

TAG	Contains	Description	Parent Tag	Required
EVENT_LIB	Elements	Indicates data about Event API custom Modules	SMPUBLISH	Optional
AUTH_LIB	Elements	Indicates data about Authentication API custom Modules	SMPUBLISH	Optional
DS_LIB	Elements	Indicates data about Directory API custom Modules	SMPUBLISH	Optional
TUNNEL_LIB	Elements	Indicates data about Tunnel API custom Modules	SMPUBLISH	Optional
AZ_LIB	Elements	Indicates data about Authorization API custom Modules	SMPUBLISH	Optional

There following are common to every type of custom module:

TAG	Contains	Description	Parent Tag	Required
FULL_NAME	Text	Full name of library or DLL include path.		Required
CUSTOM_INFO	Text	Information provided by the custom library.		Optional
LIB_NAME	Text	Library or DLL name		Optional
VERSION	Int	Version of the API supported		Optional

The following are specific to certain types of modules:

TAG	Contains	Description	API Type	Required
ACTIVE_FUNCTION	Text	Name of function loaded to be callable as an active expression	Authorization API	Optional

Appendix E: Error Messages

Authentication

Message	Function	Description
1) Sending a new PIN to ACE/Server for validation.	SmLoginLogoutMessage::Send-NewPinForValidation1	Information only. If you are experiencing problems with your ACE/SecurID authentication scheme(s), please provide this message to Technical Support.
2) Sending a new PIN to ACE/Server for validation %1s	SmLoginLogoutMessage::Send-NewPinForValidation2	Information only. If you are experiencing problems with your ACE/SecurID authentication scheme(s), please provide this message to Technical Support.
Ace Server --- couldn't get PIN policies	SmLoginLogoutMessage::Sm-AuthAceGetPinPoliciesFail	The message is given in the SecurID authentication scheme when ACE server backend PIN policy cannot be retrieved using SecurID/ACE API call.
Ace Server --- couldn't get PIN params	SmLoginLogoutMessage::Sm-AceHtmlPinParamFail	The message is given in the SecurID authentication scheme when ACE PIN parameters cannot be retrieved using SecurID/ACE API call.
ACE State not ACM_NEXT_CODE_REQUIRED. State = %1i	SmLoginLogoutMessage::Ace-NextTokenCodeState	The message in given in HTML SecurID authentication scheme when token code value is expired and the user is required to wait for the next code before attempting a new authentication.
Ace/Server - new PIN is required, AceAPI returned ambiguous value for isselectable PIN attribute. Cannot complete Ace authentication.	SmLoginLogoutMessage::Sm-AceHtmlPinRequired	Information only. If you are experiencing problems with your ACE/SecurID authentication scheme(s), please provide this message to Technical Support.

Message	Function	Description
Ace/Server - new PIN is required, can choose or accept system PIN , returning Sm_AuthApi_Reject, Sm_Api_Reason_New_PIN_ Select.	SmLoginLogoutMessage::Sm-AceHtmlChooseNewOrSysPin	The message is given in the SecurID authentication scheme when ACE user is configured to use either self-chosen or system-generated PIN.
Ace/Server - new PIN is required, Must accept system PIN, returned Sm_Api_Reason_New_PIN_ Sys_Tokencode	SmLoginLogoutMessage::Sm-AceHtmlCannotChoosePin	The message is given in the SecurID authentication scheme when ACE user is configured to always use system-generated PIN.
Ace/Server - new PIN is required, must choose PIN, returning Sm_AuthApi_Reject, Sm_Api_Reason_New_User_-PIN _Tokencode.	SmLoginLogoutMessage::Sm-AceHtmlChooseNewPin	The message is given in the SecurID authentication scheme when ACE user is configured to always use self-chosen PIN.
ACE/Server: ACM_NEW_PIN_ACCEPTED failed with aceRetVal %1i	SmLoginLogoutMessage::Ace-ServerNewPinAcceptedFailed	Used in HTML SecurID authentication scheme. Given when the new user PIN was not accepted by ACE server.
ACE/Server: ACM_NEW_PIN_ACCEPTED failed with aceRetVal %1i, ACE status %2i	SmLoginLogoutMessage::Not-WinAceServerNewPinAccepted-Failed	Used in HTML SecurID authentication scheme. Given when the new user PIN was not accepted by ACE server.
ACE/Server: ACM_NEW_PIN_ACCEPTED failed.	SmLoginLogoutMes-sage::NewPinAcceptedFailed	Used in HTML SecurID authentication scheme. Given when the new user PIN was not accepted by ACE server.
AceCheck Access denied by ACE/Server.	SmLoginLogoutMessage::Ace-CheckAccessDenied	The message is given in the SecurID authentication scheme when authentication request is rejected by ACE server.
AceCheck not processed aceRetVal = %1i	SmLoginLogoutMessage::Ace-CheckNotProcessed	The error message is given in the SecurID authentication scheme if ACE authentication process through the ACE/SecurID API cannot be completed.
AceCheck returned not ACM_NEW_PIN_REQUIRED but %1i	SmLoginLogoutMessage::Acm-NewPinRequiredFail	Information only. If you are experiencing problems with your ACE/SecurID authentication scheme(s), please provide this message to Technical Support.

Message	Function	Description
AceCheck returned not ACM_NEW_PIN_REQUIRED but %1i	SmLoginLogoutMessage::Invalid-ReturnAceCheckNewPin	Information only. If you are experiencing problems with your ACE/SecurID authentication scheme(s), please provide this message to Technical Support.
AceCheck:Denied---aceRetVal = %1i	SmLoginLogoutMessage::Sm-AuthAceCheck-Denial	The message is given in the SecurID authentication scheme when authentication request is rejected by ACE server.
AceGetMaxPinLen failed	#REF!	Used in HTML SecurID authentication scheme. Given when the scheme fails to retrieve max length of user PIN allowed by ACE server.
AceSendPin failed	SmLoginLogoutMessage::Ace-SendPinFailed	The error message is given by HTML SecurID authentication scheme when it fails to send user PIN using to the RSA ACE server ACE/SecurID API. The authentication scheme rejects the request.
AceServer - CANNOT_CHOOSE_PIN	SmLoginLogoutMessage::Ace-ServerCannotChoosePin	Information only. If you are experiencing problems with your ACE/SecurID authentication scheme(s), please provide this message to Technical Support.
AceServer - MUST_CHOOSE_PIN	SmLoginLogoutMessage::Ace-ServerMustChoosePin	Information only. If you are experiencing problems with your ACE/SecurID authentication scheme(s), please provide this message to Technical Support.
AceServer :: Sm_Api_Reason_New_PIN_Select	SmLoginLogoutMessage::Sm-ApiNewPinSelectReason	Information only. If you are experiencing problems with your ACE/SecurID authentication scheme(s), please provide this message to Technical Support.
AceServer returning Sm_Api_Reason_New_PIN_Accepted	SmLoginLogoutMessage::Sm-ApiSuccessReason	Used in HTML SecurID authentication scheme. Given when the user PIN is successfully changed by the user.

Message	Function	Description
AceServer:: returning Sm_AuthApi_Reject Sm_Api_Reason_New_PIN_ Accepted, but not success message can be given, don't know the target.	SmLoginLogoutMessage::Sm-ApiRejectReasonMessage	Information only. If you are experiencing problems with your ACE/SecurID authentication scheme(s), please provide this message to Technical Support.
AceSetPasscode = %1s	SmLoginLogoutMessage::Sm-AuthAceSetPassCode	The message is given when the SecurID authentication scheme is making attempt to register passcode for ACE authentication with ACE/SecurID API.
AceSetPasscode failed with aceRetVal = %1i	SmLoginLogoutMessage::Ace-SetPasscodeFailed	The error message is given by SecurID authentication schemes when it fails to register passcode for ACE authentication with ACE/SecurID API. The authentication scheme rejects the request.
AceSetPin failed	SmLoginLogoutMessage::Ace-SetPinFailed	The error message is given by HTML SecurID authentication scheme when it fails to set user PIN using ACE/SecurID API. The authentication scheme rejects the request.
AceSetSelectionCode DECRYPT = %1s	SmLoginLogoutMessage::-SelectioncodeDecrypt	Information only. If you are experiencing problems with your ACE/SecurID authentication scheme(s), please provide this message to Technical Support.
AceSetUsername failed with aceRetVal = %1i	SmLoginLogoutMessage::Ace-SetUserNameFailed	The message is given by SecurID authentication schemes when it fails to register username for ACE authentication with ACE/SecurID API. The authentication scheme rejects the request.
AddCurrentPWToHistory - Can't set password history info.	SmLoginLogoutMes-sage::ErrorSettingPassword-History	Failed to add current password to the list of most recent passwords.
AuthenticateUserDir - Can't update user blob data	SmLoginLogoutMessage::Blob-UpdateFailed	Failed to update Password Blob Data during Authentication process.
Cannot get AceAlphanumeric	SmLoginLogoutMessage::Get-AceAlphanumericFail	Failed to find method in ACE client library.

Message	Function	Description
Cannot get AceCancelPin	SmLoginLogoutMessage::Get-AceCancelPinFail	Failed to find method in ACE client library.
Cannot get AceCheck	SmLoginLogoutMessage::Get-AceCheckFail	Failed to find method in ACE client library.
Cannot get AceClientCheck	SmLoginLogoutMessage::Get-AceClientCheckFail	Failed to find method in ACE client library.
Cannot get AceClose	SmLoginLogoutMessage::Get-AceCloseFail	Failed to find method in ACE client library.
Cannot get AceGetAuthenticationStatus	SmLoginLogoutMessage::Ace-GetAuthenticationStatusFail	Failed to find method in ACE client library.
Cannot get AceGetMaxPinLen	SmLoginLogoutMessage::Null-AceGetMaxPinLen	Failed to find method in ACE client library.
Cannot get AceGetMinPinLen	SmLoginLogoutMessage::Null-AceGetMinPinLen	Failed to find method in ACE client library.
Cannot get AceGetPinParams	SmLoginLogoutMessage::Get-AcePinParamFail	Failed to find method in ACE client library.
Cannot get AceGetShell	SmLoginLogoutMessage::Ace-GetShellFail	Failed to find method in ACE client library.
Cannot get AceGetSystemPin	SmLoginLogoutMessage::Ace-GetSystemPinFail	Failed to find method in ACE client library.
Cannot get AceGetTime	SmLoginLogoutMessage::Ace-GetTimeFail	Failed to find method in ACE client library.
Cannot get AceGetUserData	SmLoginLogoutMessage::Ace-GetUserDataFail	Failed to find method in ACE client library.
Cannot get AceGetUserSelectable	SmLoginLogoutMessage::Ace-GetUserSelectable-Fail	Failed to find method in ACE client library.
Cannot get AceInit	SmLoginLogoutMessage::Get-AceInitFail	Failed to find method in ACE client library.
Cannot get AceInitialize	SmLoginLogoutMessage::Ace-InitializeFail	Failed to find method in ACE client library.
Cannot get AceLock	SmLoginLogoutMessage::Ace-LockFail	Failed to find method in ACE client library.
Cannot get AceSendNextPasscode	SmLoginLogoutMessage::Ace-SendNextPasscodeFail	Failed to find method in ACE client library.

Message	Function	Description
Cannot get AceSendPin	SmLoginLogoutMessage::Null-AceSendPin	Failed to find method in ACE client library.
Cannot get AceSetNextPasscode	SmLoginLogoutMessage::Ace-SetNextPasscodeFail	Failed to find method in ACE client library.
Cannot get AceSetPasscode	SmLoginLogoutMessage::Ace-SetPasscodeFail	Information only. If you are experiencing problems with your ACE/SecurID authentication scheme(s), please provide this message to Technical Support.
Cannot get AceSetPin	SmLoginLogoutMessage::Null-AceSetPin	Failed to find method in ACE client library.
Cannot get AceSetUserClientAddress	SmLoginLogoutMessage::Ace-SetUserClientAddressFail	Failed to find method in ACE client library.
Cannot get AceSetUsername	SmLoginLogoutMessage::Ace-SetUsernameFail	Failed to find method in ACE client library.
Cannot load aceclnt.dll	SmLoginLogoutMessage::Ace-lntDllLoadFail	Failed to load ACE client library.
Cannot retrieve new password from password message	SmLoginLogoutMessage::New-PasswordRetrieveFail	When processing Login request, and breaking up password for New and Old, failed to retrieve New Password.
Cannot retrieve old password from password message	SmLoginLogoutMessage::Old-PasswordRetrieveFail	When processing Login request, and breaking up password for New and Old, failed to retrieve Old Password.
Cannot retrieve token from password message	SmLoginLogoutMessage::Token-RetrieveFail	When processing Login request, and breaking up password for New and Old, failed to retrieve password token.
ChangePassword - Can't change password via the provider	SmLoginLogoutMessage::Pwd-ChangeFailViaProvider	Failed to change password in User Directory during Change Password request.
ChangePassword - Can't validate the new password	SmLoginLogout-Message::ChangePwdValidation-Fail	Failed to validate password in User Directory during Change Password request.
CheckPasswordPolicies - authentication status changed to failure due to password policy misconfiguration.	SmLoginLogout-Message::CheckPwdFailCause-Misconfig	When checking password policies, failed to validate login attempt. Probably because password policy is misconfigured.

Message	Function	Description
Could not find the Variable to delete %1s	SmLoginLogout-Message::VariableFindErrorTo-Delete	Session Variable flag were passed as part of Request before Session Variable name.
CSmAuthUser - ChangePassword - Can't update user blob data	SmLoginLogoutMes-sage::ChangePwdBlobUpdateFail	Failed to update Password Blob Data during Change Password request.
DelVariable :Internal Error : Could not find the Variable	SmLoginLogoutMessage::Del-VariableFindError	Variable name is empty when trying to delete it from Session Store.
DelVariable Returned Error %1i for Variable %2s	SmLoginLogoutMessage::Del-VariableReturnError	Failed to delete this variable from Session Store.
Did not set AceSetUsername = %1s	SmLoginLogoutMessage::Sm-AuthNotSetUserId	The message is given by SecurID authentication schemes when it fails to register username for ACE authentication with ACE/SecurID API. The authentication scheme rejects the request.
Error finding the name of variable to be deleted %1s:Invalid Index %2i	SmLoginLogout-Message::VariableNameFind-InvalidIndexError	Session Variable flag were passed as part of Request for Session Variable with empty name.
Error in scheme configuration parameter lpszServerParam corrupted.	SmLoginLogoutMessage::Error-SchemeConfigServerParam	Used in SecurID authentication schemes. Same as above.
Error in scheme configuration parameter: Empty String	SmLoginLogoutMessage::Error-SchemeConfigParam	Both basic and form based SecurID authentication schemes require "ACE User ID Attribute Name in Directory" parameter. The error is displayed when this parameter is missing or misconfigured.
Failed to authenticate user '%1s' using scheme '%2s'. Unsupported API version.	SmLoginLogoutMessage::User-AuthFail	Failed to authenticate because of old version of authentication provider library.
Failed to find authentication realm '%1s	SmLoginLogoutMessage::Auth-RealmFindFail	When processing Radius Authentication request, failed to find Realm protected by given Agent / Agent Group.
FindApplicablePassword Policies - error fetching Root	SmLoginLogoutMessage::Error-FetchingApplicablePolicyRoot	Failed to fetch Root object while validating Logging attempt.

Message	Function	Description
FindApplicablePassword Policies - error finding Matching Password Policies	SmLoginLogoutMessage::Error-FindingMatchingPolicies	Failed to fetch PasswordPolicy object while validating Logging attempt.
FindApplicablePassword Policies - No Password Data attribute defined for user dir %1s	SmLoginLogout-Message::PasswordDataAttrib-NotDefined	User Directory that we are using has not defined the appropriate attributes for the blob.
FindApplicablePassword Policies - user or directory is NULL	SmLoginLogoutMessage::Null-ApplicablePwdPolicyDir	Both User and Directory objects are NULL when looking for Applicable Password Polices while validating Logging attempt.
GetRandomPassword - Shortest Length greater than Longest Length	SmLoginLogoutMessage::Long-PwdLength	Created random password exceeds maximum allowed length.
GetRedirect - Can't find applicable password policies.	SmLoginLogoutMessage::Error-FindingPasswordPolicy	Failed to Find Applicable Policies while looking for the first applicable password policy that contains redirect information.
GetRedirect - Can't retrieve password policy.	SmLoginLogoutMessage::Error-RetrievePasswordPolicy	Failed to fetch PasswordPolicy object while validating New Password.
GetVariable : Internal Error:DelVar %1s does not match Var: %2s	SmLoginLogoutMessage::Get-VariableMatchError	Variable to be deleted when fetched, has different names for fetching and deleting.
GetVariable(Del) Returned Error %1i for Variable %2s	SmLoginLogoutMessage::Get-VariableDelReturnError	Failed to delete this variable from Session Store.
GetVariable(Fetch) Returned Error %1i for Variable %2s	SmLoginLogoutMessage::Get-VariableFetchReturnError	Failed to find this variable in Session Store.
GetVariable: Internal Error :Could not find variable	SmLoginLogoutMessage::Get-VariableFindError	Variable name is empty when trying to get Session Variables.
Invalid format for CA SiteMinder® generated user attribute %1s	SmLoginLogoutMessage::Invalid-SmUserAttribFormat	ApplcationRole User property has wrong format.
New PIN was accepted = %1s	SmLoginLogoutMessage::New-PinAccepted	Used in HTML SecurID authentication scheme. Given when the user PIN is successfully changed by the user.

Message	Function	Description
Nonstandard SelectionCode = %1s	SmLoginLogoutMessage::Ace-Server NonStandard-Selectioncode	Information only. If you are experiencing problems with your ACE/SecurID authentication scheme(s), please provide this message to Technical Support.
Passcode not allocated.	SmLoginLogout-Message::Passcode Not-Allocated	Used in SecurID authentication scheme. Failure to allocate buffer for user passcode.
PassCode1 not Allocated	SmLoginLogoutMessage::Mem-Alloc Passcode1Fail	Used in SecurID authentication scheme. Failure to allocate buffer for user passcode.
PassCode1 not Allocated	SmLoginLogout-Message::Passcode 1Not-Allocated	Used in SecurID authentication scheme. Failure to allocate buffer for next user passcode.
PassCode1 not checked, Error = %1i	SmLoginLogoutMes-sage::PassCode 1NotChecked	The error message is given in the SecurID authentication scheme if ACE authentication process through the ACE/SecurID API cannot be completed.
PassCode1 not set, Error = %1i	SmLoginLogoutMessage::Pass-Code 1NotSet	The message is given when the SecurID authentication scheme is making attempt to register passcode for ACE authentication with ACE/SecurID API.
PassCode1 not set, Error = %1i	SmLoginLogoutMessage::Pass-Code 2NotSet	The error message is given by HTML SecurID authentication scheme when it fails to register next passcode for ACE authentication with ACE/SecurID API. The authentication scheme rejects the request.
PassCode2 not Allocated	SmLoginLogoutMessage::Mem-Alloc Passcode2Fail	Used in SecurID authentication scheme. Failure to allocate buffer for user passcode.
PassCode2 not Sent as NextPasscode, Error = %1i	SmLoginLogoutMessage::Pass-Code 2NotSentAsNextPasscode	The error message is given by HTML SecurID authentication scheme when it fails to send next passcode to ACE server through ACE/SecurID API. The authentication scheme rejects the request.

Message	Function	Description
Password Message could not be parsed	SmLoginLogout-Message::Password Message-ParseFail	When processing Login request, and breaking up password for New and Old, failed to parse password string.
PIN allocation failed	SmLoginLogoutMessage::Pin-AllocationFailed	Used in HTML SecurID authentication scheme. Failure to allocate buffer for user PIN.
pszBuf allocation failed	SmLoginLogoutMessage:pszBuf-AllocFail	Used in SecurID authentication scheme. Failure to allocate buffer for RSA SecurID user ID attribute name in CA SiteMinder® user directory.
Returning encrypted System PIN in Cookie via UserMsg %1s	SmLoginLogoutMes-sage::Returning Encrypted-SystemPin	Information only. If you are experiencing problems with your ACE/SecurID authentication scheme(s), please provide this message to Technical Support.
SelectionCode not allocated.	SmLoginLogout-Message::Selection CodeNot-Allocated	Information only. If you are experiencing problems with your ACE/SecurID authentication scheme(s), please provide this message to Technical Support.
Server exception occurred while authenticating user '%1s' using scheme '%2s	'SmLoginLogoutMessage::User-Auth Exception	Unknown error happened during Authentication process. Most likely in authentication provider library.
Server exception occurred while validating authentication for user '%1s	'SmLoginLogoutMessage::Valid-AuthException	Error occurred in advanced password services shared library when called during Authentication process.
Set Username Error = %1i	SmLoginLogoutMessage::Set-UserNameError	The message is given by SecurID authentication schemes when ti fails to register username for ACE authentication with ACE/SecurID API. The authentication scheme rejects the request.
SetVariable :Internal Error: Could not find Variable	SmLoginLogoutMessage::Set-VariableFindError	Variable name is empty when trying to set it into Session Store.
SetVariable :Internal Error: NULL Value found for Variable %1s	SmLoginLogoutMessage::Set-VariableNullValueFound	Variable value is empty when trying to set it into Session Store.

Message	Function	Description
SetVariable Returned Error %1i for Variable %2s	SmLoginLogoutMessage::Set-VariableReturnError	Failed to add/update this variable into Session Store.
SmAuthenticate: AceInitialization failed	SmLoginLogoutMessage::Sm-AuthAceInitFail	Failed to Initialize ACE client library.
SmAuthenticate: Cannot create Event.	SmLoginLogoutMessage::Create-EventFail	Used in SecurID authentication scheme. Failure to create event object in SecurID authentication scheme.
SmAuthenticate: Couldn't get allocate memory for PIN	SmLoginLogoutMessage::Sm-AceHtmlPinMemAllocFail	Used in SecurID authentication scheme. Failure to allocate buffer for ACE system-generated PIN.
SmAuthenticate: Did not set AceSetPasscode = %1s	SmLoginLogoutMessage::Sm-AuthAceDidNotSetPassCode	The error message is given by SecurID authentication schemes when it fails to register passcode for ACE authentication with ACE/SecurID API. The authentication scheme rejects the request.
SmAuthenticate: No numeric value found for SM_ACE_FAILOVER_ATTEMPTS environment variable, proceeding with default value.	SmLoginLogoutMessage::Zero-SmAuthAceFailover	To support RSA ACE/SecurID failover, CA SiteMinder® Policy Server has an environment variable SM_ACE_FAILOVER_ATTEMPTS. By default, it set to 3. The error message is given when the value of SM_ACE_FAILOVER_ATTEMPTS is 0. In this case RSA ACE/SecurID failover may not work properly with CA SiteMinder®.
SmAuthenticate:Cannot allocate storage for EventData	SmLoginLogoutMessage::Event-DataMemAllocFail	Used in SecurID authentication scheme. Failure to allocate memory for RSA SecurID API structure.
SmAuthenticate:Cannot proceed to AceInit--NOT ACE_PROCESSING. aceRetVal= %1i	SmLoginLogoutMessage::Sm-AuthAceInitProcessingFail	The message is given by SecurID authentication schemes when it fails to initialize ACE/SecurID API. The authentication scheme rejecting the request and the authentication fails.
SmAuthenticate:Did not continue to AceCheck. aceRetVal= %1i	SmLoginLogoutMessage::Sm-AuthAceCheckDidNotContinue	The error message is given in the SecurID authentication scheme if ACE authentication process through the ACE/SecurID API cannot be completed.

Message	Function	Description
SmAuthenticate:Did not continue to AceInit completion. pEventData->asynchAceRet= %1i	SmLoginLogoutMessage::Sm-AuthAceInitCompletionFail	The message is given by SecurID authentication schemes when it fails to initialize ACE/SecurID API. The authentication scheme rejecting the request and the authentication fails.
SmAuthenticate:Name Lock Request has been denied by ACE/Server communication failure.	SmLoginLogoutMessage::Sm-AuthNameLockReqDenied	The message is given by SecurID authentication schemes when it fails to initialize ACE/SecurID API. The authentication scheme rejecting the request and the authentication fails.
SmAuthenticate:Thread Sync failed. wRet= %1ul	SmLoginLogoutMessage::Sm-AuthThreadSyncFail	The message is given on Windows platform by SecurID authentication schemes when the call to asynchronous ACE API call fails.
SmAuthenticate:Unable to Lock the UserName. aceRetVal= %1i	SmLoginLogoutMessage::Sm-AuthUserNameLockFail	The message is given by SecurID authentication schemes when it fails to lock username for ACE server. In this case CA SiteMinder® authentication scheme rejects the authentication requests. The name lock feature is available in RSA ACE product of version 5.0 and above.see RSA ACE product documentation for additional information on name lock feature.
SmAuthUser - Failed to fetch Az Realm.	SmLoginLogoutMessage::Fetch-AzRealmFailed	Failed to find user Realm when getting Application Role User property.
SmAuthUser - Failed to fetch Domain object.	SmLoginLogoutMessage::Fetch-DomainObjFailed	Failed to find user Domain when getting Application Role User property.
The new PIN can contain alpha-numeric characters only.	SmLoginLogoutMessage::Alpha-NumericOnlyNewPin	The message is used in HTML SecurID authentication scheme when user was required to change a PIN, and user enters a PIN that contains non-alphanumeric characters.
The new PIN can contain digits only.	SmLoginLogoutMessage::Digit-OnlyNewPin	The message is used in HTML SecurID authentication scheme when user was required to change a PIN, and user enters a PIN that contains non-digits.

Message	Function	Description
The new PIN is too long	SmLoginLogoutMessage::Long-New Pin	The message is used in HTML SecurID authentication scheme when user was required to change a PIN and a new PIN is too long.
The new PIN is too short	SmLoginLogoutMessage::Short-New Pin	The message is used in HTML SecurID authentication scheme when user was required to change a PIN and a new PIN is too short.
Unable to proceed PIN change, unknown PIN type.	SmLoginLogoutMessage::Ace-Server UnableToProceedPin-Change	Information only. If you are experiencing problems with your ACE/SecurID authentication scheme(s), please provide this message to Technical Support.
Unexpected Message ID found while looking for SmPasswordMsg_Change Password: %1ul	SmLoginLogout-Message::Unexpect edMessage-ID	When processing Login request, and breaking up password for New and Old, message ID stored in password field is unknown.
Usage: %1s[:AppName]	SmLoginLogoutMessage::Usage-Sm UserAttribFormat	Help string for correct Application Role User property formatting.
UserPIN not allocated.	SmLoginLogoutMessage::User-PinN otAllocated	Used in SecurID authentication scheme. Failure to allocate buffer for user PIN.
ValidateLoginAttempt - Error Applying Password Policy	SmLoginLogoutMessage::Error-Appl yingPasswordPolicy	Failed when tried to Apply Password Policy while validating Logging attempt.
ValidateLoginAttempt - Error Fetching Password Policy	SmLoginLogoutMessage::Error-Fetc hingPasswordPolicy	Failed to fetch PasswordPolicy object while validating Logging attempt.
ValidateLoginAttempt - Error Finding Applicable Policies	SmLoginLogoutMessage::Error-Findi ngApplicablePolicy	Failed to Find Applicable Policies while validating Logging attempt.
ValidateNewPassword - Can't set password change info.	SmLoginLogoutMessage::Error-Pass wordChange	Failed to set password info while trying to Update Password Blob Data.
ValidateNewPassword - Error fetching Match regular expressions	SmLoginLogoutMessage::Match-Exp rFetchError	Failed to get the desired regular expressions for the password policy.
ValidateNewPassword - Error fetching NoMatch regular expressions	SmLoginLogoutMessage::No-Match ExprFetchError	Failed to get the desired regular expressions for the password policy.
ValidateNewPassword - Error fetching password policy	SmLoginLogoutMessage::Err-Fetchi ngValidPwdPolicy	Failed to fetch PasswordPolicy object while validating New Password.

Message	Function	Description
ValidateNewPassword - Error finding applicable password policies.	SmLoginLogoutMessage::Err-Finding ValidPwdPolicy	Failed to Find Applicable Policies while validating New Password.
ValidateNewPassword could not load callout '%1s	'SmLoginLogoutMessage::Load-Call outFail	Failed to Load external library to check password.
ValidateNewPassword failed to resolve function '%1s' in '%2s'. Error: %3s	SmLoginLogoutMessage::Err-Resolv eFuncValidPwd	Failed to find method in external library to check password.

Authorization

Error Message	Function	Description
Bad %1s request detected	SmIsAuthorizedMessage::Bad-Request Detected	The Authorization Request message failed to conform to the proper format.
Cannot process active expression with variables without licensed eTelligent Options	SmIsAuthorizedMessage::CanNot-Proc essActiveExpr	The license for the eTelligent Rules feature is not found. The Active Expression will not be processed.
Caught exception while adding variable	SmIsAuthorizedMessage::Exc-AddingV ar	A software exception was raised while resolving eTelligent Rules variables.
Exception in IsOk.	SmIsAuthorizedMessage::Unk-ExcInIsO K	An unknown exception occurred while performing an Authorization.
Exception in IsOk. %1s	SmIsAuthorizedMessage::ExcIn-IsOK	An exception occurred while performing an Authorization.
Failed to Fetch Active Expression %1s	SmIsAuthorizedMessage::Failed-Fetch ActiveExpr	Could not fetch the Active Expression object from the object store.
Failed to Load Active Expression %1s	SmIsAuthorizedMessage::Failed-LoadA ctiveExpr	The Active Expression could not be loaded.
Failed to Load Domain %1s	SmIsAuthorizedMessage::Failed-LoadD omain	Failed to retrieve the Domain object during eTelligent Rules variable processing.

Error Message	Function	Description
Failed to Load Variable %1s	SmIsAuthorizedMessage::Failed-LoadVar	Failed to get the specified eTelligent Rules variable.
Failed to Load Variable Type %1s	SmIsAuthorizedMessage::Failed-LoadVarType	Failed to get the type of the specified variable.
Failed to Load Variables for Active Expression %1s	SmIsAuthorizedMessage::Failed-LoadVarActiveExpr	There was a problem resolving Variables, therefore the Active Expression will not be invoked.
Failed to Load Variables for active expression %1s	SmIsAuthorizedMessage::Failed-LoadVarsForActiveExpr	Failed to load eTelligent Rules Variables for an Active Expression
Failed to resolve attribute %1s	SmIsAuthorizedMes-sage::FailedToResolveAttr	Could not fetch the Response Attribute object from the object store.
Failed to resolve dictionary vendor attribute %1s	SmIsAuthorizedMes-sage::FailedToResolveDictVendAttr	Could not find the specified Vendor Attribute in the Vendor Attribute Dictionary.
Failed to resolve response %1s	SmIsAuthorizedMes-sage::FailedToResolveResponse	Could not fetch the Response object from the object store.
Failed to resolve response group %1s	SmIsAuthorizedMes-sage::FailedToResolveResponseGp	Could not fetch the Response Group object from the object store.
Failed to resolve user policy %1u	SmIsAuthorizedMes-sage::FailedToResolveUserPolicy	Could not fetch the User Policy object from the object store.
Ignoring variable response - no license for eTelligent Options	SmIsAuthorizedMessage::No-eTelligentLicense	The license for the eTelligent Rules feature was not found. Variables will not be processed.
Invalid response attribute %1s. Dictionary conflict - attribute may not be in the response	SmIsAuthorizedMessage::Invalid-ResponseAttr	An invalid Response Attribute was not included in the Authorization response.
IsOk failed. %1s	SmIsAuthorizedMessage::IsOK-Failed	The Authorization check failed

Server

Message	Function	Description
Failed to initialize TCP server socket: Socket error:%1i	SmServerMessage::TCP-ServerSocketInitFail	see the operating system documentation for the specifics of the socket error. (The most common errors are attempting to open a socket already in use on the system or not having sufficient privilege for the socket.)
Failed to initialize UDP server socket on port: %1ul. Socket error:%2i	SmServerMessage::UDP-ServerSocketInitFailOnPort	see the operating system documentation for the specifics of the socket error. (The most common errors are attempting to open a socket already in use on the system or not having sufficient privilege for the socket.)
Failed to initialize WinSock library	SmServerMessage::WinSock-LibInitFail	(Windows systems.) The Windows Sockets library could not be initialized. Verify the library is installed and that its version is supported.
Failed to listen on TCP server socket. Socket error %1i	SmServerMessage::TCP-ServerSocketListenFail	see the operating system documentation for the specifics of the socket error. (The most common errors are attempting to open a socket already in use on the system or not having sufficient privilege for the socket.)
Failed to load event handler	SmServerMessage::Event-HandlerLoadFail	An Event Handler library could not be loaded. Verify the pathnames and access permissions of the configured Event Handlers.
Failed to load library '%1s'. Error: %2s	SmServerMessage::FailedTo-LoadLib	The reported Authentication Scheme library could not be loaded. If the accompanying error text does not explain the problem, verify that the named library exists and that the file system protections allow access.

Message	Function	Description
Failed to locate required entry point(s) in event provider '%1s'	SmServerMessage::Req-EntryPointInEventProvider-LocateFail	The named library is not a valid Event/Audit Log provider.
Failed to write audit log record. Record dropped.	CSmReports::LogAccess	The Policy Server could not write to the audit log. Verify the status of the audit log store.
Failed to obtain host name. Socket error %1i	SmServerMessage::Host-NameObtainError	The Audit Logger provider could not retrieve the local system's network hostname, probably due to a network error. The accompanying error code (an errno for UNIX systems, a SOCKET_ERROR for Windows systems) may provide more detail.
Failed to obtain host name. Socket error %1i	SmServerMessage::Host-NameObtainFail	The local system's network hostname could not be retrieved, probably due to a network error. The accompanying error code (an errno for UNIX systems, a SOCKET_ERROR for Windows systems) may provide more detail.
Failed to open Audit log file for append '%1s'	SmServerMessage::Audit-LogFileAppendFail	The Audit Logger provider could not open the named file for appending entries. Verify that the pathname provided is valid and that file access permissions are correct.
Failed to open RADIUS log file (no file defined)	SmServerMessage::Radius-LogFileNotDefined	The registry does not have an entry for the RADIUS log file's name, or the name was an empty string,
Failed to open RADIUS log file: %1s	SmServerMessage::Radius-LogFileOpenFail	A RADIUS log file with the given name could not be opened for overwriting (if it already exists) or be created (if it does not exist). Check access permissions to the directory and to the file (if it exists).

Message	Function	Description
Failed to query authentication scheme '%1s'	SmServerMessage::Fail-QueryAuthScheme	The Policy Server's query of the given Authentication Scheme failed, so the Authentication Scheme could not be initialized.
Failed to read on UDP socket. Socket error %1i	SmServerMessage::UDP-SocketReadFail	The Policy Server detected an unexpected network error while trying to read a UDP packet carrying either an Admin service connection request or a RADIUS message. The accompanying error code (an errno for UNIX systems, a SOCKET_ERROR for Windows systems) may provide more detail.
Failed to receive request on session # %1i : %2s/%3s:%4i. Socket error %5s	SmServerMessage::Request-ReceiveOnSessionFail	The Policy Server detected an unexpected network error while trying to read the agent request in the given session, so it closed the connection. The accompanying error code (an errno for UNIX systems, a SOCKET_ERROR for Windows systems) may provide more detail.
Failed to resolve agent key '%1s'	SmServerMessage::Unresolved-AgentKey	The reported Agent Key could not be found in the Policy Store when Agent Keys were being updated.
Failed to resolve agent keys	SmServerMessage::FailTo-ResolveAgentKeys	No Agent keys could be accessed in the Policy Store for Agent Key Update.
Failed to resolve agent keys	SmServerMessage::Agent-KeysResolveFail	No Agent keys could be accessed in the Policy Store for Agent Key Update.
Failed to resolve agent keys '%1s'	SmServerMessage::Fail-ToResolveAgentKey	The reported Agent Key could not be found in the Policy Store when Agent Keys were being updated.
Failed to resolve Agent or AgentGroup %1s	SmServerMessage::Agent-OrAgentGroupResolveFail	The given Agent or Agent Group does not exist or its Policy Store record has become corrupted.

Message	Function	Description
Failed to resolve all domains	SmServerMessage::Domain-ResolutionFailed	The Domain root object record in the Policy Store is missing or has become corrupted.
Failed to resolve all vendors. No vendor dictionary will be created.	SmServerMessage::Failed-ToResolveVendors	The Vendors root object record in the Policy Store is missing or has become corrupted.
Failed to resolve auth-az mapping %1s	SmServerMessage::Fail-ToResolveAuthAzMap	The given Auth-Az Map does not exist or its Policy Store record has become corrupted.
Failed to resolve function '%1s' in '%2s' . Error: %3s	SmServerMessage::Failed-ToResolveFunc	The reported entry point in the given Authentication Scheme library could not be resolved (see the accompanying error text), so the library was not loaded.
Failed to resolve function '%1s' in '%2s'. Error: %3s	SmServerMessage::Function-ResolveFail	The reported entry point in the given TransactEMS library could not be resolved (see the accompanying error text), so the library was not loaded.
Failed to resolve function '%1s' in '%2s'. Error: %3s	SmServerMessage::Fail-ToResolveFunction	The reported entry point in the given library which reports system configuration information could not be resolved (see the accompanying error text), so the library was not loaded.
management object	SmServerMessage::Key-ManagementObjResolveFail	The Policy Server detected an error when it attempted to read the Key Management Object from the Policy Store.
Failed to resolve key management object	SmServerMessage::Resolve-KeyMgmtObjFail	The Agent Key Management Object could not be read from the Policy Store.
Failed to resolve key management object '%1s'	SmServerMessage::Key-ManagementObjResolve-FailwithVal	The Agent Key Management Thread detected an error when it attempted to read the given Agent Key Management Object from the Policy Store.

Message	Function	Description
Failed to resolve list of auth-az mappings	SmServerMessage::Fail-ToResolveAuthAzMapList	The Auth-Az Map root object record in the Policy Store is missing or has become corrupted.
Failed to resolve log file name	SmServerMessage::Log-FileNameResolveFail	The Audit Logger provider could not retrieve the name for the log file from the registry. Verify that a file name has been configured.
Failed to resolve shared secret policy object	SmServerMessage::Shared-SecretResolveFail	The Shared Secret Rollover Policy object record in the Policy Store is missing or has become corrupted.
Failed to resolve user directory %1s	SmServerMessage::Fail-ToResolveUserDir	The given User Directory object does not exist or its Policy Store record has become corrupted.
Failed to resolve user identity. Denying access.	SmServerMessage::User-IdentityFail	Because there was a failure while searching the policies of the applicable realms, the user's identity could not be resolved and access was denied.
Failed to resolve Version 6 function '%1s' in '%2s' . Error: %3s	SmServerMessage::Failed-ToResolveVer6Func	The reported entry point in the given Version 6 Authentication Scheme library could not be found (see the accompanying error text), so the library will not be used. Verify that the Auth Scheme is not an older version.
Failed to retrieve audit log flush interval. Setting to infinite	SmServerMessage::Audit-LogFlushIntervalRetrieveFail	The Audit Logger ODBC provider could not retrieve the flush interval from the registry. Verify that an interval has been configured.
Failed to retrieve audit log provider library for namespace '%1s'	SmServerMessage::AuditLog-ProviderLibRetrieveFail	The registry does not have a library name entry for the given Audit Log Provider namespace.
Failed to retrieve audit log row flush count. Setting to 1000	SmServerMessage::Audit-LogRowFlushCountRetrieveFail	The registry does not have an entry for the ODBC Audit Log Provider's row flush count for asynchronous logging, so the default of 1000 will be used.

Message	Function	Description
Failed to retrieve message from the message queue	SmServerMessage::Retrieve-FromMessageQueueFail	(Windows) An error occurred when the Policy Server process attempted to retrieve a message on its Windows Application Queue.
Failed to rollover trusted host shared secrets	SmServerMessage::Trusted-HostSharedSecretsRolloverFail	An error occurred while attempting to roll over trusted host shared secrets. Verify that the rollover policy is valid.
Failed to save key management object	SmServerMessage::Save-NewMgmtKeyObjFail	The Agent Key Management Object could not be read from the Policy Store when a new Persistent Key was to be saved.
Failed to save key management object after key update	SmServerMessage::Save-NewMgmtKeyObjAfter-KeyUpdateFail	The Policy Server generated new Agent Keys for roll over but could not record that they are available for use.
Failed to save key management object after persistent key update	SmServerMessage::Save-NewMgmtKeyObjAfter-PersistentKeyUpdateFail	The new Persistent Key could not be saved in the Agent Key Management Object in the Policy Store.
Failed to save key management object after session key update	SmServerMessage::Save-NewMgmtKeyObjAfterSession-KeyUpdateFail	The new Agent Session Key could not be saved in the Policy Store.
Failed to save new 'current' agent key '%1s'	SmServerMessage::Save-NewCurrentAgentKeyFail	The given Agent Session Key could not be saved as the Agent's "current" key.
Failed to save new key management object	SmServerMessage::Agent-KeyManagementObjSaveFail	The Agent Key management thread generated new Agent Keys for roll over but could not record that they are available for use.
Failed to save new 'last' agent key '%1s'	SmServerMessage::Save-NewLastAgentKeyFail	The given Agent Session Key could not be saved in the Policy Store as the Agent's "last" key.
Failed to save new 'next' agent key '%1s'	SmServerMessage::Save-NewNextAgentKeyFail	The given Agent Session Key could not be saved in the Policy Store as the Agent's "next" key.
Failed to save new persistent agent key '%1s'	SmServerMessage::Failed-ToSaveNewPersistentAgentKey	The given Persistent Agent Key could not be saved in the Policy Store.

Message	Function	Description
Failed to send response on session # %1i : %2s/%3s:%4i. Socket error %5i	SmServerMessage::Response-SendOnSessionFail	The response to an agent request in the given session could not be sent due to a network error (or possibly the Agent failing). The accompanying error code (an errno for UNIX systems, a SOCKET_ERROR for Windows systems) may provide more detail.
Failed to start agent command management watchdog thread	SmServerMessage::Agent-CommandManagementThread-CreationFail	The "watchdog" thread which ensures that the Agent Command Management Thread is running failed to start. Check the operating system's configured per-process limits for maximum number of threads and for maximum open file descriptors.
Failed to start journal management thread	SmServerMessage::Journal-ThreadCreateFail	The "watchdog" thread could not [re-]start the Policy Store Journal Cleanup Management Thread. Check the operating system's configured per-process limits for maximum number of threads and for maximum open file descriptors.
Failed to start journal management watchdog thread	SmServerMessage::Journal-ManagementThreadFail	The "watchdog" thread which ensures that the Policy Store Journal Management Cleanup Thread is running failed to start. Check the operating system's configured per-process limits for maximum number of threads and for maximum open file descriptors.
Failed to start key management thread	SmServerMessage::AgentKey-ThreadCreateFail	The "watchdog" thread could not [re-]start the Agent Key Management Thread. Check the operating system's configured per-process limits for maximum number of threads and for maximum open file descriptors.

Message	Function	Description
Failed to start key management watchdog thread	SmServerMessage::Key-ManagementThreadCreateFail	The "watchdog" thread which ensures that the Agent Key Management Thread is running failed to start. Check the operating system's configured per-process limits for maximum number of threads and for maximum open file descriptors.
Failed to start main reactor thread	SmServerMessage::Main-ReactorThreadStartFail	The Network IO Dispatcher Thread failed to start. Check the operating system's configured per-process limits for maximum number of threads and for maximum open file descriptors.
Failed to start object store journal thread	SmServerMessage::Journal-StartFailed	The "watchdog" thread could not [re-]start the Policy Store Journal Management Thread. Check the operating system's configured per-process limits for maximum number of threads and for maximum open file descriptors.
Failed to start object store watchdog thread	SmServerMessage::Watchdog-Failed	The "watchdog" thread which ensures that the Policy Store Journal Management Thread is running failed to start. Check the operating system's configured per-process limits for maximum number of threads and for maximum open file descriptors.
Failed to stat management command channel	SmServerMessage::Stat-MangmCmdChannelFail	(Unix/Linux) The stat() of an already-existing Server Command Management pipe/file unexpectedly failed. If also the Server Command Management Thread fails to start, verify that another Policy Server process is not running and delete the pipe/file manually.
Failed to update agent keys	SmServerMessage::FailTo-UpdateAgentKeys	The Administrator command that Agents update their keys could not be saved in the Policy Store.

Message	Function	Description
Failed to update agent keys from server command	SmServerMessage::Failed-ToUpdate AgentKeys	An Agent's new "current" or "next" Session Key could not be saved in the Policy Store.
Failed to update changes agent keys	SmServerMessage::Fail-ToUpdateCh angesToAgentKeys	The command that Agents update their keys could not be saved in the Policy Store.
Failed to update persistent key	SmServerMessage::Failed-ToUpdate PersistentKey	An Agent's Persistent Key could not be saved in the Policy Store.
Failed to write on UDP socket. Socket error %1i	SmServerMessage::UDP-SocketWrit eFail	An Admin GUI initialization packet or a RADIUS response packet could not be sent due to a network error (or possibly the Agent failing). The accompanying error code (an errno for UNIX systems, a SOCKET_ERROR for Windows systems) may provide more detail.
file not found	SmServerMessage::File-NotFound	(Windows systems.) The service to start the One View Monitor could not read the bin\smmon.bat file.
Getting processor affinity failed	SmServerMessage::Get-ProcessorAff inityFail	(Windows) The performance tuning parameter for processor affinity could not be processed, so the existing affinity setting will be unchanged.
Handshake error: Unknown client name '%1s' in hello message	SmServerMessage::Handshake-Error UnknownClient	A client provided the reported name when attempting to connect, but an Agent with that name could not be found in the Policy Store. Also caused by the agent using the wrong shared secret.
Inconsistent agent key marker (%1i)	SmServerMes-sage::InconsistentAge nt-KeyMarker	An Agent Key record in the Policy Store has the given unrecognized key type.
Inconsistent number of agent keys (%1i)	SmServerMes-sage::InconsistentNu mberOf-AgentKeys	The Policy Store contains the given incorrect number of keys for an Agent.

Message	Function	Description
Internal error computing realm list. Denying access.	SmServerMessage::Realm-Corrupt	An unexpected Policy Store failure occured while attempting to fetch the realm list to perform access authorization, so access is denied.
Invalid agent key marker (%1i)	SmServerMessage::Invalid-AgentKeyMarker	An Agent Key record in the Policy Store has the given unrecognized key type.
IP address resource filter not yet suppported by IsOk	SmServerMessage::IPAddr-ResourceFilterNotSupported	Action rules matching in realms does not support matching IP addresses or ranges.
IsInDictionary - Could not add Password Dictionary to holder %1s	SmServerMessage::Add-PasswordDictToHolderFailed	The named password dictionary could not be cached, probably because no more than 100 dictionaries may be cached. Passwords to be matched against entries in the dictionary are assumed to match.
IsInDictionary - Could not create Password Dictionary %1s	SmServerMessage::Create-PasswordDictFailed	An unexpected error (probably an out-of-memory condition) occurred while preparing to cache the named password dictionary. Passwords to be matched against entries in the dictionary are assumed to match.
IsInDictionary - Could not set the Password Dictionary %1s	SmServerMessage::Set-PasswordDictFailed	An error occurred while caching the named password dictionary. Passwords to be matched against entries in the dictionary are assumed to match.
IsInDictionary - Password Dictionary not open %1s	SmServerMessage::Open-PasswordDictFailed	The given password dictionary has been loaded but unexpectedly is not open. Passwords to be matched against entries in the dictionary are assumed to not match.

Message	Function	Description
IsInProfileAttributes - Error fetching property names	SmServerMessage::Fetching-PropertyNameFail	While comparing a password to user profile attribute values, the user attribute names could not be retrieved, so the password is assumed to match.
IsInProfileAttributes - Error fetching property values	SmServerMessage::Fetching-PropertyValueFail	While comparing a password to user profile attribute values, an attribute value could not be retrieved, so the password is assumed to match.
Monitor request for unrecorded data, Null values returned	SmServerMessage::MonReq-UnrecordedDataNullValue	The Policy Server did not recognize the name passed it in a request for monitored data.
No agent encryption keys found	SmServerMessage::Agent-EncryptionKeyNotFound	When an Agent's set of keys was fetched from the Policy Store, a complete set was not found.
No agent keys in key store	SmServerMessage::AgentKey-NotFoundInKeyStore	While attempting to update the Agent Keys in the Policy Store, none were found.
No initial agent keys	SmServerMessage::Empty-AgentKeys	The Policy Store holds no Agent Keys and Key Generation has not been enabled.
No initial key management object found. This policy server is configured in read-only key management mode. Unable to proceed	SmServerMessage::Key-ManagementObjNotFound	The Policy Store does not hold an initial Agent Key Management object and Key Generation has not been enabled.
No namespace available for the audit log provider	SmServerMessage::No-NamespaceAvailForAudit-LogProvider	The registry does not have an entry for the Audit Log Provider namespace.
No Root Config object found, Please run smobjimport to import smpolicy.smdif!	SmServerMessage::Root-ConfigObjNotFound	The Policy Store has not been successfully initialized.
No session pointer while processing request %1s	SmServerMessage::Null-SessionPointer	The given Agent request was received but the corresponding Agent Session object was not found or valid, so the request packet was returned without processing.

Message	Function	Description
Please check file permissions or path for validity	SmServerMessage::File-PermissionOrPathCheck	A file could not be opened. An error message giving the file's path name should precede this message.Verify that the pathname provided is valid and that file access permissions are correct.
Policy Server caught exception in ProcessMessage. (no message text)	SmServerMessage::Unknown-PolSrvExcpCaught	The Policy Server had an unexpected exception while processing an Agent request, so an empty response was returned.
Policy Server caught exception in ProcessMessage. Text: %1s	SmServerMessage::PolSrv-ExcpCaught	The Policy Server had an unexpected exception while processing an Agent request, so an empty response was returned. The accompanying text may recommend corrective action.
Policy store failed operation '%1s' for object type '%2s' . %3s	SmServerMessage::Policy-StoreOperFail	The Policy Store object layer caught the described exception.
Processor affinity left at default setting, cannot set affinity to zero	SmServerMessage::Processor-AffinitySetZeroFail	(Windows) Zero is an invalid value for the performance tuning parameter for processor affinity, so the existing affinity setting will be unchanged.
Reject %1s : Failed to write access log	SmServerMessage::Write-FailInAccessLog	Audit logging failed for the given rejected Authentication or Authorization request.
Saw agent name in DoManagement() command %1s, request %2s	SmServerMessage::Agent-NameInDoManagement	The "Do Management" Agent command was rejected.
Saw agent name in Logout() command %1s , request %2s	SmServerMessage::Agent-NameInLogout	The Logout request was rejected.
Setting processor affinity failed	SmServerMessage::Set-ProcessorAffinityFail	(Windows) The performance tuning parameter for processor affinity could not be processed, so the existing affinity setting will be unchanged.

Message	Function	Description
SM exception caught during initialization (%1s)	SmServerMessage::SMExcp-DuringInit	During the Policy Server startup "GlobalInit" phase, an exception was caught and startup failed. The accompanying text may provide more detail.
SM exception caught during server shutdown (%1s)	SmServerMessage::SMExcp-DuringServerShutdown	During the Policy Server shutdown "GlobalRelease" phase, an exception was caught. The accompanying text may provide more detail.
TCP port initialization failure	SmServerMessage::TCP-PortInitFail	During Policy Server startup the TCP ports enabled for Access Control or Administration requests could not be initialized, so startup was terminated.
The service loader failed to start %1s. Error %2i %3s	SmServerMes-sage::SZSERVER_StartFail	(Windows) The service loader could not be started (see error text), so it could not start the Policy Server or One View Monitor.
This policy server does not have a session encryption key	SmServerMessage::Session-EncryptKeyNotFound	The Policy Server does not have an initial Session Key and Key Generation is not enabled. If Access Control Requests or Administration Requests are configured to be served, startup is terminated.
Thread Pool thread caught exception	SmServerMessage::ExcpIn-ThreadPool	A Policy Server Worker Thread terminated due to an unexpected condition. A replacement thread will be added to the Thread Pool.
UDP port initialization failure	SmServerMessage::UDPPort-InitFail	During Policy Server startup the UDP ports enabled for Administration or RADIUS requests could not be initialized, so startup was terminated.
UDP processing exception.	SmServerMessage::UDP-ProcessingExcp	While an Admin GUI initialization packet or a RADIUS response packet was being processed an unexpected error occurred. No response is sent.

Message	Function	Description
Unable to create console output collector. Tracing will not be enabled	SmServerMessage::Trace-NotEnableConsoleOutput-CollecCreateFail	The Policy Server process could not access the console (or terminal window) as output for the Profiler (trace) log output. Verify that it has appropriate access permission to open the console.
Unable to create file output collector. Tracing will not be enabled	SmServerMessage::Trace-NotEnableFileOutput-CollecCreateFail	A Profiler (trace) log file could not be opened for overwriting (if it already exists) or be created (if it does not exist). Check access permissions to the directory and to the file (if it exists).
Unable to create shared secret rollover policy object	SmServerMessage::Shared-SecretCreateFail	During Policy Server startup no Shared Secret policy object was found in the Policy Store, then creation of an initial policy object failed so startup was terminated.
Unable to enable tracing	SmServerMessage::Trace-NotEnable	The initial setup of Profiler (trace) logging was successful but the remainder was not.
Unable to reset logger options dynamically	SmServerMessage::Dynamic-LoggerResetFail	The thread which detects that logger configuration options were changed while the Policy Server is running could not start, so such changes will not be acted upon unil the Policy Server has been restarted.
Unable to resolve agent for request %1s	SmServerMessage::Unresolved-AgentIdentity	The Agent request is required to include the Agent identity but it could not be verified. The request is rejected.
Unable to resolve agent name %1s , request %2s	SmServerMessage::AgentName-UnResolved	The Agent request is required to include the Agent identity but it could not be verified for the named Agent. The request is rejected.
Unable to update password blob data	SmServerMessage::Blob-UpdateFailed	A user’s "Password Blob" data for Password Services could not be updated in the User Store. If it is so configured, the Policy Server rejected the user’s authentication attempt.

Message	Function	Description
Unexpected exception while publishing AZ Libs	SmServerMes-sage::UnexpectedException-PublishingAzLibs	An unexpected exception occurred while querying information about loaded custom authorization modules for diagnostic "Publish" information, so information regarding custom authorization libraries will not be published.
Unknown agent key type %1i	SmServerMessage::Agent-KeyTypeUnknown	While Processing a "Do Management" request, An Agent Key record in the Policy Store was found with the given unrecognized key type, and the request was rejected.
Unknown Exception caught while publishing Auth Libs	SmServerMessage::Unknown-ExcpPublishAuthLibs	An unexpected exception occurred while querying custom authentication scheme libraries for diagnostic "Publish" information, so information regarding loaded custom authentication schemes will not be published.
Unknown exception caught while publishing Event Lib info	SmServerMessage::Unknown-ExcpWhilePublishEventLibInfo	An unexpected exception occurred while querying a custom event handler library for diagnostic "Publish" information, so information regarding custom event libraries loaded by CA SiteMinder® will not be published.
Socket Error 104	104 - A call to bind() function failed.	This message is returned due to an error occurring when the message is sent across the TLI layer.

Java API

Error Message	Function	Description
%1s could not fetch administrator directory	SmJavaApiMes-sage::Administrator Directory-FetchFail	Unable to fetch the Registration Administrator User Directory. Check Policy Store.
%1s could not fetch registration directory	SmJavaApiMes-sage::RegistrationDirectory-FetchFail	Unable to fetch the Registration User Directory. Check Policy Store.
%1s could not fetch registration domain	SmJavaApiMes-sage::RegistrationDomain-FetchFail	Unable to fetch the Registration domain. Check Policy Store.
%1s could not fetch registration realm	SmJavaApiMes-sage::RegistrationRealm-FetchFail	Unable to fetch the Registration realm. Check Policy Store.
%1s could not fetch registration scheme	SmJavaApiMes-sage::RegistrationScheme-FetchFail	Unable to fetch the Registration scheme. Check Policy Store.
%1s invalid realm oid (null)	SmJavaApiMessage::Invalid-Realm Oid	Unable to get the realm oid. Ensure that the user login was successful and a valid Session ID is available.
(CSmEmsCommand::Set-ObjectClasses) Could not rollback properties of directory user %1s after setting properties failed	SmJavaApiMessage::Csm-EmsSetObjectClasses-RollBackPropertiesFail	Unable to reset the properties of the user after new values were rejected. Verify that the user store is operating correctly and the Policy Server can establish a connection.
(CSmEmsCommand::Set-Properties) Could not rollback properties of directory user %1s after setting properties failed.	SmJavaApiMessage::CSm-EmsSetPropertiesRollback-PropertiesFail	Unable to reset the properties of the user after new values were rejected. Verify that the user store is operating correctly and the Policy Server can establish a connection.
(CSmEmsCommandV2::Set-Object Classes) Could not rollback properties of directory user %1s after setting properties failed.	SmJavaApiMessage::Set-ObjectClassesDir-UserRollbackFail	Unable to reset the properties of the user after new values were rejected. Verify the directory connection defined in the policy store.
(CSmEmsCommandV2::Set-Properties) Could not rollback properties of directory object %1s after setting properties failed.	SmJavaApiMessage::Set-Properties DirObjRollbackFail	Unable to reset the properties of the object after new values were rejected. Verify the directory connection defined in the policy store.

Error Message	Function	Description
Exception in Transact SessionTimeoutThread.	SmJavaApiMessage::Unknown-Excp TransactSessionTimeout-Thread	An unknown error occurred while trying to process expired sessions.
Exception in Transact SessionTimeoutThread. Msg: %1s	SmJavaApiMessage::Excp-TransactS essionTimeoutThread	An error occurred while trying to process expired sessions.
Failed to create EmsSession Timeout Thread	SmJavaApiMessage::Ems-SessionTi meoutThread-CreateFail	There are not enough system resources to create a new thread.
Failed to resolve all domains	SmJavaApiMessage::Domain-Resol veFail	A problem occurred while trying to retrieve all domains associated with the current administrator. Check for Policy Store corruption.
getUsersDelegatedRoles failed, error = %1s	SmJavaApiMessage::IMSget-UsersD elegatedRolesFail	Unable to retrieve roles for this user. Make sure the library smobjims.dll (libsmobjims.so) is installed.
getUsersDelegatedRolesInApp failed, error = %1s	SmJavaApiMessage::IMSget-UsersD elegatedRolesInAppFail	Unable to retrieve user roles for the application. Make sure the library smobjims.dll (libsmobjims.so) is installed.
getUsersDelegatedTasks failed, error = %1s	SmJavaApiMessage::IMSget-UsersD elegatedTasksFail	Unable to retrieve tasks for this user. Make sure the library smobjims.dll (libsmobjims.so) is installed.
getUsersDelegatedTasksInApp failed, error = %1s	SmJavaApiMessage::IMS-getUsersD elegatedTasksIn-AppFail	Unable to retrieve user tasks for the application. Make sure the library smobjims.dll (libsmobjims.so) is installed.
getUsersRoles failed, error = %1s	SmJavaApiMessage::IMS-getUsersR olesFail	Unable to retrieve roles for this user. Make sure the library smobjims.dll (libsmobjims.so) is installed.
getUsersRolesInApp failed, error = %1s	SmJavaApiMessage::IMS-getUsersR olesInAppFail	Unable to retrieve user roles for the application. Make sure the library smobjims.dll (libsmobjims.so) is installed.
getUsersTasks failed, error = %1s	SmJavaApiMessage::IMS-getUsersT asksFail	Unable to retrieve tasks for this user. Make sure the library smobjims.dll (libsmobjims.so) is installed.
getUsersTasksInApp failed, error = %1s	SmJavaApiMessage::IMS-getUsersT asksInAppFail	Unable to retrieve user tasks for the application. Make sure the library smobjims.dll (libsmobjims.so) is installed.

Error Message	Function	Description
IMSObjectProviderFactory: getIMSBaseObjectProvider() - getProcAddress('%1s') failed	SmJavaApiMessage::getIMSB-aseObjectProvider_getProc-AddressFail	Make sure the library smobjims.dll (libsmobjims.so) is installed.
IMSObjectProviderFactory:get-Provider() - error loading provider library	SmJavaApiMes-sage::IMS_getProviderLib-LoadError	This message is generated at startup if IdentityMinder not installed, or not installed correctly.
IMSObjectProviderFactory:get-Provider() - getProcAddress of %1s failed	SmJavaApiMes-sage::IMS_getProvider_get-ProcAddressFail	The library is corrupt or the Policy Server could not load the library due to lack of resources.
ImsRBACProviderFactory:get-Provider() - getProcAddress of %1s failed	SmJavaApiMessage::Ims-RBACProvider-Factory_getProviderFail	This message is generated at startup if IdentityMinder not installed, or not installed correctly.
IsAssociatedWithDirectory failed, error = %1s	SmJavaApiMessage::IMSIs-AssociatedWithDirectoryFail	An error occurred while trying to determine if the user directory is valid for the associated IMS Environment.
IsUserAssignedRole failed, error = %1s	SmJavaApiMessage::IMSIs-UserAssignedRoleFail	An error occurred while trying to determine if the user belongs to a role.
IsUserDelegatedRole failed, error = %1s	SmJavaApiMessage::IMSIs-UserDelegatedRoleFail	An error occurred while trying to determine if the user belongs to a role.
SmJavaAPI: Error finding class ActiveExpressionContext %1p	SmJavaApiMessage::MSG_E_-FINDING_CAEClog	The JVM was unable to find the Active Expression class during unitization. Make sure the Option Pack is installed on the Policy Server. Check classpath for smjavaapi.jar.
SmJavaAPI: Error finding class NativeCallbackError %1p	SmJavaApiMessage::MSG_E_-FINDING_CNCElog	Make sure a valid smjavaapi.jar exists and is included in the classpath. Check to see if the JVM version is supported for this release.
SmJavaAPI: Error finding class SmAuthenticationContext %1p	SmJavaApiMessage::MSG_E_-FINDING_CAUTHClog	Make sure a valid smjavaapi.jar exists and is included in the classpath.

Error Message	Function	Description
SmJavaAPI: Error finding class Throwable %1p	SmJavaApiMessage::MSG_E_-FINDING_CTHROWlog	The JVM/JRE appears to not have been installed properly. Check to see if a valid rt.jar exists. Ensure that CA SiteMinder® is configured to use a supported version of the JVM.
SmJavaAPI: Error finding class TunnelServiceContext %1p	SmJavaApiMessage::MSG_E_-FINDING_CTSClog	Make sure the Option Pack is installed on the Policy Server a valid smjavaapi.jar exists and is included in the classpath.
SmJavaAPI: Error finding class UserAuthenticationException %1p	SmJavaApiMessage::MSG_E_-FINDING_CUAElog	Make sure a valid smjavaapi.jar exists and is included in the classpath. Check to see if the JVM version is supported for this release.
SmJavaAPI: Error finding method ActiveExpressionContext. invoke %1p	SmJavaApiMessage::MSG_E_-FIND_MINVOKElog	Make sure the Option Pack is installed on the Policy Server a valid smjavaapi.jar exists and is included in the classpath
SmJavaAPI: Error finding method ActiveExpressionContext. release %1p	SmJavaApiMessage::MSG_E_-FIND_MRELEASElog	Make sure the Option Pack is installed on the Policy Server a valid smjavaapi.jar exists and is included in the classpath
SmJavaAPI: Error finding method SmAuthenticationContext. authenticate %1p	SmJavaApiMessage::MSG_E_-FIND_MAUTHENTICATElog	Make sure a valid smjavaapi.jar exists and is included in the classpath. Check to see if the JVM version is supported for this release.
SmJavaAPI: Error finding method SmAuthenticationContext. init %1p	SmJavaApiMessage::MSG_E_-FIND_MAUTHINITlog	Make sure a valid smjavaapi.jar exists and is included in the classpath. Check to see if the JVM version is supported for this release.
SmJavaAPI: Error finding method SmAuthenticationContext. query %1p	SmJavaApiMessage::MSG_E_-FIND_MAUTHQUERYlog	Make sure a valid smjavaapi.jar exists and is included in the classpath. Check to see if the JVM version is supported for this release.
SmJavaAPI: Error finding method SmAuthenticationContext. release %1p	SmJavaApiMessage::MSG_E_-FIND_MAUTHRELEASElog	Make sure a valid smjavaapi.jar exists and is included in the classpath. Check to see if the JVM version is supported for this release.

Error Message	Function	Description
SmJavaAPI: Error finding method Throwable.getLocalized-Message %1p	SmJavaApiMessage::MSG_E_-FIND_GLMlog	The JVM/JRE appears to not have been installed properly. Check to see if a valid rt.jar exists. Ensure that CA SiteMinder® is configured to use a supported version of the JVM.
SmJavaAPI: Error finding method TunnelServiceContext.tunnel %1p	SmJavaApiMessage::MSG_E_-FIND_MTUNNELlog	Make sure a valid smjavaapi.jar exists and is included in the classpath
SmJavaAPI: Error initializing Java active expressions %1p	SmJavaApiMessage::MSG_E_-ACTEXPR_INITlog	Unable to load the Active Expression library. Check to see if smactiveexpr.jar is in the classpath
SmJavaAPI: Error initilizing JNI references for SMJavaAPI %1p	SmJavaApiMessage::MSG_E_-INIT_JNI_REFSlog	The JVM encountered an internal error. Check JVM installation.
SmJavaAPI: Error making global reference to class ActiveExpressionContext %1p	SmJavaApiMessage::MSG_E_-GLOBAL_CAEClog	The JVM encountered an internal error establishing the active expression context
SmJavaAPI: Error making global reference to class NativeCallbackError %1p	SmJavaApiMessage::MSG_E_-GLOBAL_CNCElog	Make sure a valid smjavaapi.jar exists and is included in the classpath. Check to see if the JVM version is supported for this release.
SmJavaAPI: Error making global reference to class SmAuthenticationContext %1p	SmJavaApiMessage::MSG_E_-GLOBAL_CAUTHClog	The JVM encountered an internal error establishing a authentication context
SmJavaAPI: Error making global reference to class Throwable %1p	SmJavaApiMessage::MSG_E_-GLOBAL_CTHROWlog	The JVM/JRE appears to not have been installed properly. Check to see if a valid rt.jar exists. Ensure that CA SiteMinder® is configured to use a supported version of the JVM.
SmJavaAPI: Error making global reference to class TunnelServiceContext %1p	SmJavaApiMessage::MSG_E_-GLOBAL_CTSClog	The JVM encountered an internal error establishing a tunnel connection
SmJavaAPI: Error making global reference to class UserAuthenticationException %1p	SmJavaApiMessage::MSG_E_-GLOBAL_CUAElog	Make sure a valid smjavaapi.jar exists and is included in the classpath. Check to see if the JVM version is supported for this release.

Error Message	Function	Description
SmJavaAPI: Error releasing Java active expressions %1p	SmJavaApiMessage::MSG_E_-ACTEXPR_RELEASElog	The JVM encountered an internal error. Check JVM installation.
SmJavaAPI: Error releasing JNI references for SMJavaAPI %1p	SmJavaApiMessage::MSG_E_-REL_JNI_REFSlog	The JVM encountered an internal error. Check JVM installation.
SmJavaAPI: Unable to get a JVM environment %1p	SmJavaApiMessage::MSG_-ERR_GETTING_JVMlog	The JVM encountered an internal error. Check JVM installation.
SmJavaAPI: Unable to initialize JNI references %1p	SmJavaApiMessage::MSG_-ERR_INIT_JNI_REFlog	The JVM encountered an internal error. Check JVM installation.
SmJavaAPI: Unable to release JNI references %1p	SmJavaApiMessage::MSG_-ERR_REL_JNI_REFlog	Policy Server could not completely release resources either after authorization or during shutdown.
SmJVMSupport: Error attaching JVM to thread %1p	SmJavaApiMessage::MSG_E_-ATTACH_TO_THREADlog	The JVM might not have been properly initialized. Make sure there are no stray java processes running
SmJVMSupport: Error creating JVM %1p	SmJavaApiMessage::MSG_E_-CREATE_JVMlog	Make sure the JVM is installed correctly and the library jvm.dll (libjvm.so) is valid
SmJVMSupport: Error destroying JVM %1p	SmJavaApiMessage::MSG_E_-DESTROYING_JAVA_VMlog	The Policy Server did not execute a clean shutdown. JVM resources were not released.
SmJVMSupport: Error detaching JVM from thread %1p	SmJavaApiMessage::MSG_E_-DETACH_THREADlog	The Policy Server did not execute a clean shutdown. JVM resources were not released.
SmJVMSupport: Error finding class System to release resources from JVM %1p	SmJavaApiMessage::MSG_E_-JVM_RR_FSYSlog	The Policy Server did not execute a clean shutdown. JVM resources were not released.
SmJVMSupport: Error getting CLASSPATH environment variable when creating JVM %1p	SmJavaApiMessage::MSG_E_-GETENV_CPlog	Ensure that the CLASSPATH variable is correctly defined
SmJVMSupport: Error getting JVM environment to release resources from JVM %1p	SmJavaApiMessage::MSG_E_-JVM_RR_ENVlog	The Policy Server did not execute a clean shutdown. JVM resources were not released.
SmJVMSupport: Error getting method GC on class System to release resources from JVM %1p	SmJavaApiMessage::MSG_E_-JVM_RR_GGClog	The JVM was unable to run the garbage collection. Ensure the validity of rt.jar

Error Message	Function	Description
SmJVMSupport: Error opening NETE_JVM_OPTION_FILE %1p	SmJavaApiMessage::MSG_E_-OPEN _JVM_OPTION_FILElog	Ensure that the environment variable NETE_JVM_OPTION_FILE is set and the file is valid
SmJVMSupport: Error trying to get a created JVM %1p	SmJavaApiMessage::MSG_E_-GET_ CREATED_JVM_LOG	The JVM might not have been properly initialized. Make sure there there are no stray java processes running .
SmJVMSupport: Unknown error caught when creating JVM %1p	SmJavaApiMessage::MSG_E_-CAUG HT_CREATE_JVMlog	Make sure the JVM is installed correctly and the library jvm.dll (libjvm.so) is valid

LDAP

Error Message	Function	Description
(AddMember) Group DN: '%1s', User DN: '%2s'. Status: Error %3i . %4s	SmLdapMessage::ErrorLdap-AddM emberGroupDN	Failed to add a given user to a given group in an LDAP user directory. See the included LDAP error message for additional information.
(AuthenticateUser) DN: '%1s' . Status: Error %2i . %3s	SmLdapMes-sage::AuthenticateUs erDNLd-Error	The Policy Server failed to authenticate a user against an LDAP user directory. This may happen for a variety of reasons, including but not limited to the user supplying a wrong password. See the included LDAP error message for additional information.
(Bind - init) Server: '%1s', Port: %2ul. Status: Error	SmLdapMessage::ErrorBindInit	The LDAP server configured for a user directory could not be initialized. Troubleshoot the LDAP server specified in the error message.
(Bind - init) Server: failed to load Security Integration file	SmLdapMessage::BindInit-LoadSec urityIntegrationFileFail	(Obsolete)
(Bind - init) Server: failed to load Security Integration secret	SmLdapMessage::BindInit-LoadSec urityIntegrationSecret-Fail	(Obsolete)

Error Message	Function	Description
(Bind - ldap_set_option CONNECT_TIMEOUT). Status: Error %1i . %2s	SmLdapMessage::ErrorBind-LdapOptionConnectTimeout	Unable to set LDAP option. Check the error string for more information.
(Bind - ldap_set_option LDAP_OPT_PROTOCOL_-VERSION). Status: Error %1i . %2s	SmLdapMessage::ErrorBind-LdapOptionProtocolVersion	Unable to set LDAP option. Check the error string for more information.
(Bind - ldap_set_option LDAP_OPT_REFERRALS). Status: Error %1i. %2s	SmLdapMessage::ErrorBind-LdapOptionReferrals	Unable to set enable automatic referral handling. Check the error string for more information.
(Bind - ldap_set_option LDAPL_VERSION2). Status: Error %1i . %2s	SmLdapMessage::ErrorBind-LdapOptionVersion2	Unable to set LDAP option. Check the error string for more information. Make sure your LDAP server is one of the supported versions.
(Bind - ldap_set_option SIZELIMIT). Status: Error %1i. %2s	SmLdapMessage::ErrorBind-LdapOptionSizeLimit	Unable to set LDAP option. Check the error string for more information.
(Bind - ldap_set_option THREAD_FN_PTRS). Status: Error %1i . %2s	SmLdapMessage::ErrorBind-LdapOptionThreadFnPirs	Unable to set LDAP option. Check the error string for more information.
(Bind - ldap_set_option TIMELIMIT). Status: Error %1i. %2s	SmLdapMessage::ErrorBind-LdapOptionTimeLimit	Unable to set LDAP option. Check the error string for more information.
(Bind - SSL client init failed during LDAP Initialization) Server: '%1s', Port: %2ul, Cert DB: '%3s' . Status: Error	SmLdapMessage::BindSSL-LdapClientInitFailed	Unable to connect to LDAP server. Make sure your LDAP server is running, and the LDAP server and port are correct. (try ping from the policy server machine.)
(Bind - SSL client init) Cert DB: '%1s' . Status: Error	SmLdapMessage::BindSSL-ClientCertDBFailed	The client-side initialization of an SSL connection to the LDAP server configured for a user directory failed. Verify if the certificate database is specified correctly.
(Bind - SSL init) Server: '%1s', Port: %2ul. Status: Error. Check LDAP server and port.	SmLdapMessage::BindSSL-InitFailed	Unable to initialize to LDAP server with SSL. Check the LDAP server and port. Make sure your LDAP server is configured for SSL.

Error Message	Function	Description
(Bind) DN: '%1s'. Status: Error %2i . %3s	SmLdapMessage::BindDN-RequireCredentialsError	Unable to bind to LDAP server. Make sure the credentials are correct. See CA SiteMinder® management console.
(Bind) Status: Error %1i. %2s	SmLdapMessage::Bind-StatusError	Unable to set LDAP option. Check the error string for more information.
(ChangeUserPassword) DN: '%1s'. Status: Error %2i. %3s	SmLdapMessage::Change-UserPasswordLdError	A password change failed for the specified user because it couldn't bind to the LDAP server using his/her old password. See the error message for any additional information.
(ChangeUserPassword) DN: '%1s'. Status: Error %2s	SmLdapMessage::Change-UserPasswordDNFail	A password change failed for the specified user. See the error message for any additional information.
(CSmDsLdapProvider::Add-Entry) DN: '%1s'. Status: Error %2i . %3s	SmLdapMessage::ErrorLdap-AddEntryDN	Failed to add a given DN entry to an LDAP user directory. See the included LDAP error message for additional information.
(GetObjProperties) DN: '%1s' . Status: Error %2i . %3s	SmLdapMessage::GetObj-PropertiesDNLdError	The Policy Server failed to get a requested property of a requested DN in an LDAP user directory. See the included LDAP error message for additional information.
(GetUserProp) DN: '%1s', Filter: '%2s' . Status: Error %3i . %4s	SmLdapMessage::GetUser-PropDNLd-Error	An error occurred when searching for a given DN and specifying an attribute to be retrieved. See the included LDAP error message for additional information.
(GetUserProp) DN: '%1s', Filter: '%2s' . Status: Error %3i . %4s	SmLdapMessage::GetUser-PropsDNLdError	An error occurred when searching for a given DN and specifying attributes to be retrieved. See the included LDAP error message for additional information.
(RemoveEntry) DN: '%1s'. Status: Error %2i . %3s	SmLdapMessage::ErrorLdap-RemoveEntryDN	Failed to find a DN entry to be removed from an LDAP user directory. See the included LDAP error message for additional information.

Error Message	Function	Description
(RemoveMember) Group DN: '%1s', User DN: '%2s'. Status: Error %3i . %4s	SmLdapMessage::ErrorLdap-RemoveMemberGroupDN	Failed to remove a given user from a given group in an LDAP user directory. See the included LDAP error message for additional information.
(SetUserProp) DN: '%1s', PropName: '%2s', PropValue: '%3s' . Status: Error %4i . %5s	SmLdapMessage::SetUser-PropDN Error	Failed to modify a given DN entry in an LDAP user directory. See the included LDAP error message for additional information.
(SetUserProp) DN: '%1s'. Status: Error %2i . %3s	SmLdapMessage::SetUser-PropsDNLdError	Failed to modify a given DN entry in an LDAP user directory. See the included LDAP error message for additional information.
(SI Bind - init) Server: '%1s', Port: %2ul. Status: Error	SmLdapMessage::ErrorSI-BindInit	The LDAP server configured for a user directory could not be initialized. Troubleshoot the LDAP server specified in the error message.
(SmDsLdap) Failed to get servers.	SmLdapMessage::SmDs-LdapFailToGetServers	Internal error occurred while trying to rebind to referred LDAP server. Data may not be available.
(SmDsLdapConnMgr(Bind): SSL client init failed in LDAP Initialization). Server %1s : %2ul, Cert DB: %3s	SmLdapMessage::Ldap-ConnMgrBindSSLCertDBInit-Fail	Unable to initialize to LDAP server with SSL. Check the LDAP server and port. Make sure your LDAP server is configured for SSL.
"ldap_url_parse returns error '1%i' when parsing '%2s'"	SmLdapMessage::Error_ldap_url_parse	An internal LDAP URL could not be parsed. It must conform to RFC 2255 format.
(SmDsLdap-LdapAdd) DN: '%1s'. Status: Received referral but no handling is implemented.	SmLdapMessage::SmDsLdap-AddHandlingImplError	Error was caused Add call returning a referral request.
(SmDsLdap-LdapDelete) DN: '%1s'. Status: Received referral but no handling is implemented.	SmLdapMessage::SmDs-LdapDeleteHandlingImplError	Error was caused Delete call returning a referral request.
(SmDsLdap-LdapModify) DN: '%1s'. Status: Received referral but no handling is implemented.	SmLdapMessage::SmDs-LdapModifyHandlingImplError	Error was caused Modify call returning a referral request.

Error Message	Function	Description
(SmDsLdap-Referral) Error while parsing %1s LDAP URL.	SmLdapMessage::Ldap-URLParsing Error	The Policy Server failed to parse a given LDAP URL. The usual cause of failure is a faulty LDAP URL passed as a referral, in which case verify that your LDAP topology is defined correctly and/or disable enhanced LDAP referral handling in the Policy Server Management Console.
CSmDsLdapConnMgr (ldap_unbind_s). Server %1s : %2ul	SmLdapMessage::Error-LdapConn MgrUnbind	Error while unbinding from the LDAP server.
CSmDsLdapConnMgr (ldap_unbind_s). Server %1s : %2ul	SmLdapMessage::Unknown-Except ionLdapConnMgrUnbind	Internal error occurred while unbinding from the LDAP server.
CSmDsLdapProvider::Search(): Wrong syntax of LDAP search filter: %1s	SmLdapMessage::Wrong-SyntaxLd apSearchFilter	Verify if the LDAP search filter has correct syntax.
CSmDsLdapProvider::Search-Binar y(): Wrong syntax of LDAP search filter: %1s	SmLdapMessage::Wrong-SyntaxLd apSearchBinFilter	Verify if the LDAP search filter has correct syntax.
CSmDsLdapProvider::Search-Count (): Wrong syntax of LDAP search filter: %1s	SmLdapMessage::Wrong-SyntaxLd apSearchCountFilter	Verify if the LDAP search filter has correct syntax.
CSmObjLdapConnMgr Exception (ldap_unbind_s). Server %1s:%2ul	SmLdapMessage::Excp-CSmObjLda pConn-Mgrldap_unbind_s	The CA SiteMinder® Policy Server failed to unbind from the LDAP server configured for the policy store. Troubleshoot the LDAP server specified in the error message.
Directory's Disabled Flag attribute not proper for password services functionality in CSmDsLdapProvider::Set-Disabled UserState	SmLdapMessage::DirDisabled-Flag NotProper	There is a user attribute in the directory that represents the Disabled Flag. The attribute does not work with Password Services. Change the attribute.
Exception (ldap_controls_free) in CSmDsLDAPConn::Create-LDAPCo ntrols	SmLdapMessage::Unknown-Except ionFreeLDAPControls	Unexpected error occurred while releasing an internal object back to LDAP library. This is likely a memory or configuration error on the policy server system.

Error Message	Function	Description
Exception (ldap_count_entries) in CSmDsLdapProvider::Search-Count	SmLdapMessage::Unknown-ExceptionLdapCountEntries	Unknown exception when processing results of an LDAP search in the user directory provider layer.
Exception (ldap_explode_dn) in CSmDsLdapProvider::Get-GroupMembers	SmLdapMessage::Ldap-ExplodeExceptionGet-GroupMembers	Unknown exception when converting a DN into its component parts.
Exception (ldap_init) in CSmDsLdapProvider::Bind	SmLdapMessage::Unknown-ExceptionLdapInitBind	Unknown exception when initializing an LDAP server configured for a user directory.
Exception (ldap_init) in SecurityIntegrationCheck	SmLdapMessage::Unknown-ExceptionLdapInit	Unknown exception when initializing an LDAP server configured for a user directory.
Exception (ldap_modify_s) in CSmDsLdapProvider::Add-Entry	SmLdapMessage::Unknown-ExceptionLdapModifyAdd-Entries	Unknown exception when adding an entry to an LDAP user directory.
Exception (ldap_modify_s) in CSmDsLdapProvider::Set-UserProps	SmLdapMessage::Unknown-ExceptionLdapModify-SetUserProps	Unknown exception when modifying an entry in an LDAP user directory.
Exception (ldap_search_ext_s) in CSmDsLdapProvider::Ping-Server	SmLdapMessage::Unknown-ExceptionPingServer	Unable to connect to LDAP server. Make sure your LDAP server is running, and the LDAP server and port are correct. (try ping from the policy server machine.)
Exception (ldap_search_ext_s) in CSmDsLdap-Provider::Search	SmLdapMessage::Unknown-ExceptionLdapSearchExt	Unknown exception when performing an LDAP search in the user directory provider layer.
Exception (ldap_search_ext_s) in CSmDsLdapProvider::-SearchBinary	SmLdapMessage::Unknown-ExceptionLdapSearchBinExt	Unknown exception when performing an LDAP search in the user directory provider layer.
Exception (ldap_search_ext_s) in CSmDsLdapProvider::-SearchCount	SmLdapMessage::Unknown-ExceptionSearchCount	Unknown exception when performing an LDAP search in the user directory provider layer.
Exception (ldap_search_s) in CSmDsLdapProvider::Get-ObjProperties	SmLdapMessage::Unknown-ExceptionLdapSearchGet-ObjProperties	Unknown exception when performing an LDAP search in the user directory provider layer.

Error Message	Function	Description
Exception (ldap_search_s) in CSmDsLdapProvider::Get-UserProp	SmLdapMessage::Unknown-ExceptionLdapSearchGet-UserProp	Unknown exception when performing an LDAP search in the user directory provider layer.
Exception (ldap_search_s) in CSmDsLdapProvider::Get-UserProps	SmLdapMessage::Unknown-ExceptionLdapSearchGet-UserProps	Unknown exception when performing an LDAP search in the user directory provider layer.
Exception (ldap_search_s) in CSmObjLdapProvider::Ping-Server	SmLdapMessage::Excp-Ldap_Search_S	The LDAP server configured for the policy store could not be pinged. Check if it is up and running.
Exception (ldap_search_st) in CSmObjLdapProvider::Ping-Server	SmLdapMessage::Excpldap_-search_st	The LDAP server configured for the policy store could not be pinged with the given timeout value. Check if it is up and running.
Exception (ldap_simple_bind_s) in CSmDsLdapProvider::Bind	SmLdapMessage::Unknown-Exception-LdapSimpleBind	Unable to connect to LDAP server. Make sure your LDAP server is running, and the LDAP server and port are correct. (try ping from the policy server machine.)
Exception (LdapModify) in CSmDsLdapProvider::Add-Entry	SmLdapMessage::Unknown-ExceptionLdapModifyAddEntry	Unknown exception when adding an entry to an LDAP user directory. Try disabling the enhanced referral handling to see if it helps.
Exception (LdapModify) in CSmDsLdapProvider::Add-Member	SmLdapMessage::Unknown-ExceptionLdapModifyAdd-Member	Unknown exception when adding a member to a group in an LDAP user directory. Try disabling the enhanced referral handling to see if it helps.
Exception (LdapModify) in CSmDsLdapProvider::Remove-Member	SmLdapMessage::Unknown-ExceptionLdapModify-RemoveMember	Unknown exception when removing a member from a group in an LDAP user directory. Try disabling the enhanced referral handling to see if it helps.
Exception (LdapModify) in CSmDsLdapProvider::Set-UserProp	SmLdapMessage::Unknown-ExceptionLdapModifySet-UserProp	Unknown exception when modifying an entry in an LDAP user directory. Try disabling the enhanced referral handling to see if it helps.

Error Message	Function	Description
Exception (ldapssl_client_init) in CSmDsLdapProvider::Init-Instance	SmLdapMessage::Unknown-ExceptionLdapSSLClinetInit	The client-side initialization of an SSL connection to the LDAP server configured for a user directory failed. Verify if the certificate database is specified correctly.
Exception (ldapssl_init) in CSmDsLdapProvider::Bind	SmLdapMessage::Unknown-ExceptionLdapSSLInitBind	Unable to initialize to LDAP server with SSL. Check the LDAP server and port. Make sure your LDAP server is configured for SSL.
Exception in CSmDsLDAPConn::Create-LDAPControls	SmLdapMessage::Unknown-ExceptionCreateLDAPControls	Unexpected error occurred while requesting internal object from LDAP library. This is likely a memory or configuration error on the policy server system.
Exception in CSmDsLDAPConn::Free-LDAPControls	SmLdapMessage::Unknown-exceptionCSmDsLDAP-Conn_FreeLDAPControls	Internal error occurred while releasing LDAP controls.
Exception in CSmDsLDAPConn::Parse-LDAPControls	SmLdapMessage::Unknown-ExceptionParseLDAPControls	Unable to parse response from LDAP server. Is the LDAP server running properly?
Exception in CSmDsLdapProvider::Get-ObjProperties	SmLdapMessage::Unknown-ExceptionGetObjProperties	Unknown exception when processing results of an LDAP search in the user directory provider layer.
Exception in CSmDsLdapProvider::Get-UserProp	SmLdapMessage::Unknown-ExceptionGetUserProp	Unknown exception when processing results of an LDAP search in the user directory provider layer.
Exception in CSmDsLdapProvider::Get-UserProps	SmLdapMessage::Unknown-ExceptionGetUserProps	Unknown exception when processing results of an LDAP search in the user directory provider layer.
Exception in CSmDsLdapProvider::Search	SmLdapMessage::Unknown-ExceptionCSmDsLdap-ProviderSearch	Unknown exception when processing results of an LDAP search in the user directory provider layer.
Exception in CSmDsLdapProvider::Search-Binary	SmLdapMessage::Unknown-ExceptionSearchBinary	Unknown exception when processing results of an LDAP search in the user directory provider layer.

Error Message	Function	Description
Exception in SecurityIntegrationCheck	SmLdapMessage::Unknown-ExceptionSecurityIntegration-Check	Unknown exception trying to identify if an LDAP server configured for a user directory is an instance of Security Integration LDAP.
Failed to create a paging control	SmLdapMessage::Create-PagingControlFail	Internal error occurred while requesting internal object from LDAP library. This is likely a memory or configuration error on the policy server system.
Failed to create a sorting LDAP control	SmLdapMessage::Create-SortLdapControlFail	Internal error occurred while requesting internal object from LDAP library. This is likely a memory or configuration error on the policy server system.
Failed to fetch user property '%1s' for DN '%2s'	SmLdapMessage::FailedTo-FetchUserPropertyForDN	The specified DN does not exist on the LDAP server configured for a user directory, or it does not have the specified property. This can happen, for example, if a CA SiteMinder® SDK application attempts to add a user to a group that does not exist.
Failed to parse LDAP message	SmLdapMessage::Ldap-ParseMsgFail	Received invalid response from LDAP server. Is the LDAP server running properly?
Failed to parse the server-side sorting response control	SmLdapMessage::Parsing-ServerSideResponse-ControlFail	Unable to parse response from LDAP server. Is the LDAP server running properly?
Failed to parse the virtual list view response control	SmLdapMessage::Virtual-ListViewResponseControlFail	Unable to parse response from LDAP server. Is the LDAP server running properly?
Failed to retrieve cert db location from registry	SmLdapMessage::Retrieve-CertDBRegFailed	The HKLM\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\LdapPolicyStore\CertDbPath registry entry was not found. Create that entry, entering the appropriate SSL certificate database path or leaving empty if not using SSL connection to the policy store. On a UNIX system, use the sm.registry file in <install-dir>/registry.

Error Message	Function	Description
Failure executing the server-side sorting LDAP control	SmLdapMessage::Server-SideSortingLdapExecFail	Unable to parse response from LDAP server. Is the LDAP server running properly?
LDAP admin limit exceeded searching for ActiveExpr entries in policy store	SmLdapMessage::Admin-LimitExceedSearchFor-ActiveExpr	A search for active expressions in the policy store exceeded the look-through limit the LDAP instance was configured with. Increase the look-through limit on the LDAP server side.
LDAP admin limit exceeded searching for Agent entries in policy store	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_Device	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP admin limit exceeded searching for AgentCommand entries in policy store	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_AgentCommand	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP admin limit exceeded searching for AgentGroup entries in policy store	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_DeviceGroup	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP admin limit exceeded searching for AgentKey entries in policy store	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_AgentKey	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP admin limit exceeded searching for AgentType entries in policy store	SmLdapMessage::Admin-LimitExceedSearchFor-AgentType	A search for agent types in the policy store exceeded the look-through limit the LDAP instance was configured with. Increase the look-through limit on the LDAP server side.

Error Message	Function	Description
LDAP admin limit exceeded searching for AgentTypeAttr entries in policy store	SmLdapMessage::Admin-LimitExceedSearchFor-AgentTypeAttr	A search for agent type attributes in the policy store exceeded the look-through limit the LDAP instance was configured with. Increase the look-through limit on the LDAP server side.
LDAP admin limit exceeded searching for AuthAzMap entries in policy store	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_AuthAzMap	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP admin limit exceeded searching for CertMap entries in policy store	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_CertMap	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP admin limit exceeded searching for Domain entries in policy store	SmLdapMessage::LdapAdmin-SizeLimitExceeded_Domain	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP admin limit exceeded searching for KeyManagement entries in policy store	SmLdapMessage::LdapAdmin-SizeLimit-Exceeded_KeyManagement	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP admin limit exceeded searching for ODBCQuery entries in policy store	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_ODBCQuery	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.

Error Message	Function	Description
LDAP admin limit exceeded searching for PasswordPolicy entries in policy store	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_PasswordPolicy	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP admin limit exceeded searching for Policy entries in policy store	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_Policy	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP admin limit exceeded searching for PolicyLink entries in policy store	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_PolicyLink	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP admin limit exceeded searching for Property entries in policy store	SmLdapMessage::Admin-LimitExceedSearchFor-Property	A search for property objects in the policy store exceeded the look-through limit the LDAP instance was configured with. Increase the look-through limit on the LDAP server side.
LDAP admin limit exceeded searching for PropertyCollection entries in policy store	SmLdapMessage::Admin-LimitExceedSearchFor-PropertyCollection	A search for property collections in the policy store exceeded the look-through limit the LDAP instance was configured with. Increase the look-through limit on the LDAP server side.
LDAP admin limit exceeded searching for PropertySection entries in policy store	SmLdapMessage::AdminLimit-ExceedSearchForProperty-Section	A search for property sections in the policy store exceeded the look-through limit the LDAP instance was configured with. Increase the look-through limit on the LDAP server side.

Error Message	Function	Description
LDAP admin limit exceeded searching for Realm entries in policy store	SmLdapMessage::LdapAdmin-SizeLimitExceeded_Realm	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP admin limit exceeded searching for Response entries in policy store	SmLdapMessage::Ldap-AdminSizeLimit-Exceeded_Response	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP admin limit exceeded searching for ResponseAttr entries in policy store	SmLdapMessage::AdminLimit-ExcedSearchForRespAttr	A search for response attributes in the policy store exceeded the look-through limit the LDAP instance was configured with. Increase the look-through limit on the LDAP server side.
LDAP admin limit exceeded searching for ResponseGroup entries in policy store	SmLdapMessage::AdminLimit-ExcedSearchForRespGroup	A search for response groups in the policy store exceeded the look-through limit the LDAP instance was configured with. Increase the look-through limit on the LDAP server side on the LDAP server side.
LDAP admin limit exceeded searching for RootConfig entries in policy store	SmLdapMessage::AdminLimit-ExcedSearchForRootConfig	This should never happen, since there may only be one RootConfig object in the policy store. Possible policy store corruption.
LDAP admin limit exceeded searching for Rule entries in policy store	SmLdapMessage::AdminLimit-ExcedSearchForRule	A search for rules in the policy store exceeded the look-through limit the LDAP instance was configured with. Increase the look-through limit on the LDAP server side.
LDAP admin limit exceeded searching for RuleGroup entries in policy store	SmLdapMessage::AdminLimit-ExcedSearchForRuleGroup	A search for rule groups in the policy store exceeded the look-through limit the LDAP instance was configured with. Increase the look-through limit on the LDAP server side.

Error Message	Function	Description
LDAP admin limit exceeded searching for Scheme entries in policy store	SmLdapMessage::AdminLimit-ExceedSearchForScheme	A search for authentication schemes in the policy store exceeded the look-through limit the LDAP instance was configured with. Increase the look-through limit on the LDAP server side.
LDAP admin limit exceeded searching for SelfReg entries in policy store	SmLdapMessage::AdminLimit-ExceedSearchForSelfReg	A search for registration schemes in the policy store exceeded the look-through limit the LDAP instance was configured with. Increase the look-through limit on the LDAP server side.
LDAP admin limit exceeded searching for ServerCommand entries in policy store	SmLdapMessage::Admin-LimitExceedSearchForServer-Command	A search for server commands in the policy store exceeded the look-through limit the LDAP instance was configured with. Increase the look-through limit on the LDAP server side.
LDAP admin limit exceeded searching for SharedSecretPolicy entries in policy store	SmLdapMessage::Admin-LimitExceedSearchFor-SharedSecretPolicy	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP admin limit exceeded searching for TaggedString entries in policy store	SmLdapMessage::Admin-LimitExceedSearchFor-TaggedString	A search for tagged strings in the policy store exceeded the look-through limit the LDAP instance was configured with. Increase the look-through limit on the LDAP server side.
LDAP admin limit exceeded searching for TrustedHost entries in policy store	SmLdapMessage::Admin-LimitExceedSearchFor-TrustedHost	A search for trusted hosts in the policy store exceeded the look-through limit the LDAP instance was configured with. Increase the look-through limit on the LDAP server side.
LDAP admin limit exceeded searching for UserDirectory entries in policy store	SmLdapMessage::Admin-LimitExceedSearchForUser-Directory	A search for user directories in the policy store exceeded the look-through limit the LDAP instance was configured with. Increase the look-through limit on the LDAP server side.

Error Message	Function	Description
LDAP admin limit exceeded searching for UserPolicy entries in policy store	SmLdapMessage::Admin-LimitExceedSearchForUser-Policy	A search for user policies in the policy store exceeded the look-through limit the LDAP instance was configured with. Increase the look-through limit on the LDAP server side.
LDAP admin limit exceeded searching for Variable entries in policy store	SmLdapMessage::Admin-LimitExceedSearchForVariable	A search for variables in the policy store exceeded the look-through limit the LDAP instance was configured with. Increase the look-through limit on the LDAP server side.
LDAP admin limit exceeded searching for VariableType entries in policy store	SmLdapMessage::Admin-LimitExceedSearchFor-VariableType	A search for variable types in the policy store exceeded the look-through limit the LDAP instance was configured with. Increase the look-through limit on the LDAP server side.
LDAP admin size limit exceeded searching for Admin entries in policy store	SmLdapMessage::LdapAdmin-SizeLimitExceeded_Admin	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP Error in Domain_FetchProperty for IMSEnvironments - unsupported policy store version for IMS objects	SmLdapMessage::Error-DomainFetchIMSEnv	The Policy server version must be 5.1 or greater.
LDAP Error in Domain_SaveProperty for IMSEnvironments - unsupported policy store version for IMS objects	SmLdapMessage::Error-DomainSaveIMSEnv	The Policy server version must be 5.1 or greater.
LDAP size limit exceeded searching for ActiveExpr entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForActiveExpr	A search for active expressions in the policy store exceeded the size limit the LDAP instance was configured with. Increase the size limit on the LDAP server side.

Error Message	Function	Description
LDAP size limit exceeded searching for Admin entries in policy store	SmLdapMessage::LdapSize-LimitExceeded_Admin	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP size limit exceeded searching for Agent entries in policy store	SmLdapMessage::LdapSize-LimitExceeded_Device	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP size limit exceeded searching for AgentCommand entries in policy store	SmLdapMessage::LdapSize-LimitExceeded_Agent-Command	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP size limit exceeded searching for AgentGroup entries in policy store	SmLdapMessage::LdapSize-LimitExceeded_DeviceGroup	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP size limit exceeded searching for AgentKey entries in policy store	SmLdapMessage::LdapSize-LimitExceeded_AgentKey	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP size limit exceeded searching for AgentType entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForAgentType	A search for agent types in the policy store exceeded the size limit the LDAP instance was configured with. Increase the size limit on the LDAP server side.

Error Message	Function	Description
LDAP size limit exceeded searching for AgentTypeAttr entries in policy store	SmLdapMessage::SizeLimit-Exceed SearchForAgent-TypeAttr	A search for agent type attributes in the policy store exceeded the size limit the LDAP instance was configured with. Increase the size limit on the LDAP server side.
LDAP size limit exceeded searching for AuthAzMap entries in policy store	SmLdapMessage::LdapSize-LimitEx ceeded_AuthAzMap	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP size limit exceeded searching for CertMap entries in policy store	SmLdapMessage::LdapSize-LimitEx ceeded_CertMap	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP size limit exceeded searching for Domain entries in policy store	SmLdapMessage::LdapSize-LimitEx ceeded_Domain	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP size limit exceeded searching for KeyManagement entries in policy store	SmLdapMessage::LdapSize-Limit-E xceeded_KeyManagement	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP size limit exceeded searching for ODBCQuery entries in policy store	SmLdapMessage::LdapSize-LimitEx ceeded_ODBCQuery	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.

Error Message	Function	Description
LDAP size limit exceeded searching for PasswordPolicy entries in policy store	SmLdapMessage::LdapSize-Limit-Exceeded_PasswordPolicy	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP size limit exceeded searching for Policy entries in policy store	SmLdapMessage::LdapSize-LimitExceeded_Policy	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP size limit exceeded searching for PolicyLink entries in policy store	SmLdapMessage::LdapSize-LimitExceeded_PolicyLink	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP size limit exceeded searching for Property entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForProperty	A search for property objects in the policy store exceeded the size limit the LDAP instance was configured with. Increase the size limit on the LDAP server side.
LDAP size limit exceeded searching for PropertyCollection entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForProperty-Collection	A search for property collections in the policy store exceeded the size limit the LDAP instance was configured with. Increase the size limit on the LDAP server side.
LDAP size limit exceeded searching for PropertySection entries in policy store	SmLdapMessage::SizeLimit-ExceedSearchForProperty-Section	A search for property sections in the policy store exceeded the size limit the LDAP instance was configured with. Increase the size limit on the LDAP server side.
LDAP size limit exceeded searching for Realm entries in policy store	SmLdapMessage::LdapSize-LimitExceeded_Realm	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.

Error Message	Function	Description
LDAP size limit exceeded searching for Response entries in policy store	SmLdapMessage::LdapSize-LimitExceeded_Response	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP size limit exceeded searching for ResponseAttr entries in policy store	SmLdapMessage::SizeLimit-Exceed SearchForResponse-Attr	A search for response attributes in the policy store exceeded the size limit the LDAP instance was configured with. Increase the size limit on the LDAP server side.
LDAP size limit exceeded searching for ResponseGroup entries in policy store	SmLdapMessage::SizeLimit-Exceed SearchForRespGroup	A search for response groups in the policy store exceeded the size limit the LDAP instance was configured with. Increase the size limit on the LDAP server side.
LDAP size limit exceeded searching for RootConfig entries in policy store	SmLdapMessage::SizeLimit-Exceed SearchForRootConfig	This should never happen, since there may only be one RootConfig object in the policy store. Possible policy store corruption.
LDAP size limit exceeded searching for Rule entries in policy store	SmLdapMessage::SizeLimit-Exceed SearchForRule	A search for rules in the policy store exceeded the size limit the LDAP instance was configured with. Increase the size limit on the LDAP server side.
LDAP size limit exceeded searching for RuleGroup entries in policy store	SmLdapMessage::SizeLimit-Exceed SearchForRuleGroup	A search for rule groups in the policy store exceeded the size limit the LDAP instance was configured with. Increase the size limit on the LDAP server side.
LDAP size limit exceeded searching for Scheme entries in policy store	SmLdapMessage::SizeLimit-Exceed SearchForScheme	A search for authentication schemes in the policy store exceeded the size limit the LDAP instance was configured with. Increase the size limit on the LDAP server side.
LDAP size limit exceeded searching for SelfReg entries in policy store	SmLdapMessage::SizeLimit-Exceed SearchForSelfReg	A search for registration schemes in the policy store exceeded the size limit the LDAP instance was configured with. Increase the size limit on the LDAP server side.

Error Message	Function	Description
LDAP size limit exceeded searching for ServerCommand entries in policy store	SmLdapMessage::SizeLimit-Exceed SearchForServer-Command	A search for server commands in the policy store exceeded the size limit the LDAP instance was configured with. Increase the size limit on the LDAP server side.
LDAP size limit exceeded searching for SharedSecretPolicy entries in policy store	SmLdapMessage::SizeLimit-Exceed SearchForShared-SecretPolicy	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the CA SiteMinder® admin UI to check the sizelimit that CA SiteMinder® will use for this LDAP server. Set this to match the server configuration.
LDAP size limit exceeded searching for TaggedString entries in policy store	SmLdapMessage::SizeLimit-Exceed SearchForTaggedString	A search for tagged strings in the policy store exceeded the size limit the LDAP instance was configured with. Increase the size limit on the LDAP server side.
LDAP size limit exceeded searching for TrustedHost entries in policy store	SmLdapMessage::SizeLimit-Exceed SearchForTrustedHost	A search for trusted hosts in the policy store exceeded the size limit the LDAP instance was configured with. Increase the size limit on the LDAP server side.
LDAP size limit exceeded searching for UserDirectory entries in policy store	SmLdapMessage::SizeLimit-Exceed SearchForUser-Directory	A search for user directories in the policy store exceeded the size limit the LDAP instance was configured with. Increase the size limit on the LDAP server side.
LDAP size limit exceeded searching for UserPolicy entries in policy store	SmLdapMessage::SizeLimit-Exceed SearchForUserPolicy	A search for user policies in the policy store exceeded the size limit the LDAP instance was configured with. Increase the size limit on the LDAP server side.
LDAP size limit exceeded searching for Variable entries in policy store	SmLdapMessage::SizeLimit-Exceed SearchForVariable	A search for variables in the policy store exceeded the size limit the LDAP instance was configured with. Increase the size limit on the LDAP server side.
LDAP size limit exceeded searching for VariableType entries in policy store	SmLdapMessage::SizeLimit-Exceed SearchForVariableType	A search for variable types in the policy store exceeded the size limit the LDAP instance was configured with. Increase the size limit on the LDAP server side.

Error Message	Function	Description
Length of the string supplied is more than the allowed limit.Please see LDAP store documentation for more details .	SmLdapMessage::Ldap-LengthConstrain-Violation_CertMap	The value used in the search was too long.
SmDsLdapConnMgr (ldap_search_ext_s) in PingServer : %1s	SmLdapMessage::ErrorLdap-ConnMgrPingServer	Unable to connect to LDAP server. Make sure your LDAP server is running, and the LDAP server and port are correct. (try ping from the policy server machine.)
SmDsLdapConnMgr Bind - init. Server %1s : %2ul	SmLdapMessage::LdapConn-MgrBindInitFail	Unable to connect to LDAP server. Make sure your LDAP server is running, and the LDAP server and port are correct. (try ping from the policy server machine.)
SmDsLdapConnMgr Bind - SetOption CONNECT_TIMEOUT %1i . Server %2s : %3ul	SmLdapMessage::LdapConn-MgrBindSetOptionConnect-Timeout	Unable to set LDAP option. Check the error string for more information.
SmDsLdapConnMgr Bind - SSL init. Server %1s : %2ul	SmLdapMessage::LdapConn-MgrBindSSLInitFail	Unable to initialize to LDAP server with SSL. Check the LDAP server and port. Make sure your LDAP server is configured for SSL.
SmDsLdapConnMgr Bind. Server %1s : %2ul. Error %3i-%4s	SmLdapMessage::ErrorLdap-ConnMgrBind	Unable to connect to LDAP server. Make sure your LDAP server is running, and the LDAP server and port are correct. (try ping from the policy server machine.)
SmDsLdapConnMgr Exception (ldap_init). Server %1s : %2ul	SmLdapMessage::Unknow-ExceptionLdapConnMgrInit	Unexpected error while connecting to LDAP server. Check the LDAP server and port configuration settings.
SmDsLdapConnMgr Exception (ldap_simple_bind_s). Server %1s : %2ul	SmLdapMessage::Unknown-ExceptionLdapConnMgrSimpleBind	Unexpected error while connecting to LDAP server. Check the LDAP server and port configuration settings.
SmDsLdapConnMgr Exception (ldapssl_init). Server %1s : %2ul	SmLdapMessage::Unknow-ExceptionLdapConnMgrSSLInit	Unexpected error while connecting to LDAP server with SSL. Check the LDAP server and port configuration settings. Is the server configured for SSL?

Error Message	Function	Description
SmObjLdap failed to bind to LDAP server %1s:%2i as %3s . LDAP error %4i-%5s	SmLdapMessage::SmObj-LdapFailToBindToLdapServer	Unable to connect to LDAP server. Make sure your LDAP server is running, and the LDAP server and port are correct. (try ping from the policy server machine.)
SmObjLdap failed to init LDAP connection to %1s : %2i	SmLdapMessage::SmObj-LdapInitLdapConnFail	Unable to connect to LDAP server. Make sure your LDAP server is running, and the LDAP server and port are correct. (try ping from the policy server machine.)
SmObjLdap failed to init SSL LDAP connection to %1s : %2i	SmLdapMessage::SmObj-LdapInitSSLLdapFail	Unable to set LDAP option. This is likely a configuration error on the policy server system. Is the proper LDAP library being used?
SmObjLdap failed to init SSL using %1s	SmLdapMessage::SmObj-LdapInitSSLFail	Unable to initialize to LDAP server with SSL. Check the LDAP server and port. Make sure your LDAP server is configured for SSL.
SmObjLdap failed to set LDAP CONNECT_TIMEOUT option	SmLdapMessage::SmObj-LdapConnectTimeoutOptFail	Unable to set LDAP option. This is likely a configuration error on the policy server system. Is the proper LDAP library being used?
SmObjLdap failed to set LDAP PROTOCOL V3 option	SmLdapMessage::SmObj-LdapProtocolV3OptFail	Unable to set LDAP option. This is likely a configuration error on the policy server system. Is the proper LDAP library being used?
SmObjLdap failed to set LDAP RECONNECT option	SmLdapMessage::SmObj-LdapReconnectOptFail	Unable to set LDAP option. This is likely a configuration error on the policy server system. Is the proper LDAP library being used?
SmObjLdap failed to set LDAP THREAD_FN option	SmLdapMessage::SmObjLdap-ThreadFnOptFail	Unable to set LDAP option. This is likely a configuration error on the policy server system. Is the proper LDAP library being used?
SmObjLdap failed to set LDAP TIMELIMIT option	SmLdapMessage::SmObjLdap-TimeoutOptFail	Unable to set LDAP option. This is likely a configuration error on the policy server system. Is the proper LDAP library being used?

Error Message	Function	Description
SmObjLdap failed to set LDAP_OPT_REFERRALS option	SmLdapMessage::SmObj-LdapOptReferralsFail	Unable to set LDAP option. This is likely a configuration error on the policy server system. Is the proper LDAP library being used?
SmObjLdapConnMgr Bind - init. Server: %1s:%2ul	SmLdapMessage::SmObj-LdapConnMgrBindinitServer	The LDAP server configured for the policy store could not be initialized. Troubleshoot the LDAP server specified in the error message.
SmObjLdapConnMgr Bind - SetOption CONNECT_TIMEOUT %1i. Server %2s:%3ul	SmLdapMessage::SmObj-LdapConnMgrBindSetOption-CONNECT_TIMEOUT	The LDAP_X_OPT_CONNECT_TIMEOUT option (LDAP_OPT_SEND_TIMEOUT when using the Microsoft Active Directory SDK) could not be set on the LDAP server configured for the policy store. Troubleshoot the LDAP server specified in the error message.
SmObjLdapConnMgr Bind - SSL client init. Server: %1s:%2ul, Cert DB: %3s	SmLdapMessage::SmObj-LdapConnMgrBindSSLclientinit	The client-side initialization of an SSL connection to the LDAP server configured for the policy store failed. Verify if the certificate database is specified correctly.
SmObjLdapConnMgr Bind - SSL init. Server: %1s:%2ul	SmLdapMessage::SmObj-LdapConnMgrBindSSLinit	The LDAP server configured for the policy store could not be initialized on an SSL connection. Troubleshoot the LDAP server specified in the error message.
SmObjLdapConnMgr Bind. Server %1s:%2ul. Error %3i - %4s	SmLdapMessage::SmObj-LdapConnMgrBindServerError	The CA SiteMinder® Policy Server failed to bind to the LDAP server configured for the policy store. See the included LDAP error message for additional information. Also verify if the Policy Server uses valid LDAP admin credentials. You can reset them in the Data tab in the Policy Server Management Console.
SmObjLdapConnMgr Exception (ldap_init). Server %1s:%2ul	SmLdapMessage::ExcpSm-ObjLdapConnMgrldap_init	The LDAP server configured for the policy store could not be initialized. Troubleshoot the LDAP server specified in the error message.

Error Message	Function	Description
SmObjLdapConnMgr Exception (ldap_simple_bind_s). Server %1s:%2ul	SmLdapMessage::ExcpSm-ObjLdap ConnMgrldap_simple_-bind_s	The CA SiteMinder® Policy Server failed to bind to the LDAP server configured for the policy store. Verify if the Policy Server uses valid LDAP admin credentials. You can reset them in the Data tab in the Policy Server Management Console.
SmObjLdapConnMgr Exception (ldapssl_client_init). Server %1s:%2ul	SmLdapMessage::ExcpSm-ObjLdap ConnMgrldap-ssl_client_init	The client-side initialization of an SSL connection to the LDAP server configured for the policy store failed. Verify if the certificate database is specified correctly.
SmObjLdapConnMgr Exception (ldapssl_init). Server %1s:%2ul	SmLdapMessage::ExcpSm-ObjLdap ConnMgrldapssl_init	The LDAP server configured for the policy store could not be initialized on an SSL connection. Troubleshoot the LDAP server specified in the error message.
Terminating the server/process.....	SmLdapMes-sage::TerminatingSer ver-Processes	Shutting down server process so important reconfiguration may take place. See previous error in log.
Unable to fetch more than %1i data entries from the Data Store. \n %2s LDAP_SIZELIMIT_EXCEEDED, Error has been detected. \n %3s Please re-configure the sizelimit parameter of your Directory Server, \n %4s as suggested in your \""Directory Server Manual\"" \n %5s or bind the Directory Server with root dn to overcome this problem. \n %6s Ex : For Iplanet / Netscape, bind the Directory Server as \""cn=Directory Manager\""	SmLdapMessage::Unable-ToFetch MoreEntriesFromData-Source	Increase sizelimit parameter of your LDAP server
Unable to retrieve LDAP directory type	SmLdapMessage::Unable-ToRetrie veLdapDir	Unable to determine LDAP vendor and type. Is the target server one of the supported LDAP servers? Processing will continue but further unexpected errors may occur.

Error Message	Function	Description
Unable to search and fetch more data entries from the Data Store. \n %1s LDAP_SIZELIMIT_EXCEEDED, Error has been detected. \n %2s Please re-configure the sizelimit parameter of your Directory Server, \n %3s as suggested in your \""Directory Server Manual\"" \n %4s or bind the Directory Server with root dn to overcome this problem. \n %5s Ex : For Iplanet / Netscape, bind the Directory Server as \""cn=Directory Manager\""	SmLdapMessage::Unable-ToSearch FetchMore-EntriesFromDataSourc e	The Policy Server cannot retrieve more data from the directory server. See the error message text for possible configuration changes.
Unexpected value of 'arg' argument in rebindproc %1i	SmLdapMes-sage::UnexpectedVal ueArg-Argument	An illegal value is being passed as the 'arg' argument in a rebindproc call. The rebindproc function is set as a rebind callback for automatic referral handling. Try enabling enhanced referral handling instead.
Unexpected value of 'arg' argument in rebindproc_sm %1i	SmLdapMes-sage::UnexpectedVal ueArg-Argument2	An illegal value is being passed as the 'arg' argument in a rebindproc_sm call. The rebindproc_sm function is set as a rebind callback for automatic referral handling. Try enabling enhanced referral handling instead.
Unknown value of ’freeit’ argument in rebindproc_sm %1i	SmLdapMes-sage::UnexpectedVal ueFreeit-Argument	An illegal value is being passed as the freeit argument in a rebindproc call (only 0 and 1 are allowed). The rebindproc function is set as a rebind callback for automatic referral handling Try enabling enhanced referral handling instead.

Error Message	Function	Description
Unknown value of 'freeit' argument in rebindproc_sm %1i	SmLdapMes-sage::UnexpectedValue-FreeitArgument2	An illegal value is being passed as the freeit argument in a rebindproc_sm call (only 0 and 1 are allowed). The rebindproc_sm function is set as a rebind callback for automatic referral handling (doesn't apply when using Microsoft Active Directory SDK). Try enabling enhanced referral handling instead.

ODBC

Error Message	Function	Description
Could not save IMS Environments. Possibly missing schema support	SmOdbcMessage::IMSSave-ErrorMissingSchema	Policy server database does not have a schema that supports IMS.
Database Error executing query (%1s) . Unknown failure.	SmOdbcMessage::Unknown-FailureDBExecQuery	An unknown error or exception has occurred while trying to execute the given SQL statement.
Database Error executing query (%1s) . Unknown failure.	SmOdbcMessage::Unknown-FailureExecODBCQuery	An unknown error or exception has occurred while trying to execute the given SQL statement.
Database Error executing query ('%1s'). Error: %2s .	SmOdbcMessage::DBError-ExecQuery	The given error occurred while trying to execute the given SQL statement.
Database Error executing query ('%1s'). Unknown failure.	SmOdbcMessage::Unknown-ExceptionDBExecQuery	An unknown error or exception has occurred while trying to execute the given SQL statement.
Database Error executing query. Error: %1s .	SmOdbcMessage::ErrorDB-ExecQuery	The given error occurred while trying to execute the a SQL query.
Database error getting escape chars. Error: %1s.	SmOdbcMessage::DBError-GetEscapeChar	Error occurred when trying to establish the escape character for use with the database.
Database error getting escape chars: unknown failure.	SmOdbcMessage::Unknown-ExceptionDBGetEscapeChar	An unknown exception occurred when trying to establish the escape character for use with the database.

Error Message	Function	Description
DB Warning: Data truncation will occur with data value: '%1s' Actual length: '%2u' Maximum allowed length: '%3u	'SmOdbcMessage::Data-TruncationInfo	A data value for the given input has exceeded the maximum allowed length. The value will be truncated to the maximum length given.
Error Code is %1i message is '%2s'.	SmOdbcMessage::ErrorCode-And Message	A failure occurred trying to connect to the given data source. An error code and error message is given indicating the problem.
Error Code is %1i.	SmOdbcMessage::ErrorCode	A failure occurred trying to connect to the given data source. An error code is given indicating the problem.
Failed to allocate query for user directory with oid: '%1s'.	SmOdbcMessage::FailedTo-AllocMemForUserDir	Failed to allocate the queries used for the user directory specified by the given OID.
Failed to connect to any of the following data sources: '%1s'.	SmOdbcMessage::FailedTo-ConnectToAnyOfDataSources	Failed to connect to any of the User Directories specified.
Failed to connect to data-source '%1s'.	SmOdbcMessage::FailedTo-ConnectToDataSource	A failure occurred trying to connect to the given data source.
Failed to fetch query for user directory with oid: '%1s'.	SmOdbcMessage::FailedTo-FetchQueryForUserDir	Search for the User Directory Query with the given oid failed.
Failed to fetch user directory with oid: '%1s'.	SmOdbcMessage::FailedTo-FetchUserDir	Search for the User Directory with the given oid failed.
Failed to find data source name for database '%1s'.	SmOdbcMessage::FailedTo-FindDataSource	Could not find ""ProviderNameSpace"" registry key for the given CA SiteMinder® database
Failed to find query definition for %1s	SmOdbcMessage::FailTo-FindQueryDefinition	Failed to find the query definition for the given query.
Failed to init DataDirect ODBC driver. Unable to load function '%1s' in library '%2s'.	DataDirectODBCDriverFunc-LoadFail	Failed to initialize the DataDirect ODBC libraries. The given initialization function could not be found in the provided library.

Error Message	Function	Description
Failed to init DataDirect ODBC driver. Unable to load library '%1s	SmOdbcMessage::DataDirect-ODBCDriverLibLoadFail	Could not load the given ODBC library. Please check to your library paths include the CA SiteMinder® ODBC library directory.
Failed to load ODBC branding library '%1s' .	SmOdbcMessage::ODBC-BrandingLibraryLoadFail	Failed to load the ODBC libraries that are branded for use by CA SiteMinder®.
Failed to resolve name of the ODBC branding library.	SmOdbcMessage::ODBC-BrandingLibraryNameResolve-Fail	Failed to resolve the name of the branding library. The library name is indicated from the registry Key OdbcBrandingLib located in the registry under Netegrity/Siteminder/Database
Failed to retrieve database registry keys for database '%1s'.	SmOdbcMessage::FailedTo-RetrieveDBRegKeys	Could not find one of the following registry keys (Data Source, User Name, or Password) for the given CA SiteMinder® Database.
Invalid credentials or server not found attempting to connect to '%1s' server '%2s'.	SmOdbcMessage::Unable-ToConnect	Invalid credentials supplied for accessing a CA SiteMinder® ODBC database.
ODBC Error executing query ('%1s') . Error: %2s.	SmOdbcMessage::ErrorExec-ODBCQuery	The given ODBC error occurred while trying to execute the given SQL statement.
ODBC Error executing query. Error: %1s.	SmOdbcMessage::Error-ODBCQueryExec	The given ODBC error occurred while trying to execute a SQL query.
ODBC Error executing query. Unknown failure	SmOdbcMessage::Unknown-ExceptionExecODBCQuery	An unknown exception occurred when trying to execute a SQL query against an ODBC database.

Directory Access

Message	Message ID	Description
%1s failed for path '%2s	'FuncFailForPath	The policy server failed to get directory information using the custom provider.
ADs EnumContainer failed; Error %1xl. %2s	ADsEnumContainerFailed	The policy server failed to enumerate container members through the ADSI interface.
ADs Get failed for property '%1s' ; Error %2xl. %3s	ADsGetFailForProperty	The policy server failed to get user property through the ADSI interface.
ADs GetGroups failed; Error %1xl. %2s	ADsGetGroupsFail	The policy server failed to get user groups.
ADs Put failed for property '%1s' ; Error %2xl. %3s	ADsPutFailForProperty	The policy server failed to set user property through the ADSI interface.
ADs put_Filter failed; Error %1xl. %2s	ADsPutFilterFailed	The policy server failed to create enumeration filter through the ADSI interface.
ADs Search failed; Error %1xl. %2s	ADsSearchFail	The policy server failed to search through the ADSI interface.
ADsBuildEnumerator failed; Error %1xl. %2s	ADsBuildEnumeratorFailed	The policy server failed to enumerate container members through the ADSI interface.
ADsBuildVarArrayStr failed; Error %1xl. %2s	ADsBuildVarArrayStrFailed	The policy server failed to build a variable array through the ADSI interface.
ADsEnumerateNext failed; Error %xl. %2s	ADsEnumerateNextFailed	The policy server failed to enumerate container members through the ADSI interface.
ADsGetObject failed; Error %1xl. %2s	ADsGetObjectFail	The policy server failed to get object properties through the ADSI interface.
ADsOpenObject failed on '%1s' . ADSI Error %2xl. %3s	ADsOpenObjectFailed	The policy server failed to create a handle to the ADSI interface.

Message	Message ID	Description
Affiliate PropertyCollection does not match group name	AffiliatePropertyCollection-GroupNameMismatch	The policy server failed to validate affiliate relationship to a policy. The affiliate property collection name does not match the specified policy name.
Could not fetch properties using '%1s' function	PropertiesFetchFail	The policy server failed to fetch object properties through the custom provider.
Exception in SmDsObj	SmDsObjUnknownException	The policy server failed to lookup a DS provider. Check if the provider shared library can be loaded by the policy server process.
Exception in SmDsObj: %1s	SmDsObjException	The policy server failed to lookup a DS provider. Check if the provider shared library is accessible by the policy server process.
Failed to find an Affiliate PropertyCollections	AffiliatePropertyCollectionsFail	The policy server failed to fetch an affiliate domain. Check the policy store for consistency.
Failed to find attribute	AttributeFindFail	The policy server failed to find the specified user attribute.
Failed to find password property	PasswordPropertyFindFail	The policy server failed to find password for the specified affiliate.
Failed to find Property in PropertySection acting as Affiliate user	AffilateUserPropertyIn-PropertySectionFindFail	The policy server failed to fetch the specified affiliate property.
Failed to find Property-Collection acting as Affiliate user directory	ActingAffiliateUserDirProps-FindFail	The policy server failed to fetch an affiliate domain. Check the policy store for consistency.
Failed to find PropertySection as Affiliate user	AffilateUserPropertySection-FindFail	The policy server failed to lookup the specified affiliate.
Failed to find PropertySection in Affiliate user directory	InAffiliateUserDirPropsFindFail	The policy server failed to fetch an affiliate from the affiliate domain. Check the policy store for consistency.

Message	Message ID	Description
Failed to find root object!	RootObjFindFail	The policy server failed to find affiliate domains. Check if affiliate objects are visible through the CA SiteMinder® Administration UI.
Failed to find user in Affiliate PropertyCollection	AffiliatePropertyCollection-UserFindFail	The policy server failed to lookup the specified affiliate.
Failed to initialize custom directory API module '%1s	'CustomDirAPIModInitFail	The policy server failed to initialize the custom provider library.
Failed to load custom directory API library '%1s'. System error: %2s	CustormDirAPILibLoadFail	The policy server failed to load the custom provider library. Check if the appropriate custom provider library is accessible by the policy server process.
Failed to resolve function '%1s' in custom directory API library '%2s'. System error: %3s	CustormDirAPILibFuncResovl-Fail	The policy server failed to initialize the custom provider library. Check if the appropriate custom provider library is accessible by the policy server process.
Get Disabled State not supported for namespace ADSI	ADSIGetDisabledState-Supported	The policy server does not support getting user disabled state through the ADSI interface.
No function '%1s' is available in custom directory API library '%2s'	CustomDirAPILibFunctNot-Found	The policy server failed to find one of the required methods in the custom provider library. Check if the appropriate custom provider library is accessible by the policy server process.
Password change not supported for namespace ADSI	ADSINoPasswordChange	The policy server does not support changing user password through the ADSI interface.
Password change not supported for namespace LanMan:	LanManPasswordChangeNot-Supported	The policy server LanMan provider does not support changing user passwords.
QueryInterface (IID_IADsContainer) failed; Error %1s %2s %3i . %4s	IID_IADsContainerFail	The policy server failed to enumerate container members through the ADSI interface.
QueryInterface (IID_IADsContainer) failed; Error %1xl. %2s	QueryInterfaceIID_IADs-ContainerFail	The policy server failed to enumerate container members through the ADSI interface.

Message	Message ID	Description
QueryInterface (IID_IADsUser) failed; Error %1xl. %2s	IID_IADsUserFail	The policy server failed to get user groups.
QueryInterface (IID_IDirectorySearch) failed; Error %1xl. %2s	IID_IDirectorySearchFail	The policy server failed to search through the ADSI interface.
Set Disabled State not supported for namespace ADSI	ADSISetDisabledState-Supported	The policy server does not support setting user disabled state through the ADSI interface.
Unsupported function called: SmDirAddEntry	UnsupportedFuncCallSmDir-AddEntry	The SmDirAddEntry function is not supported by the affiliate provider library.
Unsupported function called: SmDirAddMemberToGroup	UnsupportedFuncCallSmDir-AddMemberToGroup	The SmDirAddMemberToGroup function is not supported by the affiliate provider library.
Unsupported function called: SmDirAddMemberToRole	UnsupportedFuncCallSmDir-AddMemberToRole	The SmDirAddMemberToRole function is not supported by the affiliate provider library.
Unsupported function called: SmDirChangeUserPassword	UnsupportedFuncCallSmDir-ChangeUserPassword	The SmDirChangeUserPassword function is not supported by the affiliate provider library.
Unsupported function called: SmDirGetGroupMembers	UnsupportedFuncCallSmDir-GetGroupMembers	The SmDirGetGroupMembers function is not supported by the affiliate provider library.
Unsupported function called: SmDirGetRoleMembers	UnsupportedFuncCallSmDir-GetRoleMembers	The SmDirGetRoleMembers function is not supported by the affiliate provider library.
Unsupported function called: SmDirGetUserAttrMulti	UnsupportedFuncCallSmDir-GetUserAttrMulti	The SmDirGetUserAttrMulti function is not supported by the affiliate provider library.
Unsupported function called: SmDirGetUserClasses	UnsupportedFuncCallSmDir-GetUserClasses	The SmDirGetUserClasses function is not supported by the affiliate provider library.
Unsupported function called: SmDirGetUserGroups	UnsupportedFuncCallSmDir-GetUserGroups	The SmDirGetUserGroups function is not supported by the affiliate provider library.
Unsupported function called: SmDirGetUserProperties	UnsupportedFuncCallSmDir-GetUserProperties	The SmDirGetUserProperties function is not supported by the affiliate provider library.

Message	Message ID	Description
Unsupported function called: SmDirGetUserRoles	UnsupportedFuncCallSmDir-GetUserRoles	The SmDirGetUserRoles function is not supported by the affiliate provider library.
Unsupported function called: SmDirLookup	UnsupportedFuncCallSmDir-Lookup	The SmDirLookup function is not supported by the affiliate provider library.
Unsupported function called: SmDirRemoveEntry	UnsupportedFuncCallSmDir-RemoveEntry	The SmDirRemoveEntry function is not supported by the affiliate provider library.
Unsupported function called: SmDirRemoveMemberFrom-Group	UnsupportedFuncCallSmDir-RemoveMemberFromGroup	The SmDirRemoveMemberFromGroup function is not supported by the affiliate provider library.
Unsupported function called: SmDirRemoveMemberFrom-Role	UnsupportedFuncCallSmDir-RemoveMemberFromRole	The SmDirRemoveMemberFromRole function is not supported by the affiliate provider library.
Unsupported function called: SmDirSearch	UnsupportedFuncCallSmDir-Search	The SmDirSearch function is not supported by the affiliate provider library.
Unsupported function called: SmDirSearchCount	UnsupportedFuncCallSmDir-SearchCount	The SmDirSearchCount function is not supported by the affiliate provider library.
Unsupported function called: SmDirSetUserAttr	UnsupportedFuncCallSmDir-SetUserAttr	The SmDirSetUserAttr function is not supported by the affiliate provider library.
Unsupported function called: SmDirSetUserAttrMulti	UnsupportedFuncCallSmDir-SetUserAttrMulti	The SmDirSetUserAttrMulti function is not supported by the affiliate provider library.
Unsupported function called: SmDirSetUserDisabledState	UnsupportedFuncCallSmDir-SetUserDisabledState	The SmDirSetUserDisabledState function is not supported by the affiliate provider library.

Tunnel

Error Message	Function	Description
Bad security handshake attempt. Handshake error: %1i	SmTunnelMessage::Hand-shakeAttemptError	The client/server security handshake failed due to the specified system error.
Client cannot encrypt data successfully during handshake	SmTunnelMessage::Client-EncryptFail	The client/server security handshake failed. The client could not properly encrypt its handshake messages.
Exception caught during handshake attempt	SmTunnelMessage::ExcpIn-HandshakeAttempt	An unspecified error occurred during the client/server security handshake.
Failed to initialize tunnel service library '%1s'. %2s	SmTunnelMessage::Tunnel-ServiceLibInitFail	The requested tunnel service library failed initialization.
Failed to load tunnel service library '%1s'. System error: %2s	SmTunnelMessage::Tunnel-ServiceLibLoadFail	The requested tunnel service library could not be loaded.
Failed to resolve function '%1s' in tunnel service library '%2s'. System error: %3s	SmTunnelMessage::Tunnel-ServiceLibFuncResolveFail	The requested function could not be found in the requested tunnel service library due to a system error.
Handshake error: Bad host-name in hello message	SmTunnelMessage::Hand-shakeErrorBadHostname	The client/server security handshake failed. The initial message from the client to the server contained an incorrect host name.
Handshake error: Bad version number in hello message	SmTunnelMessage::Hand-shakeErrorBadVersionNo	The client/server security handshake failed. The initial message from the client to the server contained an incorrect version number.
Handshake error: Failed to receive client ack. Socket error %1i	SmTunnelMessage::Hand-shakeErrorToReceiveClientACK	The client/server security handshake failed. The initial message from the server to the client was not acknowledged by the client.
Handshake error: Failed to receive client hello. Client disconnected	SmTunnelMessage::Hand-shakeErrorClientHelloNot-Receive	The client/server security handshake failed. The client disconnted the connection before sending the initial message.

Error Message	Function	Description
Handshake error: Failed to receive client hello. Socket error %1i	SmTunnelMessage::Hand-shakeErrorSocketError	The client/server security handshake failed. The client did not send the initial message.
Handshake error: Failed to send server hello. Socket error %1i	SmTunnelMessage::Hand-ShakeErrorInSendSocketError	The client/server security handshake failed. The initial message from the server to the client couldn't be sent due to a communications failure.
Handshake error: Shared secret incorrect for this client	SmTunnelMessage::Hand-shakeErrorSharedSecret-Incorrect	The client/server security handshake failed. The initial message from the client to the server contained an incorrect shared secret.
This Policy Server version does not support 3.6 agents	SmTunnelMessage::Agent-VersionNotSupported	The client/server security handshake failed. The version of the client is no longer allowed to establish a tunnel connection.
Tunnel callers are not allowed to execute request %1ul	SmTunnelMessage::Tunnel-CallerExecDenied	A Tunnel call attempted to make a request that is disallowed.
Unexpected handshake error	SmTunnelMessage::Hand-shakeErrorUnexpected	The client/server security handshake failed for an unexpected reason.
Unknown Exception caught while publishing Tunnel Libs	SmTunnelMessage::Unknown-ExcpPublishTunnelLibs	An unknown exception occurred while a tunnel service library was describing itself through its publishing interface.

Index

No index entries found.