CA SiteMinder®

Policy Server Management Guide

r6.0 SP6

Second Edition

CA Technologies Product References

This document references the following CA Technologies products:

- CA SiteMinder®
- CA TransactionMinder®
- CA Identity Manager

Contact CA Technologies

Contact CA Support

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

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

Provide Feedback

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

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

Contents

Chapter 1: Policy Server Management Overview

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:

- SiteMinder--Combines the Policy Server with Web Agents to provide access control for Web servers.
- TransactionMinder--Provides access control for XML-based transactions. If you have purchased TransactionMinder, see the *CA TransactionMinder Operations Guide* for more information.
- CA Identity Manager--Provides identity management services, see *CA Identity Manager Operations Guide* for more information.

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

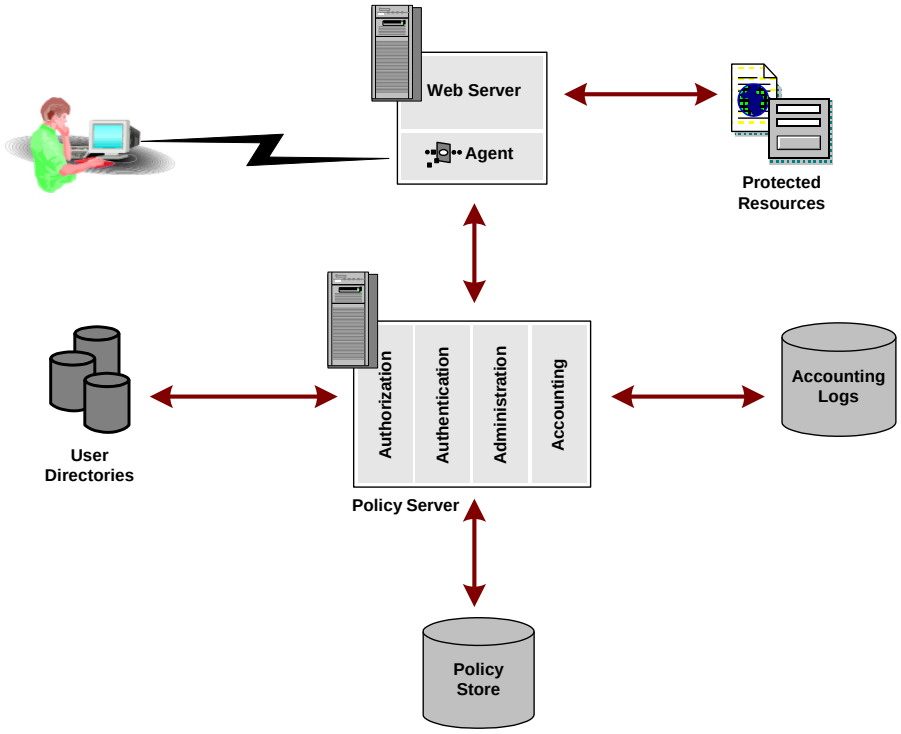
Additional components are included with various CA products, for example, SiteMinder Agents. SiteMinder Agents are integrated with a standard Web server or application server. They enable SiteMinder to manage access to Web applications and content according to predefined security policies. Other types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

Policy Server Overview

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

- **Authentication**--The Policy Server supports a range of authentication methods. It can authenticate users based on user names and passwords, via 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 Policy Server User Interface (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. Once 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 *Developer's Guide for C* and the *Java API Documentation*.

How to Manage the Policy Server Environment

As a Policy Server manager, 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 *Policy Server User Interface*.

Policy Server management tasks include the following:

- 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 Tools

Policy Server management tools include:

- The Policy Server management console
- The Policy Server User interface

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

To open the Management Console

- (Windows) Use the Policy Server Management Console shortcut in the SiteMinder program group
- (UNIX) Run *install_dir*/siteminder/bin/smconsole.

Note: Consider the following:

- (Windows 2008) If the Policy Server is installed on Windows 2008, right–click the shortcut and select Run as administrator.
- (UNIX) The X display server must be running and the display enabled by 'export DISPLAY=n.n.n.n:0.0', where n.n.n.n is 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 Policy Server User Interface lets you create and manage Policy Server objects.

To open the Policy Server User Interface

1. Open your web browser.
2. Enter the following URL in the Address bar:

   `http://policy_server_host_name.domain:non_default_port_number/siteminder`

Note: The *policy_server_host_name* is the name of the machine on which the Policy Server is installed. You must use a fully-qualified domain name, such as example.com, in the URL. If the Policy Server does *not* use the default HTTP port (80), you must specify a port number.

Your browser displays the Policy Server start page.

3. Click Administer Policy Server.

   A status bar appears while the Policy Server User Interface loads. The SiteMinder Administration Login window opens.

4. Enter your user name and password in the appropriate fields.

   If you are accessing the Policy Server for the first time, use the default super user administrator account, which you created during Policy Server installation.

5. Click Login.

   The Policy Server User Interface opens.

   The contents of this window depend on the privileges of the administrator account you use to login to the Policy Server.

   Note: For more information on the Policy Server User Interface, see the SiteMinder *Policy Design* guide.

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.

Policy Server Processes

The following lists the main Policy Server processes for Windows and UNIX:

Windows

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.

UNIX

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

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:

Management Console--Status Tab Fields and Controls (see page 159)

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\Netegrity\SiteMinder\CurrentVersion\Policy Server.
   - (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 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 Policy Server databases (policy store, key store, and audit logs) from the Management Console Data tab.

To configure Policy Server data storage 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, even if you are logged into the system as an Administrator. For more information, see the release notes for your SiteMinder component.

2. Click the Data tab.

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

3. Select the database that you want to configure from the Database drop-down list. The database you select determines the storage possibilities that are available for that database type and presented on the Storage drop-down list.

   Note: The table at the end of this procedure lists the databases you can configure and the storage options available for each one. The combination of these settings determines the settings displayed in the context-sensitive group box below them.

4. Select a storage type for the selected database from the Storage drop-down list.

5. Configure data storage options for the chosen Policy Server database in the context-sensitive group box below the Database and Storage controls.
6. When you have finished, click Apply to save your settings, or click OK to save the settings and exit the Management Console.

The following table lists SiteMinder database types and the available storage options:

Database	Database Description	Available Storage
Policy Store	The database for the Policy Store. You *must* specify the Policy Store database.	LDAP ODBC
Key Store	The database that contains keys used to encrypt cookies created by SiteMinder Agents.	LDAP ODBC
Audit Logs	The database where you store audit logs containing event information.	ODBC Text file
Session Server	The database in which the session server stores persistent session data.	ODBC

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 29).

   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.

More Information:

Configure LDAP Storage Options (see page 32)
Configure ODBC Storage Options (see page 35)
Management Console--Data Tab Fields and Controls (see page 165)

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 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.

More information:

Management Console--Data Tab Fields and Controls (see page 165)

Configure a Separate Database for the Key Store

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

More information:

Configure LDAP Storage Options (see page 32)
Configure ODBC Storage Options (see page 35)
Management Console--Data Tab Fields and Controls (see page 165)

Configure a Separate Database for the Audit Logs

The audit log database is where the Policy Server stores audit logs containing event information. These settings may reduce Policy Server performance. If this is a problem, configure auditing data logs in a text file instead of database.

To configure a separate database for audit logs

1. Choose Audit Log from the Database drop-down list.
2. Choose an available storage type (ODBC or Text file) 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, you should consider the following factors:

- SiteMinder Reporting requires that the audit logs are written to an ODBC database. Reporting will not function if the audit logs are written to a text file.
- SiteMinder audit logging to an ODBC database and to a text file supports internationalization (I18N).
- By default, SiteMinder administrator changes to policy store objects are not written to the audit database. These changes, by default, are written to a set of text files that are located at *siteminder_home*\audit. Although this information is not written to the audit database, you can configure SiteMinder to include these events in reports.
- If your Policy Server will operate under heavy load, you should consider logging to a text file rather than an ODBC database. However, if you do log to an ODBC database, you should set the following registry key values in the HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Database\ registry location to prevent loss of auditing data under heavy load:

  ConnectionHangwaitTime

  Set to 60 seconds for heavy loads. The default is 30 seconds.

  QueryTimeout

  Set to 30 seconds for heavy loads. The default is 15 seconds.

  LoginTimeout

  Set to 30 seconds for heavy loads. The default is 15 seconds.

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

Configure a Database for the Session Server

The session server database is where the Policy Server Session Server stores persistent session data.

To configure a database for the session server

1. Choose Session Server from the Database drop-down list.
2. Choose an available storage type from the Storage drop-down list.
3. Set the Enable Session Server option.

   You should only enable the Session Server if you are going to use persistent sessions in one or more realms; when enabled, the Session Server impacts Policy Server performance.

   Note: The Use Policy Store database check box is disabled. For performance reasons, the session server cannot be run on the same database as the policy store.

4. Specify Storage Options appropriate for the chosen storage type.
5. Click OK to save the settings and exit the Console.

Configure Session Server Timeout for Heavy Load Conditions

Under extremely heavy load conditions, long-running queries necessary for Session Server maintenance tasks, such as removing idled-out or expired sessions, can timeout. You can adjust the timeout for Session Server maintenance tasks (60 seconds by default), by increasing the value of the MaintenanceQueryTimeout registry setting to allow the maintenance thread to complete its' tasks successfully. The MaintenanceQueryTimeout registry setting can be found at the following registry location:

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

Configure LDAP Storage Options

Use the LDAP context-sensitive storage controls to point to an LDAP directory configured to be used as a policy store to hold policy information or to point to an LDAP directory configured to be used as a key store.

Note: Whenever you update parameters relating to an LDAP database, restart the Policy Server to make the new parameters effective.

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 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 SiteMinder's LDAP referral handling to improve performance and redundancy. Previous versions of 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.

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 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, even if you are logged into the system as an Administrator. For more information, see the release notes for your 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 Policy Server User Interface performance issues.

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

Max AdmComm Buffer Size

Specifies the Policy Server User Interface buffer size (specifically, the maximum amount of data, in bytes, that is passed from the Policy Server to the Policy Server User Interface in a single packet).

The Max AdmComm Buffer Size registry setting should be configured at the following registry location:

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

The value of this setting must be set very carefully as allocation of a larger buffer results in a decrease in overall performance. The acceptable range of Max AdmComm Buffer Size is 256KB to 2 GB. The default value this is 256KB (also applies when this registry setting does not exist).

SearchTimeout

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

The SearchTimeout registry setting should be configured at the following registry location:

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

The appropriate value for this setting depends upon and can vary according to several factors including network speed, size of the LDAP search query response, the LDAP connection state, load on LDAP server, and so on. The value should be large enough to prevent LDAP timeout when fetching large amounts of policy store data from the LDAP server. The default value is 20 seconds (also applies when this registry setting does not exist).

More information:

Configure the Policy Store Database (see page 28)
Configure a Separate Database for the Key Store (see page 30)
Policy Server Management Console (see page 157)
Management Console--Data Tab Fields and Controls (see page 165)

Configure ODBC Storage Options

Use the ODBC context-sensitive storage controls to configure an ODBC data source to hold the policy store, key store, audit logs, or session server data.

Note: For more information about installing ODBC data sources, see the *SiteMinder 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 SiteMinder Data Source1,SiteMinder Data Source2 in the Data Source Name field causes the Policy Server to look at Data Source 1 first. If SiteMinder Data Source1 does not respond, the Policy Server automatically looks for 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.

More information:

Management Console--Data Tab Fields and Controls (see page 165)

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\Netegrity\SiteMinder\CurrentVersion\Ds
   \ODBCProvider
   ```

   Solaris

   Add the following lines to the sm.registry file:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Ds
   \ODBCProvider=35921
   MaxResults=0x1; REG_DWORD
   ```

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

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 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). To allow escaping the preceding characters, enable the following registry key:
[HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Reports]
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 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\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 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 SiteMinder 5.x or 6.x schema. For more information about how to configure an ODBC database with SiteMinder schema, see the *Policy Server Installation Guide*.

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

To import audit data into an ODBC database

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

   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.

   -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

-s5 | -s6

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

Default: Supports an ODBC database 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 cert7.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 cert7.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 Policy Server User Interface 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 30)

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, even if you are logged into the system as an Administrator. For more information, see the release notes for your SiteMinder component.

2. Click the 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 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.

More information:

Management Console--Settings Tab Fields and Controls (see page 160)

Configure Policy Server Administration Settings

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

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

More information:

Management Console--Settings Tab Fields and Controls (see page 160)

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.

More information:

Management Console--Settings Tab Fields and Controls (see page 160)

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.

More information:

Management Console--Settings Tab Fields and Controls (see page 160)

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.

More information:

Management Console--Settings Tab Fields and Controls (see page 160)

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.

More information:

Management Console--Settings Tab Fields and Controls (see page 160)

Chapter 5: 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 Policy Server User Interface.

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, even if you are logged into the system as an Administrator. For more information, see the release notes for your SiteMinder component.

2. Click the 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 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.

More information:

Management Console--Super User Tab (see page 169)

Chapter 6: Configuring and Managing Encryption Keys

This section contains the following topics:

Policy Server Encryption Keys Overview

The Policy Server and Agents (SiteMinder and TransactionMinder) 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 can be read by all agents in a single sign-on environment and that are shared by all agents in a single sign-on environment, because 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, because 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.

Note: More information about configuring a key store exists in Management Console--Data Tab Fields and Controls (see page 165).

Other, special keys are:

- A *Policy store key* is used to encrypt certain data in the policy store. The policy store key is encrypted and stored 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 the Policy Server is installed.
- 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.

Cryptographic Hardware Support

Because the policy store key is used directly or indirectly to encrypt all other keys, it is the Policy Server's most critical key and the most important key to protect. Cryptographic hardware is no longer supported. Without it, the policy store key is stored in the key stash file using a proprietary encryption technique.

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 also ensures the integrity of the keys. For SiteMinder Agents that are configured for single sign-on, the key store must be replicated and shared across all SiteMinder environments in the single sign-on environment.

If the Policy Server determines that a key store that was configured separately from the policy store is unavailable, it attempts to reconnect to the key store to determine if it has come back online. 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, at which point the Policy Server 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.

You manage keys using the SiteMinder Key Management dialog box in the Policy Server User Interface.

Agent Keys

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 and TransactionMinder Agents. Dynamic keys can be rolled over at a regular interval, or by using the Key Management dialog box of the Policy Server User Interface. 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 51)
Static Keys (see page 53)
Manage Agent Keys (see page 61)

Dynamic Agent Key Rollover

Dynamic Agent key rollover is configured in the Key Management dialog of the Policy Server User Interface. 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 *SiteMinder Web Agent 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.

More information:

Manage Agent Keys (see page 61)

Agent Keys Used in Dynamic Key Rollover

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.

More information:

Static Keys (see page 53)

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 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 makes use to 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. For information on HTML Forms authentication, see the *SiteMinder Policy Design Guide.*

- 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 reauthenticate, and user tracking information becomes invalid. In addition, if the static key is used for single sign-on, users will be challenged for credentials when they attempt to access resources in another cookie domain.

More information:

Multiple Policy Stores with Separate Key Stores (see page 59)
Change Static Keys (see page 65)
Agent Keys (see page 51)

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 SiteMinder Key Management dialog box. For security reasons, the randomly generated key is recommended. However, if your SiteMinder implementation includes multiple key stores in a single sign-on environment, you must enter the same session ticket key for all key stores.

More information:

Cache Management Overview (see page 87)
Manage the Session Ticket Key (see page 67)

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 33)
Configure ODBC Failover (see page 36)

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 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 (http://www.ca.com/support) and search for the SiteMinder r6.0 SP6 Platform Support Matrix.

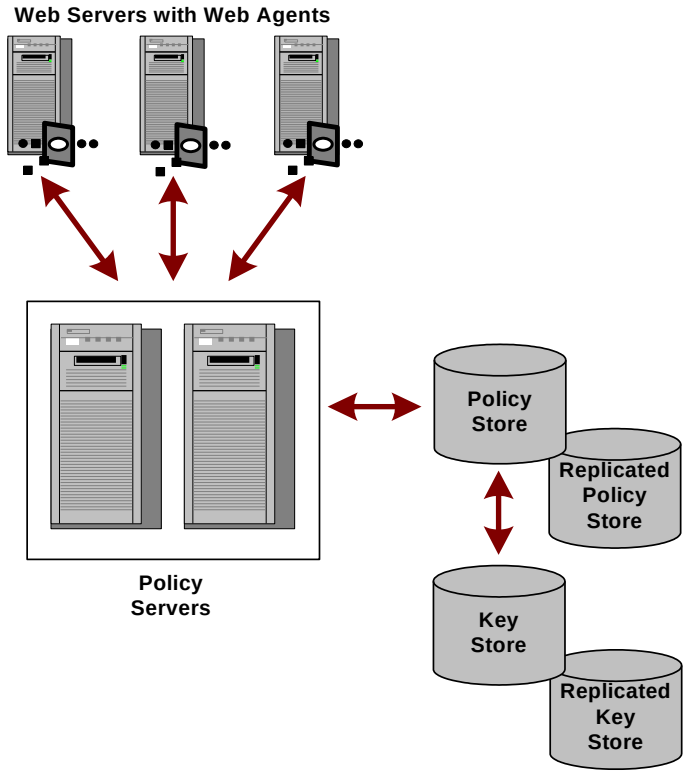
More information:

Configure Agent Key Generation (see page 61)
Configure LDAP Failover (see page 33)
Configure ODBC Failover (see page 36)

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.

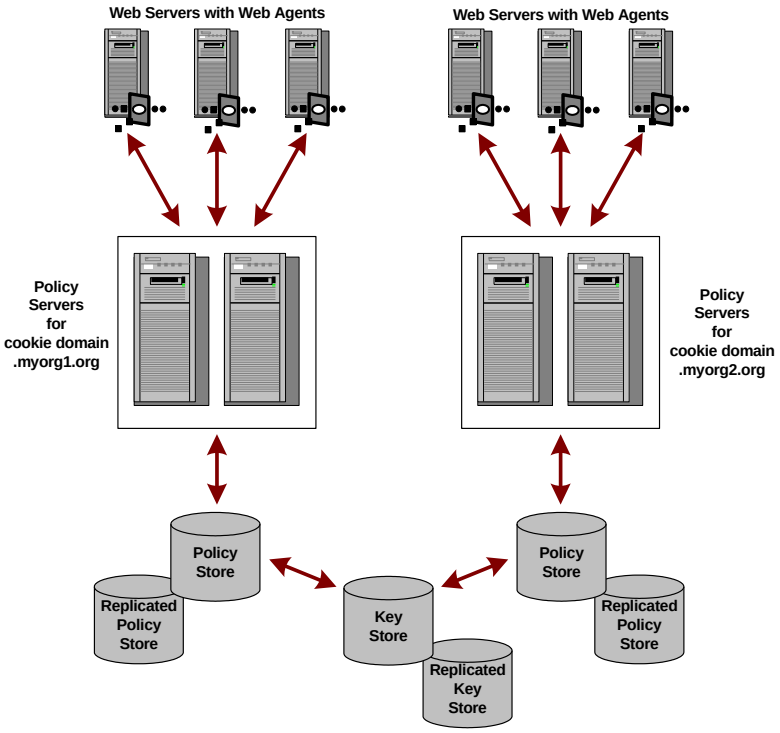
More information:

Key Management Considerations (see page 55)

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 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.

More information:

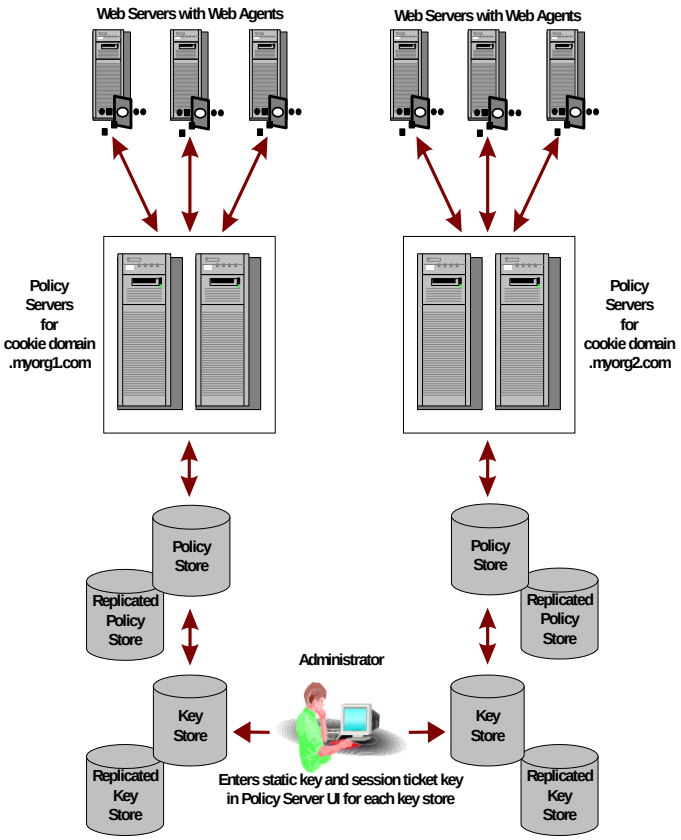
Key Management Considerations (see page 55)
Set the EnableKeyUpdate Registry Key (see page 68)
Management Console--Keys Tab (see page 169)

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 SiteMinder Web Agents.

More information:

Key Management Considerations (see page 55)

Reset the Policy Store Encryption Key

To reset the policy store Encryption Key

1. Export your existing policy store content in clear text.
2. Run smldapsetup remove to clear the policy store content and SiteMinder schema.
3. Run "smreg -key *new_encryption_key*" to reset the Encryption Key.
4. Reboot the machine.
5. Load the Policy Server Management Console and retype the Admin password for the Directory Server.
6. Open a command prompt.
7. Run "smldapsetup ldgen -f*any_filename_to_store_new_schema* -v".
   The LDAP instance is correctly identified.
8. Run "smldapsetup ldmod -f*previous_filename* -v"
   LDAP is modified with the schema file.
9. Run "smreg -su *SiteMinder_admin_password*" to reset SiteMinder Administrator password.
10. Run "smobjimport -i*smpolicy.smdif file* -dsiteminder -wpassword -v" to import SiteMinder policy store base contents to LDAP.
11. Run "smobjimport -i*the_original_exported_policy_export_file*.smdif> -dsiteminder -wpassword -v" to restore the original content of policy store.

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

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.

To configure Policy Server agent key generation

1. Start the Policy Server Management Console.

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

2. Click the 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.

More information:

Management Console--Keys Tab (see page 169)

Manage Agent Keys

The SiteMinder Key Management dialog box, which you access from the Policy Server User Interface, enables you to configure periodic Agent key rollovers, execute manual rollovers, and change the static key that Web Agents use for the features described above.

It also enables you to manage the session ticket key.

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

More information:

Configure Periodic Key Rollover (see page 62)
Manually Rollover the Key (see page 64)
Change Static Keys (see page 65)
Manage the Session Ticket Key (see page 67)

Configure Periodic Key Rollover

The Policy Server supports periodic Agent key rollovers weekly, daily, or at fixed intervals in a single day. The shortest allowable period between rollovers is one hour.

To enable periodic Agent key rollover, the Enable Agent Key Generation check box must be selected in the Keys tab of the Policy Server Management Console.

Note: If your operating system is not configured to adjust the system time for daylight savings time, key rollover may be offset by one hour. To ensure that key rollover occurs at the expected time, configure your operating system to recognize daylight savings time.

To configure periodic key rollover

1. Log into the Policy Server User Interface.
2. From the menu bar of the SiteMinder Administration window, select Tools, Manage Keys.

   The SiteMinder Key Management dialog box opens.
3. In the Agent Key tab, select the Use Dynamic Key radio button.

   The dialog box changes to support dynamic keys.
4. In the Dynamic Key Detail group box, select the Automatic Key Rollover radio button. A description of the current automatic rollover settings appears below the radio button.
5. Set the frequency of the automatic key rollover.
6. Click OK.

More information:

Set Rollover Frequency (see page 63)
Policy Server Management Console (see page 157)

Set Rollover Frequency

To set the automatic rollover frequency for agent keys

1. Click Set Rollover Frequency on the SiteMinder Key Management dialog box.

   The Set Frequency dialog box opens.

2. Select one of the following radio buttons:

   Rollover Once Per Week

   Indicates Agent keys rollover once per week on the day and time you select from the Day and Hour drop-down lists. A time of 0:00 means 12:00 am.

   Rollover Once Per Day

   Indicates Agent keys rollover once per day at the time you select from the Hour drop-down list.

   Rollover

   Indicates Agent keys rollover a number of times each day you select from the times per day drop-down list. The rollovers are distributed evenly throughout the day. For example, if you select 4 from the list, The Policy Server generates new keys at midnight, 6:00 AM, noon, and 6:00 PM.

   Note: You must specify all times as Greenwich Mean Time (GMT). Since Policy Servers may span many times zones, this ensures that a SiteMinder deployment rolls over keys at a specific moment in time across all Policy Servers in your enterprise.

3. Click OK.

Note: Session timeouts must be less than or equal to twice the interval between Agent key rollovers. If a session timeout is greater than twice the specified interval, users may be challenged to reauthenticate before their sessions terminate. For information about session timeouts, see the SiteMinder *Web Agent Guide* and the SiteMinder *Policy Design Guide*.

More information:

Coordinate Agent Key Management and Session Timeouts (see page 64)

Manually Rollover the Key

For added security, the SiteMinder Agent Key Management dialog box enables you to manually rollover Agent keys. You can use this feature to rollover keys at any time. You can also use this feature if you want the Policy Server to generate dynamic keys, but you do not want the keys to rollover at a fixed interval.

To manually rollover dynamic keys

1. Log into the Policy Server User Interface.
2. From the menu bar of the SiteMinder Administration window, select Tools, Manage Keys.

   The SiteMinder Key Management dialog box opens.
3. In the Agent Key tab, select the Use Dynamic Key radio button.

   The dialog box changes to support dynamic keys.
4. In the Dynamic Key Detail group box, select the Manual Key Rollover radio button.

   With Manual Key Rollover selected, when you close the SiteMinder Key Management dialog box, the Policy Server will not generate new dynamic keys and will not perform key rollover automatically.
5. To rollover dynamic keys, click Rollover Now.

   The Policy Server immediately generates new Agent keys.

   Note: There is no visible change in the dialog box. This button executes the rollover process on the Policy Server. Do not click this button multiple times unless you want to rollover keys more than once.

   Web Agents pick up the new keys the next time they poll the Policy Server, which may take up to **three minutes** due to cache synchronization. In a situation where, for security reasons, you want to use an entirely new set of keys to ensure security, you can rollover dynamic keys twice in order remove both the old key and the current key from Agents.

   Note: You can use the Rollover Now button to rollover keys between automatic rollovers if Automatic Key Rollover is selected.

More information:

Coordinate Agent Key Management and Session Timeouts (see page 64)

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

Although it is not recommended, you can change the static key used by SiteMinder Web Agents to encrypt identity information for certain SiteMinder features.

A static key may also be used to maintain a single sign-on environment in an environment that requires multiple Policy Servers and multiple master key stores.

Important! Changing the static key will cause some 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. Changing the static key is not recommended, except in extreme situations such as security breaches. Authenticated users may be forced to login again before single sign-on will function across multiple SiteMinder installations.

To change the static key

1. Log into the Policy Server User Interface.
2. From the menu bar of the SiteMinder Administration window, select Tools, Manage Keys.

   The the SiteMinder Key Management dialog box opens.
3. In the Agent Key tab, select the Use Static Key radio button.

   The SiteMinder Key Management dialog box changes to support static keys.

4. Do one of the following:
   - Generate a random key--Click the Rollover Now button in this group box to make the Policy Server generate a new random static key.
   - Specify a key--Enter a static key in this group box as follows:

     Static key--Specify a value for this field that the Policy Server uses as the static key. Use this option in situations where two key stores must use the static key to maintain a single sign-on environment.

     Confirm key--Re-enter the static key in this field then click Rollover Now.

   Depending on the option you selected, the Policy Server generates a new static key or uses the one you specified. The static key rolls over within three minutes.
5. Do one of the following:
   - To save your changes, click Apply.
   - To save your changes and return to the SiteMinder Administration window, click OK.
   - To return to the SiteMinder Administration window without saving your changes, click Cancel.

   Note: Click **Cancel** if you changed the static key, but you want to continue using dynamic Agent key rollover.

More information:

Static Keys (see page 53)
Multiple Policy Stores with Separate Key Stores (see page 59)
Coordinate Agent Key Management and Session Timeouts (see page 64)

Reset the Policy Store Encryption Key

To reset the policy store Encryption Key

1. Export your existing policy store content in clear text.
2. Run smldapsetup remove to clear the policy store content and SiteMinder schema.
3. Run "smreg -key *new_encryption_key*" to reset the Encryption Key.
4. Reboot the machine.
5. Load the Policy Server Management Console and retype the Admin password for the Directory Server.
6. Open a command prompt.
7. Run "smldapsetup ldgen -f*any_filename_to_store_new_schema* -v".
   The LDAP instance is correctly identified.

8. Run "smldapsetup ldmod -f*previous_filename* -v"
   LDAP is modified with the schema file.
9. Run "smreg -su *SiteMinder_admin_password*" to reset SiteMinder Administrator password.
10. Run "smobjimport -i*smpolicy.smdif file* -dsiteminder -wpassword -v" to import SiteMinder policy store base contents to LDAP.
11. Run "smobjimport -i*the_original_exported_policy_export_file*.smdif> -dsiteminder -wpassword -v" to restore the original content of policy store.

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

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.

More information:

Generate a Random Session Ticket Key (see page 67)
Manually Enter the Session Ticket Key (see page 68)

Generate a Random 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 enables the Policy Server to use an algorithm to create the key used for encryption and decryption.

To generate a random session ticket key

1. Log into the Policy Server User Interface.

2. From the menu bar of the SiteMinder Administration window, select Tools, Manage Keys.

   The the SiteMinder Key Management dialog box opens.

3. Select the Session Ticket Key tab to bring it to the front.
4. In the Generate a Random Session Ticket Key group box, click Rollover Now.

   The Policy Server generates a new session ticket key. This key immediately replaces the one that is used to encrypt and decrypt session tickets.

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.

To manually enter the session ticket key

1. Log into the Policy Server User Interface.
2. From the menu bar of the SiteMinder Administration window, select Tools, Manage Keys.

   The the SiteMinder Key Management dialog box opens.

3. Select the Session Ticket Key tab to bring it to the front.
4. In the Session Ticket Key field of the Specify a Session Ticket Key group box, enter the new session ticket key.
5. In the Confirm field, re-enter the key.
6. Click Rollover Now.

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

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 57)

Shared Secret for a Trusted Host

When you register a trusted host, the installation process automatically generates a shared secret for the Web Agent and stores that shared secret in the SmHost.conf file, the Host Configuration file. If you choose to enable shared secret rollover when registering a trusted host, you can rollover the shared secrets for trusted hosts. You can rollover shared secrets 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.

For information about installing Web Agents and registering trusted hosts, see the *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 only one Policy Server be enabled to generate keys. If there are multiple policy stores in an environment, but only a single shared key store, the shared secrets in the policy store are rolled over automatically *only* in the policy store for the Policy Server with key generation enabled. For the other policy stores, you can manually execute a rollover.

To manually rollover the shared secret, use the Policy Server User Interface or the C Policy Management API running on a Policy Server configured to the target policy store.

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

More information:

Management Console--Keys Tab (see page 169)
Configure Manual Shared Secret Rollover (see page 70)
Configure Periodic Shared Secret Rollover (see page 71)

Configure Manual Shared Secret Rollover

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

To configure manual shared secret rollover

1. Log into the Policy Server User Interface.
2. From the menu bar of the SiteMinder Administration window, select Tools, Manage Keys.

   The SiteMinder Key Management dialog box opens.
3. Select the Shared Secret Rollover tab.
4. Click the Rollover Now button.

   The Policy Server begins the process of rolling over shared secrets for all trusted hosts configured to allow shared secret rollover.

   Note: The rollover may take some time depending on the number of trusted hosts in your deployment.
5. Click OK.

Configure Periodic Shared Secret Rollover

The Policy Server supports periodic shared secret rollovers for trusted hosts hourly, daily, weekly, or monthly. The shortest allowable period between rollovers is one hour.

Unlike Agent key rollover, periodic shared secret rollover is associated with the age of the shared secret for each individual trusted host. The Policy Server initiates rollovers based on the age of the shared secret, 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. However, 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.

Note: In order to enable periodic shared secret rollover, the Enable Agent Key Generation check box must be selected in the Keys tab of the Policy Server Management Console.

To configure periodic shared secret rollover

1. Log into the Policy Server User Interface.
2. From the menu bar of the SiteMinder Administration window, select Tools, Manage Keys.

   The SiteMinder Key Management dialog box opens.
3. Select the Shared Secret Rollover tab.
4. In the Shared Secret Rollover tab, select the Rollover Shared Secret every radio button.
5. Enter a number in the first field to the right of the radio button and select a unit (Hours, Days, Weeks, or Months) from the drop-down list.
6. Click OK.

More information:

Configure Periodic Key Rollover (see page 62)
Management Console--Keys Tab (see page 169)

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.

More information:

Management Console--Logs Tab (see page 170)

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, even if you are logged into the system as an Administrator. For more information, see the release notes for your SiteMinder component.

2. Click the 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.

More information:

Management Console--Logs Tab (see page 170)

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.

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

Chapter 8: Configuring the Policy Server Profiler

This section contains the following topics:

Profiler Overview

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

You configure the Policy Server Profiler from the Management Console Profiler tab.

More information:

Management Console--Profiler Tab Fields and Controls (see page 172)

Configure the Policy Server Profiler

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

To configure the profiler

1. Start the Policy Server Management Console.

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

2. Click the Profiler tab.

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

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\Netegrity\SiteMinder\CurrentVersion\
LogConfig\TraceFilesToKeep
```

More information:

Management Console--Profiler Tab Fields and Controls (see page 172)

Change Profiler Settings

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

To configure profiler 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, even if you are logged into the system as an Administrator. For more information, see the release notes for your SiteMinder component.

2. Click the 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, choose 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 options for general, broad scope tracing.

   authentication_trace.template

   Provides options for tracing user authentications.

   authorization_trace.template.txt

   Provides options for tracing user authorizations.

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

5. Review/configure trace options by doing one or more of the following:

   - Select Components--Specify which components--actions executed by the Policy Server--to trace on the Components tab.
   - Select Data Fields--Specify which data fields--actual pieces of data used by the Policy Server to complete its tasks--to trace on the Data tab.
   - Add Filters--Specify data filters that will 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.

More information:

Policy Server Profiler Dialog Box (see page 175)
Policy Server Profiler--Components Tab (see page 177)
Policy Server Profiler--Data Tab (see page 177)
Policy Server Profiler Dialog--Filters Tab (see page 181)

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

To 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 9: Configuring Administrative Journal and Event Handler

This section contains the following topics:

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.

More information:

Management Console--Advanced Tab (see page 174)

Configure Advanced Settings for the Policy Server

To configure the Policy Server advanced 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, even if you are logged into the system as an Administrator. For more information, see the release notes for your SiteMinder component.

2. Click the 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.

More information:

Management Console--Advanced Tab (see page 174)

Chapter 10: Adjusting Global Settings

This section contains the following topics:

Enable User Tracking

The SiteMinder Global Settings dialog box, available from the Policy Server User Interface, lets you enable and disable user tracking. If you enable user tracking, SiteMinder Agents save Global Unique Identifiers (GUIDs) in cookies. When users access a resource in a realm with an Anonymous authentication scheme for the first time, the SiteMinder Agent creates a cookie that includes the user's GUID. Since each GUID is a unique value, a GUID in a cookie created by a SiteMinder Agent 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 Policy Server User Interface.
2. From the menu bar of the SiteMinder Administration window, select Tools, Global Settings.

   The SiteMinder Global Settings dialog box opens.
3. Select the Enable User Tracking check box.
4. Click OK.

   The SiteMinder Global Settings dialog box closes. The Policy Server enables user tracking.

More information:

SiteMinder Global Settings Dialog (see page 183)

Enable Nested Security

The SiteMinder Global Settings dialog box, available from the Policy Server User Interface, lets you enable and disable the nested security option, which provides backwards compatibility for older versions of SiteMinder. This option is enabled by default. CA strongly recommends that you do not modify this setting.

To enable nested security

1. Log into the Policy Server User Interface.
2. From the menu bar of the SiteMinder Administration window, select Tools, Global Settings.

   The SiteMinder Global Settings dialog box opens.
3. Select the Enable Nested Security check box.
4. Click OK.

   The SiteMinder Global Settings dialog box closes. The Policy Server enables nested security.

More information:

SiteMinder Global Settings Dialog (see page 183)

Enable Enhanced Active Directory Integration

Active Directory 2003 has several user and domain attributes that are specific to the Windows network operating system (NOS) and are not required by the LDAP standard:

- 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, you should enable the Enhanced Active Directory Integration global setting from the SiteMinder Global Settings dialog box available from the Policy Server User Interface. This option improves the integration between the Policy Server's user management feature and Password Services with Active Directory. This enhancement synchronizes Active Directory user attributes with SiteMinder mapped user attributes. For more information about this feature, see the *Policy Design Guide*.

Note: The feature is not supported with ADAM.

To enable enhanced Active Directory integration

1. Log into the Policy Server User Interface.
2. From the Policy Server User Interface menu bar, select Tools, Global Settings.

   The SiteMinder Global Settings dialog box opens.
3. Select the Enhance Active Directory Integration check box. By default, this enhancement 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 OK.

   The SiteMinder Global Settings dialog box closes. The Policy Server enables enhanced Active Directory integration.
5. Open the Active Directory user directory object in the User Directory dialog box for editing.
6. In the Root field for the SiteMinder user directory object, enter the default Windows domain's DN as the user directory root. For example:

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

   Note: AD-specific features may not work in the Root field is set to another value.
7. Click Apply.

More information:

SiteMinder Global Settings Dialog (see page 183)

Chapter 11: Cache Management

This section contains the following topics:

Cache Management Overview

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.

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.

SiteMinder also maintains an *Agent Cache* on each a 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.

Configure Caches

The Cache Management dialog is where you manage various Policy Server caches.

The following cache management options are available:

All Caches Group Box

Flush All

Flushes all Policy Server and associated agent caches: user sessions, resource information, and user directory caches, including certificate CRLs. This process takes up to twice the time specified by the Policy Server poll interval while the Policy Server synchronizes caches.

Note: Flushing all caches may adversely affect access times for protected resources, since all requests immediately following the cache flush must retrieve information from user directories and the policy store. However, this action may be necessary if critical user privileges and policy changes must go into effect immediately

User Session Caches Group Box

All

If selected, all user sessions are removed from the user cache when you click the Flush button.

Specific User DN

If selected, the DN specified using the associated Directory and DN controls will be removed from the user cache when you click Flush.

Directory

Specifies the user directory that contains the DN you want to flush from the user cache.

DN

Specifies the distinguished name you want to flush from the user cache. If you select this option, you must specify a user's DN, not a group's DN. If you do not know the DN, click Lookup to search for the DN. For information about searching for a DN, see the *Policy Server Configuration Guide.*

Flush

Clicking this button does one of the following:

- If you selected All, flushes all users
- If you selected Specific User DN, flushes a specific DN 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.

Resource Caches Group Box

Flush

Flushes all resource caches and forces Web Agents to authorize requests against the Policy Server. This process takes up to twice the time specified by your Policy Server poll interval while the Policy Server synchronizes caches.

Cache Updates

Enable/Disable

Toggles between enabling or disabling cache flushing.

More information:

Management Console--Settings Tab Fields and Controls (see page 160)

Flush Caches

SiteMinder automatically flushes appropriate cache entries when you change SiteMinder objects. The cache settings also specify a regular interval for applying administrative changes. However, if you are making sensitive changes (for example, changing the access rights to highly critical information), you can flush SiteMinder caches manually, so that unauthorized users are not able to access protected resources based on information stored in the caches.

Cache Management features, which are accessible from the SiteMinder Cache Management dialog box, let you force an update of SiteMinder data by manually flushing:

All Caches Group Box

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

User Session Caches Group Box

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

Resource Caches Group Box

Enables you to flush cached information about resources.

Cache Updates Group Box

You can view the cache status:

Cache update is disabled.

Specifies that cache flushing is disabled.

Cache update is enabled.

Specifies that cache flushing is enabled.

You can modify the cache status:

Disable/Enable

Switches the cache status from enabled to disabled or disabled to enabled.

Flush All Caches

The SiteMinder Cache Management dialog box provides a method for administrators to flush the contents of all caches. Flushing all caches may 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 may be necessary if critical user privileges and policy changes must go into effect immediately.

Note: This menu selection is 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. If the menu selection is not available, the administrator account you used to log in does not have enough privileges to access the dialog box. For information about administrative privileges, see the *Policy Design Guide* guide.

If your configuration contains two policy servers pointing to one policy store, you can ensure that the primary (object cache) is included in the Flush All command. This causes both the primary and secondary caches to be rebuilt from the policy store. To enable this functionality, you must add the following entry to the registry:

Registry Name - FlushObjCache
Type - DWORD
Value - 0 (default)
Location -
HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\ObjectStore

To flush all caches

1. Log into the Policy Server User Interface.
2. From the menu bar of the SiteMinder Administration window, select Tools, Manage Cache.

   The the SiteMinder Cache Management dialog box opens.

3. In the All Caches group box, click Flush All.

   Note: The Flush All button in the All Caches group box 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 will take up to twice the time specified by your policy server poll interval while the Policy Server synchronizes caches.

4. Click OK.

   The the SiteMinder Cache Management dialog box closes.

Flush User Session Caches

When a user successfully authenticates, the Policy Server begins a session for the authenticated user. During the user's session, the Web Agent stores authorization information in the user cache. However, if you change user access rights, it may be necessary to force the Policy Server to flush user session information from the Web Agent's cache. You can do this from the SiteMinder Cache Management dialog box.

To flush user sessions

1. Log into the Policy Server User Interface.
2. From the menu bar of the SiteMinder Administration window, select Tools, Manage Cache.

   The SiteMinder Cache Management dialog box opens.

3. In the User Session Caches group box, select one of the following radio buttons:

   All

   Indicates that all user sessions should be removed from the user cache on a flush command. If you select this radio button, skip ahead to Step 6.

   Specific User DN

   Indicates that the flush command removes a specific DN from the user cache. If you select this radio button, also complete Steps 4 and 5.

4. (If you selected Specific User DN) From the Directory drop-down list, select the user directory that contains the DN you want to flush from the user cache.

5. (If you selected Specific User DN) In the DN field, enter the distinguished name you want to flush from the user cache. If you select this option, you must specify a user's DN, not a group's DN.

   If you do not know the DN, click Lookup and search for the DN. For information about searching for a DN, see the SiteMinder *Policy Design Guide*.

   Note: The option to flush user caches is only enabled for administrators that have the Manage Users privilege. For information about administrative privileges, see the SiteMinder *Policy Design Guide*.

6. In the User Session Caches group box, click Flush.

   Depending on the radio button you selected, SiteMinder flushes all users or a specific DN from the user cache. This process will take up to twice the time specified by your policy server poll interval while the Policy Server synchronizes caches.

7. Click OK.

   The SiteMinder Cache Management dialog box closes.

Flush Resource Caches

SiteMinder Agents cache information about specific resources accessed by users in a resource cache. This 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. To flush the resource cache for a specific realm, see the SiteMinder *Policy Design Guide*. To flush the resource cache of all resources, you should perform the procedure described below.

To flush resource caches

1. Log into the Policy Server User Interface.
2. From the menu bar of the SiteMinder Administration window, select Tools, Manage Cache.

   The SiteMinder Cache Management dialog box opens.

3. In the Resource Caches group box, click Flush.

   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. For information about administrative privileges, see the SiteMinder *Policy Design Guide*.

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 information about flushing cached information for a specific resource, see the SiteMinder *Policy Design Guide.*

4. Click OK.

Manage Cache Status

You can view the refresh status of Policy Server caches and disable or enable cache flushing through the Policy Server User Interface or through three smpolicysrv command-line options. By using these options to suspend and resume cache flushing, you can resolve policy evaluation issues. These commands are issued by the central administration Policy Server to all secondary Policy Servers.

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

To manage cache status through the Policy Server User Interface

1. Log in to the Policy Server User Interface.
2. From the menu bar of the SiteMinder Administration window, select Tools, Manage Cache.

   The SiteMinder Cache Management dialog opens.
3. View the cache status in the Cache Updates group box:

   Disabled: Cache flushing is disabled.

   Enabled: Cache flushing is enabled.
4. (Optional) Click the Enable/Disable button and OK to modify the cache status.

To manage cache status through the Command Line Interface

1. Open a command prompt.

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

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.

Flush the Requests Queue on the Policy Server

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

Flush the Policy Store Cache

Flushing the policy store caches flushes all of the current entries and reloads the cache with all of entries in the policy store. During the flush, the policy store cache is taken offline. The Policy Server either pauses or uses the policy store directly to make policy decisions

To flush the policy store cache

1. Open the registry editor.
2. Navigate to \\HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Object Store.
3. Create the FlushObjCache registry key with the following values:

   Type: DWORD

   Value: 1or 0

   1

   Enables the key. When enabled, you can use the Flush All button on the Cache Management dialog to flush all Policy Server and associated SiteMinder Agent caches, including the policy store cache.

   0

   Disables the key. When disabled, you can use the Flush All button on the Cache Management dialog to flush all Policy Server and associated SiteMinder Agent caches, excluding the policy store cache.

   Note: If a value does not exist, the key is disabled.
4. Use the Cache Management dialog in the Policy Server User Interface to flush all caches.

More Information:

Flush All Caches (see page 90)

Chapter 12: 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.

In order 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 SiteMinder *Policy Design Guide*.

Flush the Session Cache

You can flush the session cache manually using the Cache Management option from the Tools menu of the Policy Server User Interface. You can choose to flush all the entries in the user session cache or clear a specific DN.

Flushing the user session cache alone does not terminate a session or disable a user. It clears out all the user authorization and response information.

More information:

Flush User Session Caches (see page 91)

Manage User Accounts

You manage user accounts using the Policy Server User Interface.

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, thereby ending the session.

To enable or disable a user account

1. Log into the Policy Server User Interface.
2. From the menu bar of the SiteMinder Administration window, select Tools, Manage Users.

   The SiteMinder User Management dialog box opens.
3. From the Directory drop-down list, select the user directory connection for the directory that contains the user you want to disable.
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 and execute a search for the user you want to enable or disable.

   The Policy Server displays search results in the User Management dialog box.
6. Select a user from the list of results.

   The Current Settings group box contains a button. This button is labeled Enable for a disabled user, or Disable for an enabled user.

   Note: You must select a single user from the list of search results.
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 User Management dialog box enables you to force password changes for users, or change user passwords to new values.

If you are using the Password Must Change feature of SiteMinder's Registration Services, you can force password changes from the User Management dialog box. However, a Password Policy must be defined. For information about password policies, see the SiteMinder *Policy Design Guide*.

Note: 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. For information on password policies, see the SiteMinder *Policy Design Guide*.

To manage user passwords

1. Log into the Policy Server User Interface.
2. From the menu bar of the SiteMinder Administration window, select Tools, Manage Users.
3. The SiteMinder User Management dialog box opens.
4. From the Directory drop-down list, select the user directory connection for the directory that contains the user for whom you want to manage passwords.
5. 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.

   Note: For information about user directory searches, see the SiteMinder *Policy Design Guide.*

   Enter search criteria and execute a search for the user for whom you want to manage passwords.

   The User Management dialog box displays the users that match your search criteria.
6. Select a user from the list of results.

   Note: You must select a single user from the list of search results.
7. To force the selected user to change passwords on their next login, in the Password group box select the User must change password at next login check box.
8. To change a user's password to a new value, in the Password group box select the Change password to check box and enter the new password in the field. Re-enter the password in the Confirm Password field.

   Note: The password that you specify is not constrained by any password policy but it is recorded in the user's password history.

9. Click Set.

   Your changes are saved.

10. Click OK.

    Note: 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. For more information, see the SiteMinder *Policy Design Guide*.

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.

Note: Session tracking is unrelated to the Enable User Tracking option in the Policy Server User Interface.

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 *SiteMinder Web Agent Guide*.

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 Policy Server User Interface.

Note: Web Agents automatically log user names and access information in native Web Server log files when users access resources.

More information:

Reporting Overview (see page 143)

Chapter 13: Clustering Policy Servers

This section contains the following topics:

Clustered Policy Servers

Load balancing and failover in a SiteMinder deployment provide a high level of system availability and improve response time by distributing requests from 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.

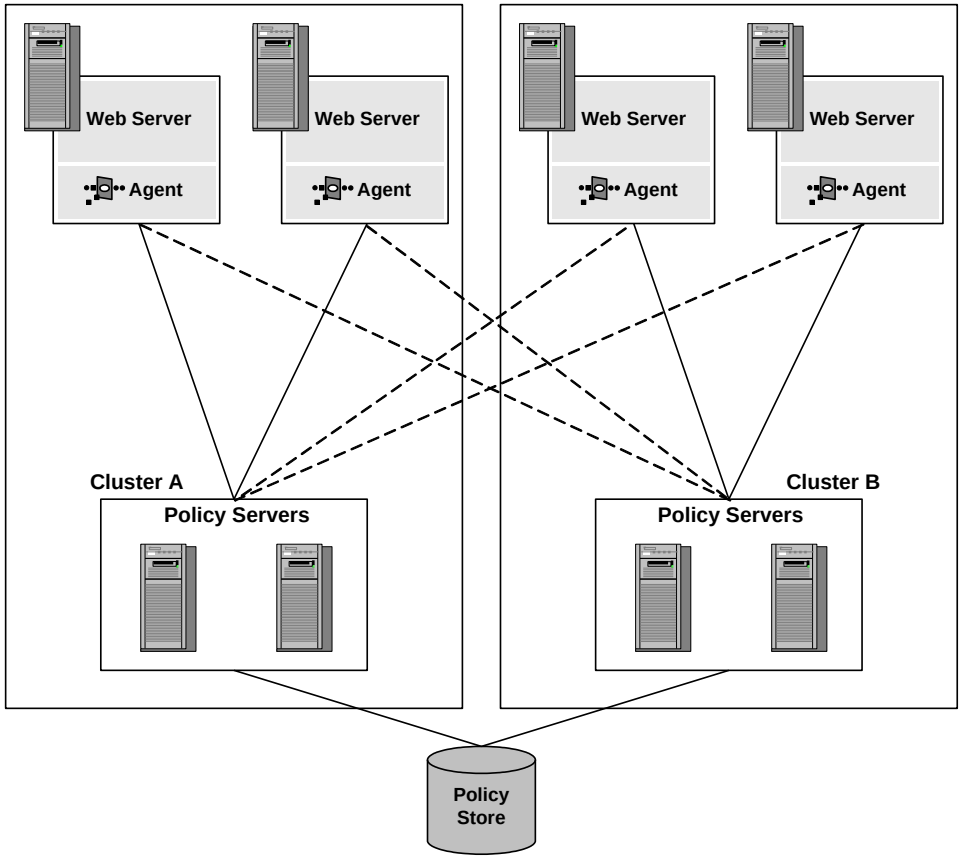
Another problem with efficiency can occur when data centers are located in different geographical regions. Sending requests to servers outside a certain locale can lead to the increased network communication overhead, and in some cases to the network congestion.

To address these issues and to improve system availability and response time, you can define a cluster of Policy Servers and associated Web 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.

The following figure illustrates a simple 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 103)
Clustered Environment Monitoring (see page 103)

Failover Thresholds

In any clustered 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.

Clustered Environment Monitoring

In a non-clustered 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 107)

Hardware Load Balancing Considerations

If you are deploying a hardware load balancer between the 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 (KB ID 21135) on the Support site.

More information:

Contact CA Technologies (see page iii)

Configure Clusters

Policy Server clusters are defined as part of a Host Configuration Object. When a SiteMinder Web Agent initializes, the settings from the Host Configuration Object are used to setup communication with Policy Servers.

Note: For information about Host Configuration Objects, see the *Web Agent Guide* and the *Policy Design* guide.

To configure a cluster as part of a host configuration object

1. Open the Policy Server User Interface.
2. In the System tab of the SiteMinder Administration window, select Host Conf Objects.
3. In the List pane, select the host configuration object to which you want to add cluster configuration information.

   Once you configure a cluster for a host configuration object, any Agent that uses the object to establish its Policy Server connections will use the specified cluster configuration.

4. From the Edit menu, select Properties of Configuration Object.

   The Host Configuration Object Properties dialog box opens.

5. Select the Clusters tab.

6. In the Clusters tab, click the Add button.

   The Cluster Setup dialog box opens.

7. In the Add Server group box, do one of the following:

   - Select the IP Address radio button and enter the IP address of a Policy Server in the cluster in the provided fields.

     Note: If you do not know the IP address of the Policy Server, but you know the host name, click the DNS Lookup button to search for the IP address of the Policy Server.

   - Select the Domain Name radio button and enter the domain name of the system where the Policy Server is installed. For example, server.company.com.

8. In the Server Port field, enter the port for Policy Server processing.

9. Click the Add to Cluster button.

   The Policy Server appears in the list of servers in the Current Setup group box.

10. Repeat steps 7 through 9 for any other Policy Servers you want to add to the cluster.

11. When you finish adding Policy Servers to the cluster, click the OK button to save your changes and return to the Host Configuration Object Properties dialog box.

12. In the Failover Threshold Percent field, enter a percentage of Policy Servers that must be active and click Apply.

    If the percentage of active servers falls below the percentage you specify, the cluster fails over to the next available cluster in the list of clusters.

    The Policy Server User interface automatically calculates the Failover Threshold values displayed in the column to the right of the lists of servers in each cluster. The number that appears in the Failover Threshold column is the minimum number of servers in the cluster that must be available. If the number of available servers falls below the specified number, failover occurs.

    When you set the Failover Threshold Percentage, it applies to all clusters that use the Host Configuration Object.

13. Click on the General tab.

14. Note the Policy Server parameter in the Parameter Name column.

    The value of the Policy Server parameter is overridden by the contents of the Clusters tab. This parameter should be commented for clarity (proceeded by a # symbol), since its value does not apply as long as Policy Servers are specified in the Clusters tab.

    Note: In order for the value of the Policy Server parameter in the General tab to apply, no Policy Servers should be specified in the Clusters tab. If clusters are configured and you decide to remove the clusters in favor of a simple failover configuration using the Policy Server parameter in the General tab, be sure to delete all Policy Server information in the Clusters tab.

15. Click OK to save your changes and close the Host Configuration Object dialog box.

More information:

Clustered Policy Servers (see page 101)

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.

To configure a Policy Server as a centralized monitor

1. Start the Policy Server Management Console.

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

2. 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:

Configuring Port Numbers (see page 120)

Point Clustered Policy Servers to the Centralized Monitor

To point Policy Servers to a centralized monitor

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, even if you are logged into the system as an Administrator. For more information, see the release notes for your 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.

More information:

Clustered Policy Servers (see page 101)
Management Console--Status Tab Fields and Controls (see page 159)

Chapter 14: Monitoring the Health of Your SiteMinder Environment

This section contains the following topics:

OneView Monitor Overview

The SiteMinder OneView Monitor identifies performance bottlenecks and provides information about resource usage in a SiteMinder deployment. It also displays alerts when certain events, such as component failure, occur. It does this by collecting operational data from the following SiteMinder components:

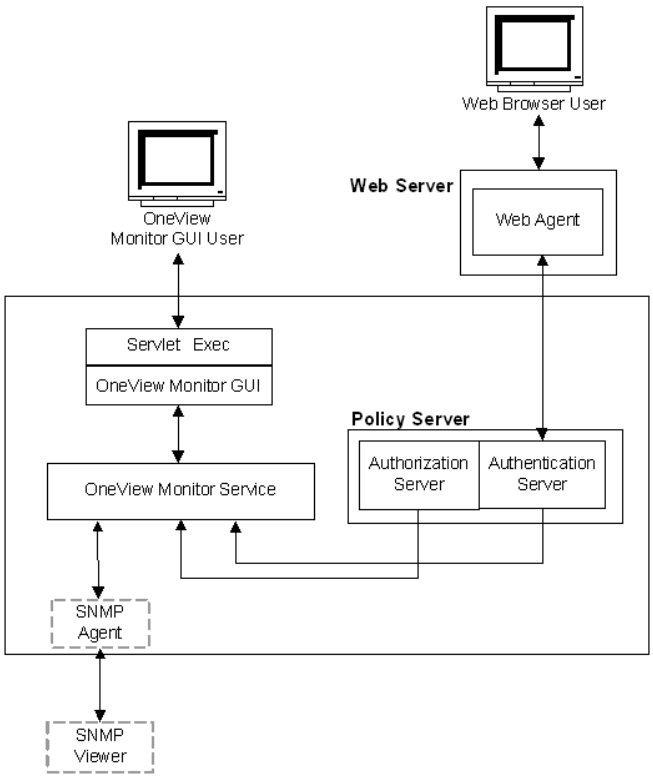
- Policy Server
- SiteMinder Web Agent

As these components are added to a 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 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:

Setting The Data Refresh Rate and Heartbeat (see page 120)
SNMP Monitoring (see page 127)
Management Console--Settings Tab Fields and Controls (see page 160)

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 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 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 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 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.

More information:

Setting The Data Refresh Rate and Heartbeat (see page 120)
Cache Management Overview (see page 87)
SNMP Monitoring (see page 127)

Configure the OneView Monitor

Configuring the OneView Monitor includes:

- Setting the data refresh rate and heartbeat
- Configuring port numbers

Setting The 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 22)
Start and Stop Policy Server Processes on UNIX Systems (see page 22)

Configuring 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 22)
Start and Stop Policy Server Processes on UNIX Systems (see page 22)
Configure a Policy Server as a Centralized Monitor for a Cluster (see page 106)

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://<*yourserver.yourcompany.org:port*>/siteminderdmonitor

where <*yourserver.yourcompany.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*.

More information:

Policy Server Management Console (see page 157)

Protect The OneView Viewer

To protect the OneView viewer, create a SiteMinder policy that protects the resources in siteminderdmonitor.

View Monitored Components

OneView Monitor provides four 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 122)
- Configuring alerts (see page 123)
- Displaying tables (see page 123)
- Sorting tables (see page 124)
- Configuring data updates (see page 124)
- Saving settings (see page 124)
- Changing the default display (see page 125)
- Loading settings (see page 125)

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 124)

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.

   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.

   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.

   SiteMinder displays a dialog box where you can select settings to load.
2. Select a setting from the list box.
3. Click OK.

Chapter 15: Monitoring SiteMinder Using SNMP

This section contains the following topics:

SNMP Monitoring

The SiteMinder SNMP module enables many operational aspects of the 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 SiteMinder Agents.
- SNMP Manager is typically a Network Management System (NMS) application such as HP OpenView.

The SiteMinder SNMP module provides SNMP request handling and configurable event trapping for the SiteMinder environment. It does this by collecting operational data from the 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 SiteMinder 5.x-based Agent applications.

SiteMinder SNMP Module Contents

The SiteMinder SNMP module consists of:

- SiteMinder SNMP MIB is the database of SiteMinder objects that can be monitored by an SNMP-compliant network management system.
- A SiteMinder SNMP Subagent responds to SNMP requests (GET and GETNEXT only) passed to it from an SNMP master agent.
- 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:

SiteMinder MIB (see page 130)
Configure the SiteMinder Event Manager (see page 138)
Start and Stop SiteMinder SNMP Support (see page 140)

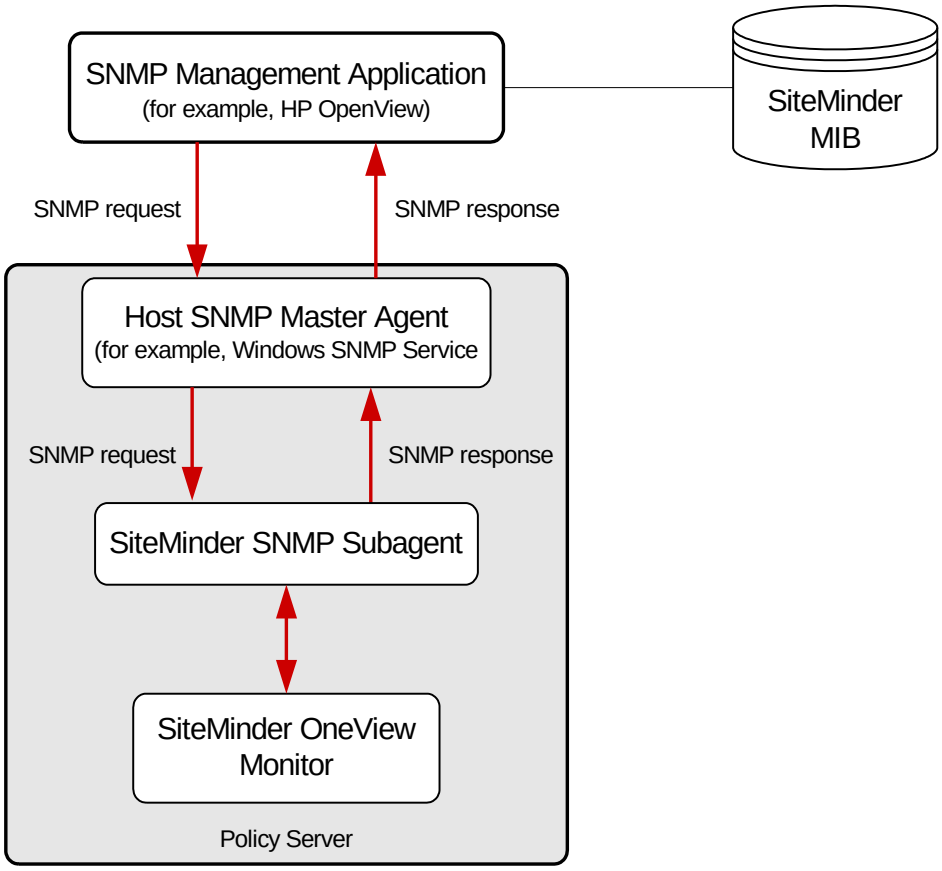
Dependencies

The SiteMinder SNMP Module has the following dependencies:

- **SiteMinder OneView Monitor**—The 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 SiteMinder SNMP Module.
- **SNMP Master Agent**—The 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 SiteMinder SNMP Module is also installed and enabled.

SNMP Component Architecture and Dataflow

The following figure illustrates SNMP module dataflow:



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 SiteMinder SNMP Subagent retrieves the requested information from OneView Monitor.
4. The 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.

SiteMinder MIB

The SiteMinder MIB provides a SNMPv2-compliant data representation of all monitored components in the SiteMinder environment.

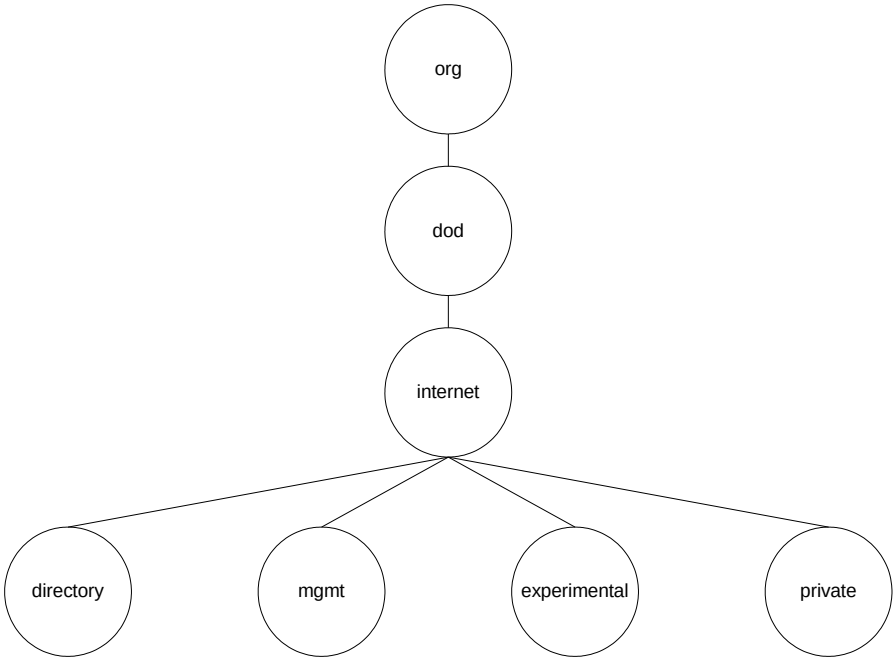
The SiteMinder MIB is supplied in an ASCII text file:

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 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.

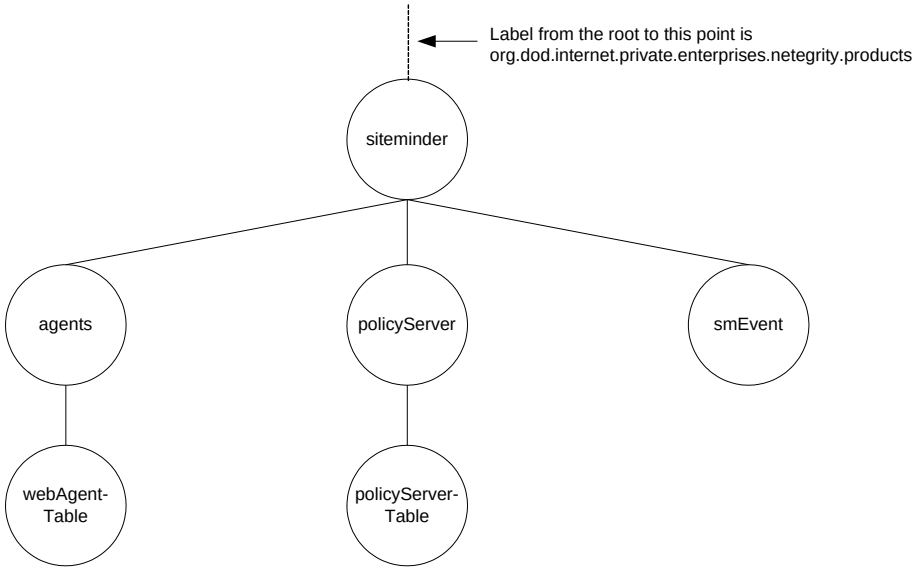


MIB branches, MIBs, and managed objects within MIBs are all identified by short text strings. Complete MIB hierarchies can be expressed notationally by concatenating branch and object identifiers, separating each entry with a period. For example, the private sub-branch of the internet entry shown above can be expressed as *iso.org.dod.internet.private.*

SiteMinder MIB Hierarchy

The 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 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 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 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 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 *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 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 SiteMinder MIB, under iso.org…siteminder.smEvents, for system events that can be mapped to SNMP traps using the 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 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).

You configure the 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 SiteMinder SNMP support when you installed the Policy Server, the SiteMinder SNMP Agent service should start automatically whenever the Policy Server initializes.

This section describes how to manually start and stop the SiteMinder SNMP subagent on Windows and UNIX Policy Servers.

Start and Stop the Windows Netegrity SNMP Agent Service

To start the 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 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 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 SiteMinder provides to help you isolate the point of failure if you have trouble establishing a management connection to, or receiving SNMP traps from 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 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.

   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 16: SiteMinder Reports

This section contains the following topics:

Reporting Overview

The Policy Server installation includes sample reports files that allow you to configure Crystal Reports for Web-based reporting of all user activity involving protected resources, and administrative activity involving the policy store. After setting up Crystal Reports to read reporting data from the Policy Server's logging database, you can run and view sample reports for all activities within every policy domain.

For more information on setting up the Policy Server and Crystal Reports to access and view reports, see the *Policy Server Installation Guide*.

Before You Begin

Verify that the following requirements are met:

- You have Crystal Reports 9.0 Developer and Crystal Reports 9.0 Application Server installed, as you will need this software to modify and run the SiteMinder reports.
- For Crystal Reports, apply the Crystal Enterprise 9 Database and Export Drivers Monthly Hot Fix (MHF) update, CE90DBEXWIN_EN.ZIP.

Report Types

There are four categories of sample reports:

- Activity Reports—Cover all activities. Reports can be organized by user, agent, or resource.
- Intrusion Reports—Cover all failed user authentication and authorization attempts. Reports can be organized by user, or agent.

- Administrative Reports—Cover all administrative activities. Reports can be organized by administrator, or object. Administrative activities are defined as any change to the SiteMinder Policy database.
- Time Series Reports—Cover successful and failed authentications and authorizations. The data is displayed graphically in a bar chart by day or by hour.

The sample report information is based on SiteMinder's audit logs. The type of events that are included in the audit logs (and the reports) is specified in the Auditing tab of the Policy Server Management Console.

Note: All times listed in SiteMinder reports are in Greenwich Mean Time (GMT).

More information:

Policy Server Management Console (see page 157)

How to View Sample Reports Using Crystal Reports

Viewing sample sample reports requires you to:

1. Set sample report files
2. Run the Web-based reports

You can view the following report types:

- Activity
- Intrusion
- Administrative
- Time series

Set Sample Reports Files

To run Web-based reports, the Crystal Reports Application Server must be configured to locate the sample SiteMinder reports files.

To configure the Crystal Reports Application Server

1. Go to Start, Programs, Crystal Enterprise 9, Tools, RAS Configuration Manager.
2. Under Report Directory, browse to the location where the SiteMinder sample reports files are installed.
3. Click OK.
4. Stop and restart the Crystal Reports Application Server using the Windows Services dialog.

Run Web-based Reports

The Crystal Reports Application Server allows you to view the sample SiteMinder reports in a Web browser.

To run a Web-based reports

1. Go to Start, Programs, Crystal Enterprise 9, Report Application Server Launch Pad.
2. Click Launch ePortfolio Lite, which brings up a Web page that displays icons for all of the sample SiteMinder reports files in *<siteminder_installation>*\reports.
3. Select the Activity, Intrusion, Administrative, or Time Series reports that you want to run.
4. In the Crystal Reports Viewer page, enter the appropriate parameters you want and then click OK to run the report.

   Note: Oracle supports dates in the mm/dd/yyyy format SQL database supports dd/mm/yyyy.
5. Enter the user name and password of the user who administers the Policy Server's logging database and click OK.

   Crystal Reports displays the sample report in the Web-based format.

Note: For more information on running reports, see the Crystal Reports documentation.

More information:

Activity Reports (see page 145)
Intrusion Reports (see page 149)
Administrative Reports (see page 152)
Time Series Reports (see page 154)

Activity Reports

Activity reports allow you to view data at different levels of granularity. These reports begin with an initial page that summarizes the data in the report. Clicking on an item in the initial page, such as a date, user, or Agent, enables you to view more detailed information. For example, if you click on a date in the Activity Report, you will see that day's events by hour. Clicking on an hour reveals details about that hour's events.

Note: The drill-down feature, which enables you to view different levels of report details is not available on Unix-based browsers. To use this feature, view reports using a Windows-based browser.

There are four types of sample Activity Reports:

- All Activity—Covers all user activity by date and time. This report contains information about the transactions and failures that occurred during the period of time covered by the report. You can select a date or time in the report to view more details.
- Activity by User—Covers all user activity by user. This report contains information about users and their sessions, including the number of transactions and failures that occurred during the period of time covered by the report. You can select a user to view more details about that user's activities.
- Activity by Agent—Covers all user activity by agent. This report lists active Agents and provides information, such as the number of transactions and failures, that occurred on each Agent during the period of time covered by the report. You can click on an Agent name to view more details about that Agent's activity.
- Activity by Resource—Covers all user activity by resource. This report contains information about the resources that were accessed during the period of time covered by the report, including host names, the number of resources accessed, the number of transactions, and the number of failed access attempts. You can select a host name to view more details.

In each of these sample reports, denials and failures are indicated by an exclamation (**!**) mark, and red text.

Note: The browser interface that displays sample report results only supports 255 characters per line. If you view a report that includes resources with long resource filters that would extend a line of report data beyond 255 characters, Crystal Reports truncates the beginning of the resource and indicates that the line has been truncated.

View an Activity Report

The following sample Activity Report reflects all activity event notifications that occurred in a specific date range.

Activity Report

1,554 Transaction(s); 280 Failure(s)
From: 5/1/2003 12:00:00AM GMT
Through: 9/1/2003 12:00:00AM GMT

Username: *
Domain: *
Agent: *

Double-click on a date below to display detailed information.

Date	# of Transactions	# of Failures
7/22/2003	12	6
7/23/2003	25	5
7/24/2003	233	92
8/18/2003	2	0
8/19/2003	1,280	177
8/20/2003	2	0

The report heading lists the dates covered in the report, and summarizes the transactions and failures that occurred during the specified dates. The report also lists the transactions and failures by date.

You can double-click a date in the main screen to view the events that occurred each hour.

Activity Report

1,554 Transaction(s); 280 Failure(s)
From: 5/1/2003 12:00:00AM GMT
Through: 9/1/2003 12:00:00AM GMT

Username: *
Domain: *
Agent: *

Double-click on a date below to display detailed information.

Date	# of Transactions	# of Failures
7/22/2003	12	6
7/23/2003	25	5
7/24/2003	233	92
8/18/2003	2	0
8/19/2003	1,280	177
8/20/2003	2	0

You can double-click an hour to view event details:

Time	User	Agent	Category	Description
7:42:55PM	siteminder	<blank agent name>	Administration	logged out
7:43:56PM	siteminder from 192.168.6.210	<blank agent name>	Administration	logged in
7:47:46PM	siteminder	<blank agent name>	Administration	logged out

Event details contain the following information:

Time

Lists the times when events occurred from the oldest time to the most recent time.

User

Contains the user name associated with the event. In this sample report, the user is *SiteMinder*.

Agent

Lists the names of the Agents where the activity occurred. Notice that the Agent column under the *SiteMinder* user contains the entry <blank agent name>. This is because the activity occurred on a Policy Server, not an Agent.

Category

Describes the type of activity that was logged. For the *SiteMinder* user, all activity was concerned with *Administration* actions.

Description

Describes the actual activity that occurred during the time noted in the Activity Report.

When any category of event is logged as a rejection or failure, the color of the text on the computer screen is red.

Intrusion Reports

Intrusion reports have a drill-down feature that allows you to view data at different levels of granularity. These reports begin with an initial page that summarizes the data in the report. Clicking on an item in the initial page, such as a date, user, or Agent, enables you to view more detailed information. For example, if you click on a date, you will see that day's events by hour. Clicking on an hour reveals details about that hour's events.

Note: The drill-down feature is not available on Unix-based browsers. To use this feature, view reports using a Windows-based browser.

There are three types of sample Intrusion *Reports*:

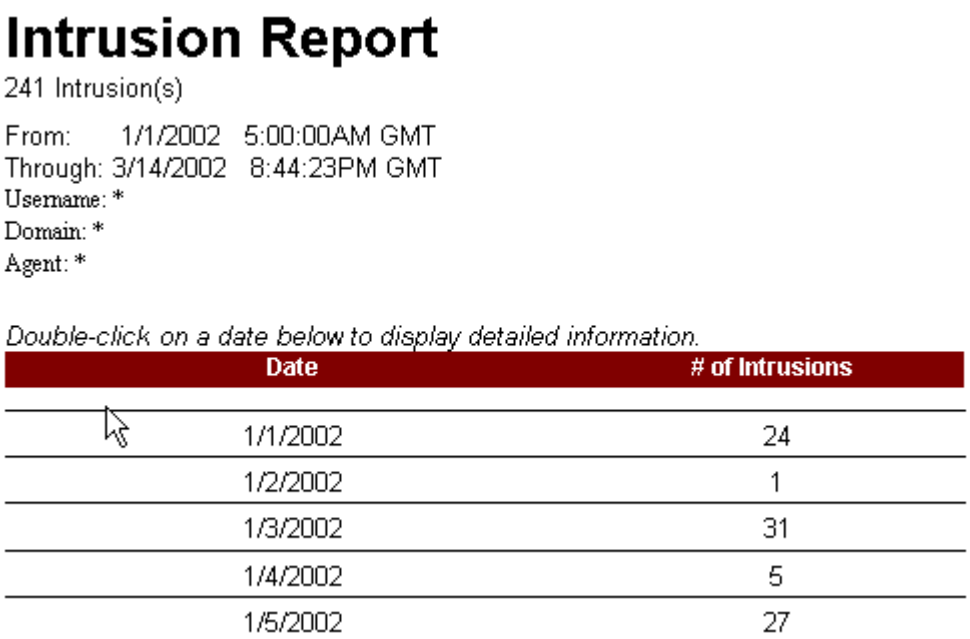
- All Failed Authentication and Authorization Attempts—Covers all failed user authentication, authorization, and administration attempts by date and time. You can select a date in the initial screen to view more information about intrusions that occurred that day.
- Failed Authentication and Authorization Attempts by User—Covers all failed user authentication and authorization attempts by user. Initially, this report lists users who unsuccessfully attempted to access a resource, and the number of failed attempts. You can click on a user to view more details about the attempts.
- Failed Authentication and Authorization Attempts by Agent—Covers all failed user authentication and authorization attempts by Agent. Initially, this report lists the Agent and the number of failed attempts. You can click on an Agent to view more details about the attempts.

In Intrusion reports, denials and failures are indicated in red text.

View an Intrusion Report

One example of an Intrusion Report is the all-inclusive Intrusion Report.

The report heading summarizes the number of intrusions that occurred during the period of time covered by the report.



Intrusion Report

241 Intrusion(s)

From: 1/1/2002 5:00:00AM GMT
Through: 3/14/2002 8:44:23PM GMT
Username: *
Domain: *
Agent: *

Double-click on a date below to display detailed information.

Date	# of Intrusions
1/1/2002	24
1/2/2002	1
1/3/2002	31
1/4/2002	5
1/5/2002	27

You can double-click a date to view intrusion information by hour:

Double-click on an hour below to display detailed information.

Hour	# of Intrusions
6:00:00AM	1
7:00:00AM	3
9:00:00AM	1
10:00:00AM	3
12:00:00PM	1
1:00:00PM	3
3:00:00PM	1
4:00:00PM	3
6:00:00PM	1

Double-click a time to view intrusion details:

All times listed in the table are Greenwich Mean Time

Time	Agent	User	Category	Description
5:03:51AM	MyAgent	SomeUser from 10.100.100.123	Authentication	rejected in realm 'TestRealm'
5:03:52AM	MyAgent	SomeUser from 10.100.100.123	Authentication	attempted in realm 'TestRealm'
5:03:58AM	MyAgent	AZUser from 10.100.100.123	Authorization	rejected for resource 'https://AZ/superpower.html'

Intrusion details include the following information:

Time

Lists the time of each intrusion, from the oldest time to the most recent time.

Agent

Lists the name of the Agent on which the intrusion occurred. When an activity is of an *administration*, not *authentication* or *authorization* category, and occurs on a Policy Server, not an Agent, the Agent field contains the entry <blank agent name>.

User

Lists the user name associated with the logged activity.

Category

Describes the type of activity that was logged.

Description

Describes the actual activity that occurred during the time noted in the Report.

When any category of event is logged as a rejection or failure, the color of the text on the computer screen is red. The exclamation (**!**) point is not used in any of the *Intrusion Reports*.

Administrative Reports

There are three types of sample Administrative Reports:

- All Administrative Activity—Covers all administrative activity by date. The columns of information include Time, Administrator, and a brief description of the activity.
- Activity by Administrator—Covers all administrative activity by administrator. The columns of information include Time, and a brief description of the activity.
- Activity by Object—Covers all administrative activity by object (Administrator, Agent, Policy, etc.). The columns of information include Time, Administrator, and a brief description of the activity.

In Administrative reports, denials and failures are indicated in red text.

View an Administrative Report

An example of an *Administrative Activity Report* is a recording of all SiteMinder administrative activity event notifications.

Administrative Activity Report

4,961 Transaction(s); 34 Failure(s)

From: 1/1/2002 5:00:00AM GMT
Through: 3/14/2002 8:44:23PM GMT

"!" indicates denial or failure

Date: Tuesday, January 01, 2002

740 Transaction(s); 6 Failure(s)

Time	Administrator		Description
5:58:00AM	SiteMinder		logged out
5:58:00AM	SiteMinder		failed login attempts countfor '' '
6:58:00AM	SiteMinder	!	login rejected
6:58:00AM	SiteMinder		failed login attempts countfor '' '
7:58:00AM	SiteMinder		flushed all
7:59:00AM	SiteMinder		flushed user '' from 'TestPolicy'
8:00:00AM	SiteMinder		flushed users
8:01:00AM	SiteMinder		flushed realms
8:02:00AM	SiteMinder		changed dynamic keys
8:03:00AM	SiteMinder		changed persistent key
8:04:00AM	SiteMinder		changed user state

The number of transactions and failures, and the dates covered in the report appear under the title of the *Administrative Activity Report*. Since this type of report contains all logged administrative events, the categories are:

Time

The exact time during which the administrative activity occurred.

Administrator

The SiteMinder Account Username is listed.

Description

The type of activity that occurred, whether it was a login, policy alteration, or other administrative activity.

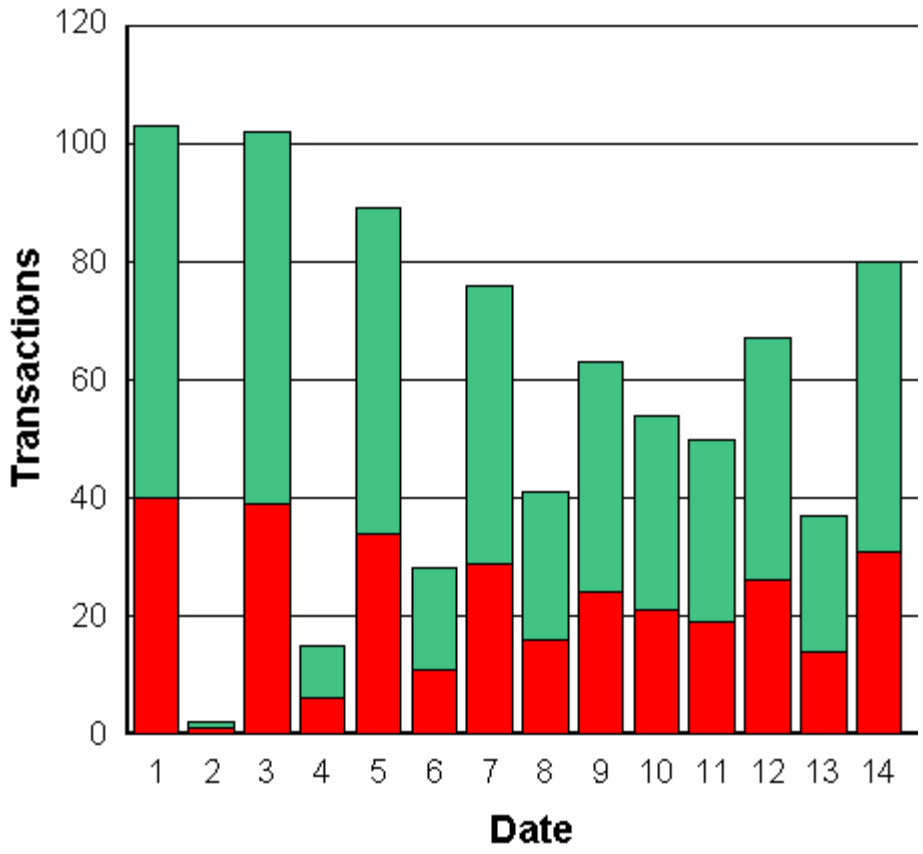
Time Series Reports

You can view two types of sample Time Series Reports:

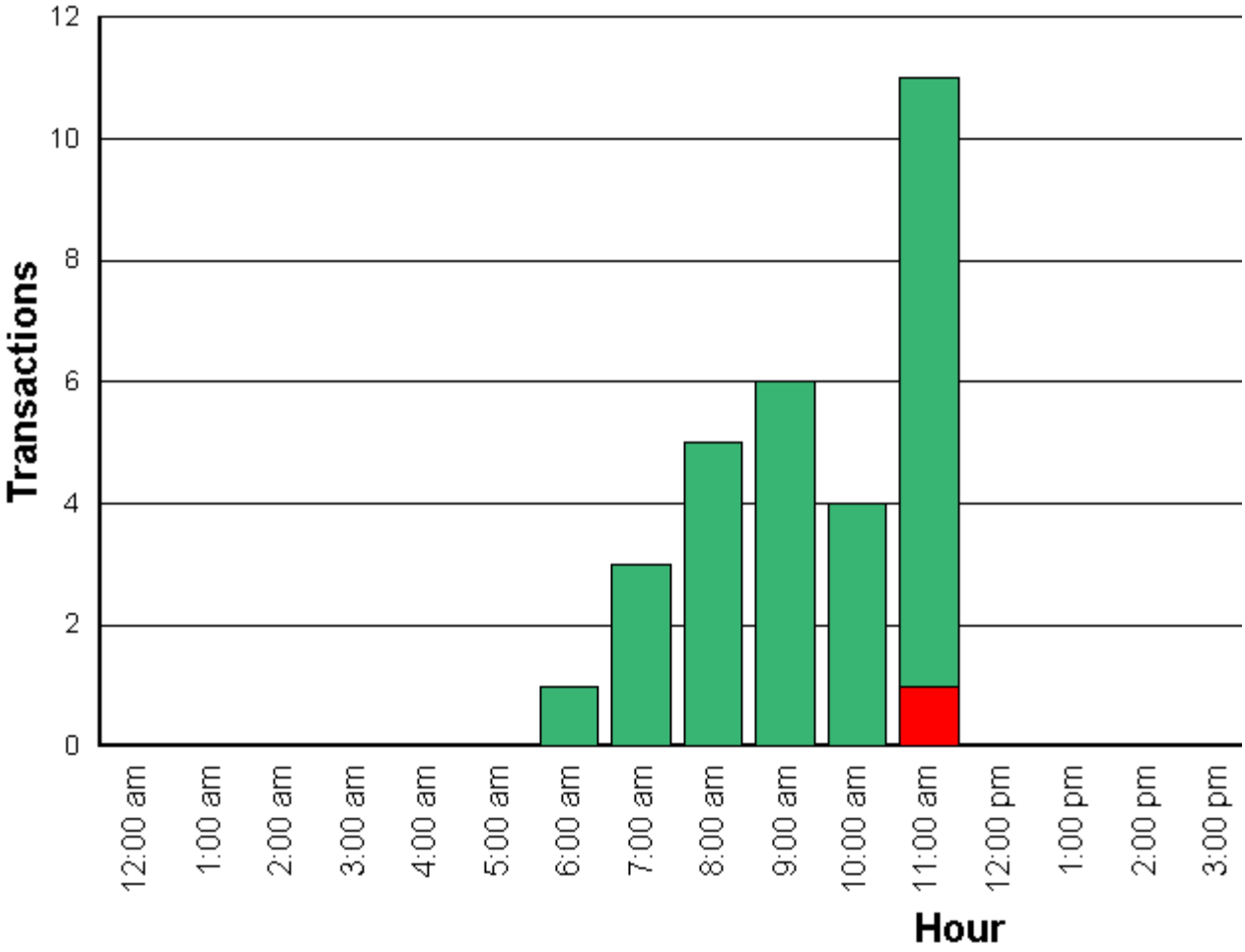
- Daily Transactions—Cover all successful and failed authentications and authorizations by day.
- Hourly Transactions—Cover all successful and failed authentications by hour. You can view all of the day's transactions, or view the authentications, authorizations, or administration transactions separately.

Time Series reports are displayed as bar charts. You can view a chart of all transactions, or view the authentications, authorizations, or administration transactions separately.

The following is an example of a Daily Transaction Report.



The following is an example of an Hourly Transaction Report.



Chapter 17: Policy Server Management Console Reference

This section contains the following topics:

Policy Server Management Console

The Policy Server Management Console is where you perform Policy Server configuration and system management functions.

Policy Server Management Prerequisites

To access the Policy Server Management Console, you must be logged in locally to the Policy Server.

Starting the Policy Server Management Console

To open the Management Console

- (Windows) Use the Policy Server Management Console shortcut in the SiteMinder program group
- (UNIX) Run *install_dir*/siteminder/bin/smconsole.

Note: Consider the following:

- (Windows 2008) If the Policy Server is installed on Windows 2008, right–click the shortcut and select Run as administrator.
- (UNIX) The X display server must be running and the display enabled by 'export DISPLAY=n.n.n.n:0.0', where n.n.n.n is the IP address of the Policy Server host system.

Policy Server Management Console Fields and Controls

The Policy Server Management Console contains the following menus and submenus:

- File menu--Contains the following items:

  Load Settings

  Enables you to load previously saved console settings.

  Save Settings

  Saves console settings to a file with a .smc file extension. By default, .smc files are saved to the *<install directory>*/SiteMinder/bin directory, though you can select any location when saving or loading .smc files.

- Help menu--Contains the following items:

  About

  Displays version information for the console.

  Management Console Help

  Opens online help for the console.

The Policy Server Management Console contains the following tabs:

Status tab

Allows you to View the status of and start and stop the five main Policy Server processes.

Settings tab

Configure TCP and UDP port settings for Policy Server administration, agents, and radius connections, and to specify a Netscape Certificate Database File.

Data tab

Configure policy store, key store, and session store databases and audit log data locations.

Super User tab

Change the password of the Policy Server Super User.

Keys tab

Configure key management policy.

Logs tab

Configure audit logging.

Profiler tab

Enable and configure output for the profiler, which you can use for debugging Policy Server issues.

Advanced tab

Adjust the settings for the Policy Server administration journal and optional Event Handler libraries.

The Policy Server Management Console also contains the following standard controls:

Apply button

Save all settings and keeps the Management Console open.

Cancel button

Closes the Management Console without saving any settings changes.

OK button

Save all settings and close the Management Console.

More information:

Management Console--Status Tab Fields and Controls (see page 159)
Management Console--Settings Tab Fields and Controls (see page 160)
Management Console--Data Tab Fields and Controls (see page 165)
Management Console--Super User Tab (see page 169)
Management Console--Keys Tab (see page 169)
Management Console--Logs Tab (see page 170)
Management Console--Profiler Tab Fields and Controls (see page 172)
Management Console--Advanced Tab (see page 174)

Management Console--Status Tab Fields and Controls

The Status tab is where you monitor and manually start and stop the main Policy Server processes.

Note: The Policy Server installation process starts Policy Server and configures your system to run it automatically whenever the Policy Server system is restarted.

Policy Server Group Box

The Policy Server group box contains the following:

Red/green traffic signal status indicator

Shows *green* when the Policy Server is started and running. Shows *red* if the Policy Server is stopped.

Start button

Click to start the Policy Server.

Stop button

Click to stop the Policy Server

OneView Monitor Group Box

The OneView Monitor group box contains the following:

Red/green traffic signal status indicator

Shows *green* when the OneView Monitor is started and running. Shows *red* if the OneView Monitor is stopped.

Start button

Click to start the OneView Monitor.

Stop button

Click to stop the OneView Monitor

Note: If you use a method other than the Start and Stop buttons to start or stop services, or a service stops for some other reason while the console is open, the graphics on the tab may not accurately represent the state of Policy Server. Click the Update button to refresh the contents of the tab.

More information:

Start and Stop Policy Server Services on Windows Systems (see page 22)
Start and Stop Policy Server Processes on UNIX Systems (see page 22)

Management Console--Settings Tab Fields and Controls

The Settings tab is where you configure a number of general Policy Server settings. From the Settings tab, you can:

- Adjust TCP ports for access control processes
- Adjust administration settings including the TCP port and Inactivity Timeout
- Adjust connection settings
- Configure RADIUS settings
- Adjust performance settings
- Configure the OneView Monitor settings

Access Control Group Box

In addition to the Administration TCP Port, the Policy Server listens on three other TCP ports that are enabled upon installation to communicate with SiteMinder Agents. This group box allows you to assign port settings and thread pooling used to communicate with SiteMinder Agents.

Enable check box

Activates the TCP ports used by the Policy Server to communicate with Agents. (Enabled by default at installation).

Authentication Port field

Port that serves requests for the Policy Server authentication process.

Default: The default value is 44442.

Authorization Port field

Port that serves requests for the Policy Server authorization process

Default: The default value is 44443.

Accounting Port field

Port that serves requests for the Policy Server accounting process.

Default: The default value is 44441.

Note: Specify corresponding port numbers for the Policy Server in the Trusted Host Configuration Object.

Verify that the Network Services file lists no other services utilizing these ports. Also verify that if a firewall is located between SiteMinder Agents and Policy Servers, the firewall is configured to allow traffic to the ports used by the Policy Server processes.

Administration Group Box

This group box contains the port used for browser-based policy management and a timeout value for administrative inactivity.

Enable check box

Activates the TCP port used by the Policy Server for the administration process.

Administration Port field

Port on which the Policy Server User Interface listens.

Default: This value is set to 44444.

UI Inactivity Timeout field

Number of minutes of inactivity allowed before a SiteMinder Administrative session times out. The default value is 0 (zero) minutes, which means that the Policy Server User Interface can stay open indefinitely without regard to activity. Otherwise, the administrative session times out after the specified number of minutes.

Note: Unless the Policy User Interface always runs in a secure location, we recommend that you specify a non-zero timeout value, so that the UI times out when left unattended.

Connection Options Group Box

This group box allows you to specify the maximum number of Policy Server threads, and the idle timeout for a connection to the Policy Server.

Max Connections field

Indicates the maximum number of connections supported by the Policy Server, independent of the number of threads. All connections share the thread pool to fulfill requests.

Default: The default value is 256. This number can be increased significantly, especially in deployments with the following: Apache Web servers protected by SiteMinder Web Agents and IIS Web servers using virtual servers protected by SiteMinder Web Agents.

Idle Timeout field

Time, in minutes, that a Policy Server connection can remain inactive before it is terminated. The default value is 10 minutes.

Performance Group Box

This group box lets you configure cache and thread settings to tune Policy Server performance.

Maximum Threads field

Determines the maximum number of worker threads in the thread pool for Normal Priority messages.

Default: 8

Limit: The maximum number of worker threads available to Normal Priority messages depends on the operating system on which the Policy Server is installed and on the amount of memory available to the system. See your vendor-specific documentation for more information about thread usage.

The default number of worker threads in the thread pool available for High Priority messages is five and the maximum number is 20. You can change the default value by adding and setting the PriorityThreadCount registry key.

To add the PriorityThreadCount registry key in Windows

1. Run regedit.
2. Navigate to:

   HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\PolicyServer
3. Add the PriorityThreadCount key using the DWORD value.

   Note: Verify that the name of the key includes the equal sign (=).

   Example: PriorityThreadCount=
4. Set PriorityThreadCount to a value in the range 5-20.

   Example: 0x6;

   Limit: A value less than five or greater than 20 disables the registry key. When the key is disabled, the number of worker threads in the pool for High Priority messages is the default value of five.

To add the PriorityThreadCount registry key in UNIX

1. Navigate to: *policy_server_home*/registry.

   policy_server_home

   Specifies the Policy Server installation path.
2. Modify sm.registry and locate:

   HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\PolicyServer
3. Add the PriorityThreadCount key using the DWORD value.

   Note: Verify that the name of the key includes the equal sign (=).

   Example: PriorityThreadCount=
4. Set PriorityThreadCount to a value in the range 5-20.

   Example: 0x6;

   Limit: A value less than five or greater than 20 disables the registry key. When the key is disabled, the number of worker threads in the pool for High Priority messages is the default value of five.

User Az Cache Size field

Number of megabytes of memory reserved for the authorization cache.

RADIUS Group Box

This group box allows you to specify settings when your deployment includes RADIUS components.

Enable check box

Select this check box to activate RADIUS UDP ports. You cannot modify the Authentication and Accounting ports unless you select this check box.

Authentication field

Port that serves RADIUS authentication requests. The default value for this port is 1645.

Accounting field

Port that serves RADIUS accounting requests.

Default: The default value for this port is 1646.

Note: Verify that the Network Services file lists no other services utilizing these ports. Also verify that if a firewall is located between SiteMinder Web Agent(s) and Policy Server(s), the firewall is configured to allow traffic to the ports listed earlier.

OneView Monitor Group Box

The OneView Monitor runs locally on a Policy Server. However, you can specify remote settings as follows:

Allow Incoming Remote Connections check box

If set, the monitor service running on the same system as the Policy Server accepts connections from other Policy Servers in a clustered environment. Marking this check box allows you to configure the local Policy Server as the central monitor in a cluster of Policy Servers.

Connect to Remote Monitor check box

If set, the monitor service is running on another Policy Server in a clustered environment. If you select Remote monitoring, supply the host name (or IP address) and port where the monitoring service is running in the field below the check box.

More information:

Configure Policy Server Settings (see page 43)
Clustered Policy Servers (see page 101)
Cache Management Overview (see page 87)
How the Policy Server Threading Model Works (see page 224)

Management Console--Data Tab Fields and Controls

The Management Console Data tab is where you configure storage locations for Policy Server databases (Policy Store, Key Store, audit logs, Session Server, and Expiry Data Server).

The Data tab contains a number of context-sensitive controls. Select the database that you want to configure from the Database drop-down list. The database you select determines the storage possibilities that are available for that database type and, therefore, the options available on the Storage drop-down list. The combination of these settings determines the settings displayed in the context-sensitive storage options group box directly below them.

Database drop-down list

Specifies the database to configure. Select from Policy Store, Key Store, Audit Logs, and Session Server.

Storage drop-down list

Specifies the type of storage in which the selected database is held. The list of options is context-sensitive, only including valid storage possibilities for the selected database.

Use Policy Store check box (Key Store and Audit Logs only)

Setting this option configures the Policy Server to use the Policy Store database to hold the selected database also.

Note: This option is only available if the Policy Store is configured with 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 currently selected database).

When Use Policy Store Database is set, the Storage drop-down list and the context-sensitive storage option group box are grayed-out.

Enable Session Server check box (Session Server database only)

When enabled, the Session Server is enabled, allowing the Policy Server to support persistent sessions.

Note: Only enable the Session Server if you are going to use persistent sessions in one or more realms; when enabled, the Session Server impacts Policy Server performance.

Storage Options Group Box

The Storage Options group box contains context-sensitive controls that allow you to configure options for the storage type selected from the Storage drop-down list.

Note: Whenever you update parameters relating to an LDAP database, restart the Policy Server to make the new parameters effective.

LDAP Storage Options

Use the LDAP storage options to configure LDAP database connections:

LDAP IP Address

Server name or IP address of the LDAP server. For performance reasons, the IP address is preferred. You can specify multiple servers in this field to allow for LDAP server failover.

If the LDAP server is not listening on the default port, be sure to specify the port on which it is listening.

Root DN

LDAP branch under which the SiteMinder schema is located in the Root DN field

Example: o=myorg.org

Use SSL

Select this check box if your system is communicating with the LDAP directory over SSL. If you select this check box, specify a certificate database in the Netscape Certificate Database File field.

Admin Username

DN of the LDAP directory administrator.

Example: cn=Directory Manager

Admin Password

Administrative password for the LDAP directory.

ConfirmPassword

Used to verify the administrative password for the LDAP directory.

Test LDAP Connection

Press to verify that the LDAP parameters you entered are correct and that the connection can be made.

ODBC Storage Options

Use the ODBC storage options to configure ODBC database connections:

Data Source Information

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

User Name

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

Password

Specifies the password of the database account.

Confirm Password

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

Maximum Connections

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

Test ODBC Connection button

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

Text File Storage Options

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

File Name field

Specifies the full path of a file in which to store the Policy Server audit logs.

Browse button

Opens a file browser in which you can navigate to the required directory and then select or type the name of a file; this selection is used to populate the File Name field.

Netscape Certificate Database File Group Box

Netscape Certificate Database File field

Specifies the full path of the Certificate database file.

Browse button

Opens a file browser in which you can navigate to the required directory and then select or type the name of a file; this selection is used to populate the Netscape Certificate Database File field.

Note: This field does not require a value for Active Directory user stores configured in the Policy Server User Interface using the AD namespace. AD user stores use the native Windows certificate repository when establishing an SSL connection.

LDAP Referral Group Box

Enable Enhanced Referrals check box

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 field

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

More information:

Configure the Policy Store Database (see page 28)
Configure the Key Store or Audit Logs to Use the Policy Store Database (see page 29)
Configure a Separate Database for the Key Store (see page 30)
Configure a Separate Database for the Audit Logs (see page 30)
Configure a Database for the Session Server (see page 31)
Configure LDAP Storage Options (see page 32)
Configure ODBC Storage Options (see page 35)
Configure Text File Storage Options (see page 37)
Specify a Netscape Certificate Database File (see page 41)

Management Console--Super User Tab

The Super User tab is where you change the password of the Policy Server Super User.

Old Password

Specifies Old SiteMinder Super User password you want to replace.

New Password

Specifies the new SiteMinder Super User password.

Confirm New Password

Confirms new SiteMinder Super User password.

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

More information:

Change the Policy Server Super User Password (see page 47)

Management Console--Keys Tab

The Keys tab is where you configure how the Policy Sever handles Agent key generation.

Enable Agent Key Generation check box

If selected, the Policy Server generates dynamic keys and writes them to the key store. If this check box is not selected, the Policy Server does not generate keys.

Leaving Agent key generation disabled is useful if you want to limit the number of Policy Servers that generate Agent keys (for example, when more than one Policy Server is pointing at the same Key Store, only one of the Policy Servers should generate keys) or if a Policy Server uses a replicated key store for its Agent keys.

Encrypt Keys Using Policy Store Encryption Key check box

If selected, the Policy Server encrypts the key store using the Policy Server's Encryption Key. If this check box is not selected, you must enter a key store encryption key in the Key Store Encryption Key field.

Key Store Encryption Key field

For most single sign-on environments, the keys used by SiteMinder for single sign-on between cookie domains are handled using a single key store common to all Policy Servers.

In the case of a common key store for separate policy stores, you must enter the same key store key in the Policy Server Management Console for each Policy Server instance, unless all of the Policy Servers use the same Encryption Key.

Confirm Encryption Key field

Re-enter the key store encryption key in this field to confirm the key.

Cache Session Key check box

If selected, the session key, which is used to encrypt session and identity specs, is stored in memory in an unencrypted state. Selecting this check box increases performance, because the key will not have to be decrypted each time it is used.

Important! Although it increases performance, selecting this check box is less secure than the default setting. If this check box is not selected, the session key is decrypted each time it is used.

More information:

Configure Agent Key Generation (see page 61)

Management Console--Logs Tab

The Logs tab is where you configure Policy Server logging.

Policy Server Log Group Box

The Policy Server Log group box is where you specify settings for the Policy Server log. This log records information about the status of the Policy Server and its processes.

Logfile field

Specifies the name and location of the log file. Enter a file name, or use the Browse button to specify a file.

(Logfile Rollover) When the server is restarted check box

If set, the Policy Server log will reset each time the server restarts. This option takes precedence over the size and time-based options.

(Logfile Rollover) When logfile reaches # MB check box

If set, the Policy Server log will create a new log file whenever the maximum log size (in megabytes) specified in the associated field is reached.

(Logfile Rollover) Time Based check box

If set, the Policy Server log will reset:

- hourly, based on the hour you select from the drop-down menu. The number must be a factor of 24 so you can select either 1, 2, 3, 4, 6, 8 or 12 as the hour. Further, the rollover time is calculated from 12:00 AM, so, if you specify 8, then log files will rollover at 8:00 AM, 4:00 PM, and 12:00 AM. The time zone is local to the machine where the Policy Server is installed.

  OR

- daily, based on a number that you specify between 1 and 100 days and at a time that follows the format (*hh*:*mm*) of a 24-hour clock. For example, you should enter 5:10 pm as 17:10. The exact time of next rollover is calculated from last time that the Policy Server had to perform a time-based log file rollover.

Retain up to # old logfile(s) field

Specifies the number of old log files that will be saved by the Policy Server. The old log files are saved in the directory you specified in the Logfile field.

Note: For Windows Policy Servers, it is generally better to write log files to local storage rather than to a network drive. If log files are written on a network drive, you must start and stop Policy Server manually from a command prompt, instead of using the Management Console Status tab. If you use the Management Console to stop and restart services, the Policy Server cannot write to a log file on a network drive.

Policy Server Audit Log Group Box

The Policy Server Audit Log group box is where you specify the types of auditing events that should be included in the Policy Server log.

Authentication Events drop down list

Specifies which client authentication events the Policy Server should log (Log All Events, Log Rejection Events only, or Log No Events).

Authorization Events drop down list

Specifies which client authorization events the Policy Server should log (Log All Events, Log Rejection Events only, or Log No Events).

Affiliate Events drop down list

Specifies which affiliate events the Policy Server should log (Log All Events, or Log No Events).

Administrator Access Events drop down list

Specifies which administrator access events the Policy Server should log (Log All Events, Log Rejection Events only, or Log No Events).

Note: For more information about auditing administrator changes to the policy store, see the *Policy Server Administration Guide*.

RADIUS Log Group Box

The RADIUS Log group box is where you specify log settings for RADIUS activity (only available if your Policy Server is configured as a RADIUS server).

Log to File check box

Select this option to enable RADIUS logging. If you select this check box, enter a path and file name for the log file in the field below the check box. You can click the Browse button to search for a location or file.

Append File check box

Select this option to append logging information to the log file you specified after a Policy Server restart. If you do not select this check box, when you restart the Policy Server, existing log file information is deleted, and the log begins recording activity from the point of the restart.

More information:

Configure the Policy Server Logs (see page 73)
Use the Policy Server as a Radius Server (see page 231)

Management Console--Profiler Tab Fields and Controls

The Profiler tab is where you set up the Policy Server Profiler to trace internal Policy Server diagnostics and processing.

Configuration Settings Group Box

The Configuration Settings group box is where you enable or disable profiling, and where you specify a configuration file for the profiler. If you want to create or edit a configuration file, you can access the Policy Server Profiler using the Configure Settings button.

Enable Profiling check box

Select to enable profiling for the Policy Server.

Configuration File drop down list

Select any Profiler configuration file that has already been selected during this management session from the list, or click the Browse button to select another configuration file.

Configure Settings button

Opens the Policy Server Profiler dialog from where you can choose components and data fields to trace, and create filters.

BufferedTracing

(Solaris) Select to buffer trace messages when written to the trace logs. This results in maximum Policy Server performance when the profiler is enabled. Deselect to allow trace messages to be written to the trace logs without being buffered. This results in slower performance, but provides maximum compatibility with the previous log writing behavior.

Output Group Box

The Output group box is where you specify the output format for information generated by the Policy Server Profiler.

Output to Console check box

Select to send profiler output to a console window.

Output to File check box

Select to send profiler output to a file. If you select this check box, specify a path and file name in the field below the check box.

Select Output Format

Select one of the following radio buttons to specify Profiler output format:

SiteMinder Default radio button

Output is provided in the standard SiteMinder format (enclosed in square brackets []).

Note: The SiteMinder Default output format is required by Customer Support. In order for Support to troubleshoot an issue, Profiler output must be provided to Support using the SiteMinder Default output format.

Fixed Width Fields radio button

Select to configure the Profiler to provide output in a text file with fixed-width fields. If the data in a field does not match the width, it is padded with spaces. If the data in a field is too long, extra characters are truncated.

XML Tags radio button

Select to configure the Profiler to generate output using XML tags to identify the output.

Field Delimiter radio button

Select to configure the Profiler to generate output delimited by the character you specify in the field to the right of the radio button.

Note: Do not use a semicolon (;) as the delimiting character.

More information:

Configure the Policy Server Profiler (see page 75)
Policy Server Profiler Dialog Box (see page 175)

Management Console--Advanced Tab

The administrative journal is a record of administrative changes applied to the Policy Server. Administrative changes are distributed to every Policy Server in a SiteMinder installation through a central policy store, where the administrative journal is kept.

On the Advanced tab, you can configure the administrative journal by specifying how often administrative changes are applied to the Policy Server and how long the Policy Server maintains a record of the applied changes. You can also configure a list of shared event handler libraries on the Advanced tab.

Administrative Journal Group Box

Apply administrative changes every (seconds)

Specifies the time interval in seconds between applications of administrative changes to the Policy Server.

Default: 60 seconds

Flush journal entries older than (minutes)

Specifies the age of journal entries in minutes after which they are flushed from the administrative journal.

Default: 60 minutes

Event Handlers Group Box

Comma separated list of event handler libraries:

Specifies a list of event handler libraries separated by commas.

Example: EventSNMP.dll

The default event handler library is located in the *policy_server_install_directory*/bin directory.

More information:

Configure Advanced Settings for the Policy Server (see page 81)
SNMP Monitoring (see page 127)

Tasks Related to the Policy Server Management Console

The following tasks are related to the Policy Server Management Console:

- Start and Stop Policy Server Services on Windows Systems (see page 22)
- Start and Stop Policy Server Processes on UNIX Systems (see page 22)
- Configure Policy Server Settings (see page 43)
- Configure Access Control Settings (see page 44)
- Configure Policy Server Administration Settings (see page 44)
- Configure Policy Server Connection Options (see page 44)
- Configure Policy Server Performance Settings (see page 44)
- Change the Policy Server Super User Password (see page 47)
- Configure Agent Key Generation (see page 61)
- Configure the Policy Server Logs (see page 73)
- Change Profiler Settings (see page 76)
- Configure Advanced Settings for the Policy Server (see page 81)

Policy Server Profiler Dialog Box

The Policy Server Profiler dialog box is where you specify which components and data fields will be included in Policy Server tracing, and apply filters to tracing output so that the profiler only captures specific values for a given component or data field.

Policy Server Profiler Dialog Prerequisites

To access the Policy Server Profiler dialog, the Enable Profiling option must be set on the Management Console Profiler tab.

Navigating to the Policy Server Profiler Dialog

To access the Policy Server Profiler dialog to configure Profiler options, click the Configure Settings button on the Management Console Profiler tab.

Policy Server Profiler Fields and Controls

The Policy Server Profiler dialog contains the following tabs:

Components tab

Contains controls that allow you to specify the Policy Server components (actions executed by the Policy Server) that the Profiler should trace.

Data tab

Contains controls that allow you to specify the Policy Server data fields (actual pieces of data used by the Policy Server to complete its tasks) that the Profiler should trace.

Filters tab

Contains controls that allow you to specify filters that will include or exclude information from the tracing process.

Other controls:

Template drop down list

Specifies a template file that file that contains a pre-defined set of components and data fields appropriate for a particular tracing task:

general_trace.template

Provides options for general, broad scope tracing.

Note: Multiple templates cannot be loaded/merged. If you wish to gather a wide range of information, use general_trace.template.

authentication_trace.template

Provides options for tracing user authentications.

authorization_trace.template.txt

Provides options for tracing user authorizations.

Note: If you have purchased SiteMinder Federation Security Services, additional federation-related templates are provided. For more information, see the *Federation Security Services Guide*.

Load Template button

Loads the profiler template file specified in the Template drop down list. Loading a Profiler template replaces the configuration currently in memory with that defined by the template.

More information:

Policy Server Profiler--Components Tab (see page 177)
Policy Server Profiler--Data Tab (see page 177)
Policy Server Profiler Dialog--Filters Tab (see page 181)

Policy Server Profiler--Components Tab

The Components tab is where you specify the Policy Server components--the actions executed by the Policy Server, divided into logical groups--that the profiler should trace.

Available Components list

List of all components that may be selected for tracing by the Profiler. Expand any component in the list to view its sub-components by clicking on the + symbol to the left of the component entry.

Selected Components list

List of components currently selected for tracing. Expand any component in the list to view its sub-components by clicking on the + symbol to the left of the component entry.

Right Arrow button

Adds a component (or subcomponent) selected from the Available Components list to the Selected Components list.

Left Arrow button

Removes a component (or subcomponent) selected from the Selected Components list and returns it to the Available Components list.

Note: When you select a subcomponent for inclusion in the Selected Components list, its parent component name is also included. For example, if you select the Resource_Protection sub-component of the IsProtected component, and click the Right Arrow button, both the IsProtected component is added to the Selected Components list. If you expand the component, you will see the Resource_Protection component has been added to the list.

Policy Server Profiler--Data Tab

The Data tab is where you specify the Policy Server data fields--actual pieces of data used by the Policy Server to complete its tasks--that the Profiler should trace.

Available Data Fields list

List of all components available for tracing.

Selected Data Fields list

List of all the currently selected components.

Right Arrow button

Adds a data field selected from the Available Data Fields list to the Selected Data Fields list.

Left Arrow button

Removes a data field selected from the Selected Data Fields list and returns it to the Available Data Fields list.

Up Arrow button

Moves selected data field up the Selected Data Fields list.

Down Arrow button

Moves selected data field down the Selected Data Fields list.

The following provides a brief explanation of the data the Policy Server can use to complete its tasks:

SearchKey

Displays the Searchkey in the form of string variable. The Searchkey indicates the key used during any searching operation done.

ErrorString

Displays the error string in the form of string variable. The error message is set in the ErrorString during the occurrence of error conditions in the code.

ErrorValue

Displays the error code returned by various functions as an integer value.

ObjectOID

Displays the object identifier (OID) of an object in the form of string variable.

Group

Displays the type of group to which the object belongs in form of string variable. The group can be rule, response or agent group.

Domain

Displays the domain of the object in form of string variable.

AgentType

Displays an agent type in form of string variable.

TransactionID

Displays the transaction ID in form of string variable.

ObjectClass

Displays the object classes for organizations in form of string variable. The object class defines the types of attributes that an entry can contain.

DomainOID

Displays the Siteminder domain OID in form of string variable pertaining to the domain in which the user is authenticated.

Property

Displays the name of the property of an object in form of string variable.

AuthStatus

Displays the Authenticating status can be redirection, error message and user message in form of string variable.

AuthReason

Displays authreason as an integer value. Authreason are the tokencodes transferred.

AuthScheme

Displays the authentication scheme used in form of string variable.

SessionSpec

Displays the server side session spec in form of string variable. Session spec provides the specification of the whole session and is encrypted and decrypted at the Policy Server side.

SessionID

Displays the server side session specification identifiers in form of string variable.

CertDistPt

Displays the distribution point of the certificate.

Action

Displays the requested action in form of string variable. It is generally of 3 types GET,POST and PUT.

RealmOID

Displays the Realm OID of the Realm in form of string variable pertaining to the realm in which the user is authenticated.

State

Displays the server state in form of string variable. It can be "INIT", "INACTIVE", "ACTIVE", "DISABLED", "INTER", "FAILED".

ClusterID

Displays the cluster identifier as an integer value. Every cluster is assigned a unique integer identifier. This id is mainly used for logging purposes.

HandleCount

Displays the handle count as an integer value. Handle count is the connection count.

Note: For SiteMinder r6.0 SP6, the BusyHandleCount and FreeHandleCount attributes are not used.

ResponseTime

Displays the average response time in milliseconds of the Policy Servers associated with a CA Web Agent or SDK Agent and API application.

Note: The ResponseTime data field cannot be enabled through the Policy Server Management Console. To output the ResponseTime to a trace log, edit the Web Agent Trace Configuration file, WebAgentTrace.conf, or other file specified in the Policy Server Configuration Object (ACO) and restart the Policy Server. For more information, see the *Web Agent Guide*.

Throughput

Displays the throughput as an integer value. Throughput is transactions per seconds.

MaxThroughput

Displays the maximum throughput (transactions per seconds) as an integer value.

MinThroughput

Displays the minimum throughput (transactions per seconds) as an integer value.

Threshold

Displays the active servers threshold number as an integer value.

TransactionName

Displays the Transaction Name in form of string variable. Transaction name is extracted from the request packet.

Data

Displays the data transferred (in response packet) in form of string variable.

HexadecimalData

Displays the hexadecimal data transferred (in response packet) in form of string variable.

Query

Displays the database access query, in form of string variable.

ActiveExpr

Displays the Active Expressions in form of string variable.

CallDetail

Displays the details of the call provided in form of string variable.

Policy Server Profiler Dialog--Filters Tab

The Filters tab is where you specify filters that will include or exclude information from the tracing process. The Filters tab contains a list of existing Profiler data filters and controls that allow you to add, remove, and those filters.

Filter Settings list

A selectable list of all existing filters.

Add button

Opens the Policy Server Profiler Filter dialog from where you can create a new filter.

Edit button

Opens an entry selected from the Filter Settings list in the Policy Server Profiler Filter dialog for editing.

Remove button

Removes a selected entry from the Filter Settings list.

More information:

Policy Server Profiler Filters Dialog (see page 181)

Tasks Related to the Policy Server Profiler Dialog

The following tasks are related to the Policy Server Profiler dialog:

- Configure the Policy Server Profiler (see page 75)
- Change Profiler Settings (see page 76)

Policy Server Profiler Filters Dialog

The Policy Server Profiler Filter dialog box is where you configure new or edit existing data filters for Profiler trace output.

If you are filtering a complete message into the smtracedefault.log profiling file, you must enter the exact text of the message into the filtering field in the Edit Filter section of the Policy Server Profiler filter dialog. The text must also match the message's case exactly.

For example, if you are filtering out the "Clearing the object cache" message, you must enter the exact message with the proper case. Entering "Clear" or "Clearing" does not work.

Navigate to the Policy Server Profiler Filters Dialog

To access the Policy Server Profiler Filters dialog to create a data filter for the Profiler

- On the Policy Server Profiler Filters tab, click the Add button on the Policy Server Profiler Filters tab.

To access the Policy Server Profiler Filters dialog to edit an existing Profiler data filter

- On the Policy Server Profiler Filters tab, Select an entry from the Filter Settings list and Click the Edit button on the Policy Server Profiler Filters tab.

Policy Server Profiler Filters Dialog Fields and Controls

Left drop down list

Specifies the data field to filter (for example, Resource, Domain, or AgentName).

Middle drop down list

Specifies the filter operator:

- Equal
- Not Equal

Right drop down list

Defines the matching value for the filter.

Tasks Related to the Policy Server Profiler Filters Dialog

The following task is related to the Policy Server Profiler Filters dialog:

- Change Profiler Settings (see page 76)

Chapter 18: System Settings Reference

This section contains the following topics:

System Settings in the Policy Server UI Overview

This sections that follow provide reference material for Policy Server management settings that are accessed from the Policy Server User Interface. These settings are not available from the Policy Server Management Console.

DMS Configuration Wizard Dialog

The DMS Configuration Wizard dialog box is where you create a set of SiteMinder objects that protect DMS resources and manage entitlements.

Note: For more information, see the *CA DMS Operations Guide*.

SiteMinder Global Settings Dialog

The SiteMinder Global Settings dialog box is where you enable or disable features with global reach throughout the SiteMinder environment:

- user tracking
- nested security
- enhanced Active Directory Integration

SiteMinder Global Settings Dialog Prerequisites

The following prerequisite must be met in order to successfully change global settings using the SiteMinder Global Settings dialog:

- Your SiteMinder administrator account must have the Manage System and Domain Objects privilege.

Navigate to the SiteMinder Global Settings Dialog

To access the SiteMinder Global Settings Dialog, select Tools, Global Settings from the Policy Server User Interface menu bar.

SiteMinder Global Settings Dialog Fields and Controls

Enable User Tracking check box

If set, SiteMinder Agents save Global Unique Identifiers (GUIDs) in cookies. Since each GUID is a unique value, a GUID in a cookie created by a SiteMinder Agent may be used to track an anonymous user and customize Web content.

Note: 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.

Enable Nested Security check box

If set, provides backwards compatibility for older versions of SiteMinder. This check box is enabled by default. CA strongly recommends that you do not modify this setting.

Enhance Active Directory Integration check box

If set, integration between an appropriately configure Active Directory user store is enhanced so that native Active Directory user persistence is synchronized when the Policy Server accesses the user store.

Note: You must have administrator credentials to modify the Active Directory user store and your SiteMinder administrator account must have the Manage Users privilege to successfully enable enhanced Active Directory integration.

Note: Enhanced Active Directory integration is not supported with ADAM.

Tasks Related to the SiteMinder Global Settings Dialog

The following tasks are related to the SiteMinder Global Settings Dialog:

- Enable User Tracking (see page 83)
- Enable Nested Security (see page 84)
- Enable Enhanced Active Directory Integration (see page 84)

SiteMinder Cache Management Dialog

The SiteMinder Cache Management dialog box is where you can flush the contents of the SiteMinder user session and resource caches.

More information:

Flush Caches (see page 89)

SiteMinder Cache Management Dialog Prerequisites

The following prerequisites must be met in order to successfully flush SiteMinder caches using the SiteMinder Cache Management dialog:

- To access the SiteMinder Cache Management dialog, your SiteMinder administrator account must have the Manage Users or Manage System and Domain Objects privilege.
- To access the Flush All caches option, your SiteMinder administrator account must have the Manage System and Domain Objects privilege.
- To access the Flush User Caches option, you must have the Manage Users privilege.

Navigate to the SiteMinder Cache Management Dialog

To access the SiteMinder Cache Management Dialog, select Tools, Manage Cache from the Policy Server User Interface menu bar.

SiteMinder Cache Management Dialog Fields and Controls

All Caches Group Box

Flush All button

Flushes all Policy Server and associated SiteMinder Agents caches: policy store, user sessions, resource information, and user directory caches, including certificate CRLs. This process takes up to twice the time specified by your policy server poll interval while the Policy Server synchronizes caches.

Note: Consider the following:

- To flush the policy store cache, enable the FlushObjCache registry key. If this key is not enabled, the policy store cache is not flushed.
- Flushing all caches may adversely affect access times for protected resources, since all requests immediately following the cache flush must retrieve information from user directories and the policy store. However, this action may be necessary if critical user privileges and policy changes must go into effect immediately.

User Session Caches Group Box

All radio button

If selected, all user sessions will be removed from the user cache when you click the Flush button.

Specific User DN radio button

If selected, the DN specified using the associated Directory and DN controls will be removed from the user cache when you click the Flush button.

Directory drop down list

Specifies the user directory that contains the DN you want to flush from the user cache.

DN field

Specifies the distinguished name you want to flush from the user cache. If you select this option, you must specify a user's DN, not a group's DN. If you do not know the DN, click the Lookup button to search for the DN. For information about searching for a DN, see the *SiteMinder Policy Design Guide*.

Flush button

Depending on the radio button selected above, flushes all users or a specific DN 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.

Resource Caches Group Box

Flush button

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.

Tasks Related to the SiteMinder Cache Management Dialog

The following tasks are related to the SiteMinder Cache Management Dialog:

- Flush All Caches (see page 90)
- Flush User Session Caches (see page 91)
- Flush Resource Caches (see page 92)
- Flush the Policy Store Cache (see page 95)

Key Management

The following sections detail how to manage Agent keys, session keys, and the Trusted Host shared secret.

SiteMinder Key Management Prerequisites

To successfully manage SiteMinder keys from the Modify Key Management pane , your SiteMinder administrator account must have the Manage Keys and Password Policies privilege.

Navigate to the SiteMinder Key Management Dialog

To access the SiteMinder Key Management Dialog, select Tools, Manage Keys from the Policy Server User Interface menu bar.

SiteMinder Key Management Dialog Fields and Controls

The SiteMinder Key Management Dialog contains the following tabs:

Agent Key tab

Allows you configure and manage Agent keys.

Session Ticket Key tab

Allows you configure and manage session ticket keys.

Shared Secret Rollover tab

Allows you to manage the Trusted Host shared secret.

SiteMinder Key Management Dialog--Agent Key Tab

The Agent Key tab is where you configure and Manage Agent keys.

Use Static Agent Key radio button

If selected, configures the Policy Server to use a static Agent Key and the lower section of the dialog changes to display controls to support static key configuration.

Use Dynamic Key radio button

If selected, configures the Policy Server to use a dynamic Agent Key and the lower section of the dialog changes to display controls to support dynamic key configuration.

(Static Agent Keys) Generate a Random Agent Key Group Box

Rollover Now button

Click to make the Policy Server generate and rollover to a new random static Agent key (within three minutes).

(Static Agent Keys) Specify an Agent Key Group Box

Static Key field

Specifies a value that the Policy Server should use as the static key. Use this option in situations where two key stores must use the static key to maintain a single sign-on environment.

Confirm

Re-specifies the static key to confirm its value.

Rollover Now button

Click to make the Policy Server generate and rollover to a new random static Agent key (within three minutes).

(Dynamic Agent Keys) Dynamic Key Detail Group Box

Manual Key Rollover radio button

Configures the Policy Server only perform Agent key rollover manually when the Rollover Now button is pressed.

Automatic Key Rollover radio button

Configures the Policy Server to automatically perform Agent key rollover at a frequency you configure by clicking the Set Rollover Frequency button.

Note: To enable automatic Agent key rollover, the Enable Agent Key Generation check box must be selected in the Keys tab of the Policy Server Management Console.

Set Rollover Frequency button

Opens the Set Rollover Frequency dialog.

Rollover Now button

Click to make the Policy Server generate and rollover to a new dynamic Agent key (within three minutes).

Note: There is no visible indication of action when you click Rollover Now. The Policy Server executes the rollover process silently. Do not click this button multiple times unless you want to rollover keys more than once.

More information:

Manage Agent Keys (see page 61)
Multiple Policy Stores with Separate Key Stores (see page 59)
Policy Server Management Console (see page 157)
Set Rollover Frequency Dialog (see page 191)

SiteMinder Key Management Dialog - Session Ticket Key Tab

The Session Ticket Key tab is where you manage SiteMinder session ticket keys.

Generate a Random Session Ticket Key Group Box

Rollover Now button

Click to cause the Policy Server to generate a new session ticket key. This key immediately replaces the one that is used to encrypt and decrypt session tickets.

Specify a Session Ticket Key Group Box

Session Ticket Key field

Specifies a new session ticket key.

Confirm field

Re-specifies the session ticket key to confirm its value.

Rollover Now button

Click to cause the Policy Server immediately replace the existing session ticket key with the value specified in the Session Ticket Key field.

More information:

Manage the Session Ticket Key (see page 67)

SiteMinder Key Management Dialog - Shared Secret Rollover Tab

Never Rollover Shared Secret radio button

Configures the Policy Server to rollover the shared secret

Rollover Shared Secret every radio button

Configures the Policy Server to rollover the shared secret according at the specified frequency (enter an integer in the first field to the right of the radio button and select a unit (Hours, Days, Weeks, or Months) from the drop down list).

Note: In order to enable periodic shared secret rollover, the Enable Agent Key Generation check box must be selected in the Keys tab of the Policy Server Management Console.

Rollover Now button

Click to cause the Policy Server to begin the process of rolling over shared secrets for all trusted hosts configured to allow shared secret rollover.

Note: The rollover may take some time depending on the number of trusted hosts in your deployment.

More information:

Policy Server Management Console (see page 157)

Tasks Related to the SiteMinder Key Management Dialog

The following tasks are related to the SiteMinder Key Management Dialog:

- Manage Agent Keys (see page 61)
- Manage the Session Ticket Key (see page 67)
- Shared Secrets (see page 69)

Set Rollover Frequency Dialog

The Set Rollover frequency dialog is where you configure the frequency at which automatic Agent key rollover should occur.

Set Rollover Frequency Dialog Prerequisites

In order to successfully set Agent key rollover frequency using the Set Rollover Key dialog, you must be in the process of configuring automatic Agent key rollover from the SiteMinder Key Management Dialog.

Navigate to the Set Rollover Frequency Dialog

To access the Set Rollover Frequency Dialog, click Set Rollover Frequency on the Agent Keys tab of the SiteMinder Key Management dialog box.

More information:

Key Management (see page 187)

Set Rollover Frequency Dialog Fields and Controls

Rollover Once Per Week radio button

If selected, the Policy Server will rollover Agent keys once per week on the day and time you select from the associated Day and Hour drop down lists. A time of 0:00 means 12:00 am.

Rollover Once Per Day

If selected, the Policy Server will rollover Agent keys once per day at the time you select from the associated Hour drop down list.

Rollover

If selected, the Policy Server will rollover Agent keys the number of times each day you select from the associated times per day drop down list. Such rollovers are distributed evenly throughout the day. For example, if you select 4 from the list, The Policy Server generates new keys at midnight, 6:00 AM, noon, and 6:00 PM.

Note: You must specify all times as Greenwich Mean Time (GMT). Since Policy Servers may span many times zones, this ensures that a SiteMinder deployment rolls over keys at a specific moment in time across all Policy Servers in your enterprise.

Session timeouts must be less than or equal to twice the interval between Agent key rollovers. If a session timeout is greater than twice the specified interval, users may be challenged to reauthenticate before their sessions terminate. For information about session timeouts, see the *SiteMinder Web Agent Guide* and the Policy Design Guide.

Tasks Related to the Set Rollover Frequency Dialog

The following task is related to the Set Rollover Frequency Dialog:

- Configure Periodic Key Rollover (see page 62)

Manage User Accounts Dialog

The Manage User Accounts dialog lets you disable a user account, change a user's password, or reset a user's password.

The User Search group box in this dialog contains the following settings:

Select/Name/Description table

Specifies the name of the user directory object and a description of the user directory, if a description was previously configured when setting up the user directory. You select the radio button that corresponds to the user directory where the user record is stored.

Important! A user directory must be part of a domain for it to show up in the list.

Search

Opens the Directory Users dialog so you can specify a search of the user directory you selected.

User Management Prerequisites

Your SiteMinder administrator account must have the Manage Users privilege to manage user accounts using the Manage User Accounts pane.

Navigate to the User Management Dialog

To access the User Management Dialog, select Tools, Manage Users from the Policy Server User Interface menu bar.

Manage User Accounts Directory Users Dialog

The Directory Users dialog lets you search the content of a user directory to locate a specific user.

This dialog contains the following settings:

Users/Groups box

Enables you to search for a user in a particular user directory.

Search Type

Specifies whether you select an attribute value or an expression.

Limits: Attribute-value, Expression

Attribute

Specifies the attribute the UI should search for in the directory. The attribute depends on the type of user directory configured for the domain. For LDAP, user directory attributes are the attributes that make up a user record, such as uid or carlicense. For ODBC, user directory attributes are named columns in the database table, such as Name or UserID.

This field is not displayed if the Search Type is an expression.

Value

Specifies the value associated with the attribute or expression. The value you enter depends on the type of user directory configured for the domain.

Example: Attribute-value search in an LDAP user directory:

Search Type: Attribute-value

Attribute: uid

Value: *

The asterisk instructs the UI to search all uids

Example: Expression search in an LDAP user directory:

Search Type: Expression

Value: uid=Admin

Change user's state group box

After you selected a user, you can click Enable (if the user is disabled), or Disable (if the user is enabled).

Change user password group box

Password

Specifies a new password for this user.

Confirm

Confirms the password you entered in the Password field.

Reset user's password

Forces a password change to modify the current password on the next login.

Tasks Related to the User Management Dialog

The following tasks are related to the User Management Dialog:

- Enable and Disable Users (see page 98)
- Manage User Passwords (see page 99)

Appendix A: General SiteMinder Troubleshooting

This section contains the following topics:

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

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.

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.

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\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 SiteMinder's LDAP referral handling to improve performance and redundancy. Previous versions of 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.

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 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\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\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\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\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. 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 Policy Server User Interface
- The error message:

  ```
  Exception occurred while executing audit log insert.
  ```

If either of these conditions occur, log to a text file instead.

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 Policy Server User Interface 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 Policy Server User Interface or the Command Line Interface.

[INFO] Server 'disablecacheupdates' command received.

This message is logged when cache flushing is disabled, either through the Policy Server User Interface or the Command Line Interface.

Appendix B: Scaling Your SiteMinder Environment

This section contains the following topics:

Environment Scaling Overview

This chapter provides general information about deploying SiteMinder in large and growing organizations. It also provides information about ways to tune the environment to improve the performance of SiteMinder.

How to Scale for Large Organizations

A large organization is generally defined as an environment that supports one or more Policy Servers and more than 20 Web Agents. Your organization may quickly expand into this category as your user population and resources grow.

SiteMinder scales to meet the needs of growing organizations. For information related to scaling to large environments, see the following sections:

- Manage Agent Keys in Large Environments (see page 208)
- How to Determine When to Add Web Agents (see page 208)
- How to Determine When to Add Policy Servers (see page 216)
- Database and Directory Considerations (see page 226)

How to Scale for Geographically Distributed Organizations

When configuring SiteMinder for an environment that is geographically distributed, see the following sections:

- Replication Considerations (see page 226)
- Timezone Considerations (see page 229)

Manage Agent Keys in Large Environments

Agent keys are used by Web Agents to encrypt and decrypt cookies passed to a user's browser. The value of an Agent key is initially set by the Policy Server when the Policy Server receives its first request from a Web Agent. The key is then used by the Web Agent to encrypt the contents of cookies it passes to the the user's browser. All Web Agents in a SiteMinder deployment must be set to the same value to participate in a single sign-on environment.

Changing the value of Agent keys on a regular basis provides the strongest security. If keys are updated on a regular basis, a key that may have lost its integrity would only be in use for a minimal amount of time.

The challenge of managing Agent keys in large organizations is that all Agent keys must be updated simultaneously. If the Agent keys in a SiteMinder installation are not all identical, communication between multiple Web Agents via single sign-on cookies cannot take place.

To address the challenge of changing all keys simultaneously, the Policy Server provides dynamic Agent key rollover. When the Policy Server is configured to use this feature, the Policy Server generates an Agent key dynamically and distributes the key to associated Web Agents. If the Web Agents are configured to work with multiple Policy Servers, new Agent keys are pushed out to these other Policy Servers in the SiteMinder installation, as well.

Note: Session timeouts must be less than two times the interval between Agent key rollovers. If a session timeout is not less than twice the interval, users may be challenged for credentials before their sessions terminate. For information about session timeouts, see the *Web Agent Guide*.

More information:

Policy Server Encryption Keys Overview (see page 49)

How to Determine When to Add Web Agents

To ensure the best performance of SiteMinder, the installation should have an adequate number of Web servers (hosting Web Agents) to support user requests. If there are not enough Web servers/Web Agents in place, users may face a delay in service if the Web servers operate under heavy loads of users. In the worst scenario, users will not be able to log in at all if their request to log in times out before being received by the Policy Server. Therefore, it is important to add more Web servers and Web Agents to the environment as user and resource requirements grow.

Estimate User Requests

There are several ways to estimate how many users a Web Agent supports:

- Generate a SiteMinder Activity report for each Web Agent in the installation. This report provides information about the time, user, category of activity, denials, failures, and a brief description of the activity.
- Generate an activity report for the Web server. For more information, see your Web server documentation.

More information:

Activity Reports (see page 145)

Determine the Number of Users the Web Agent Can Support

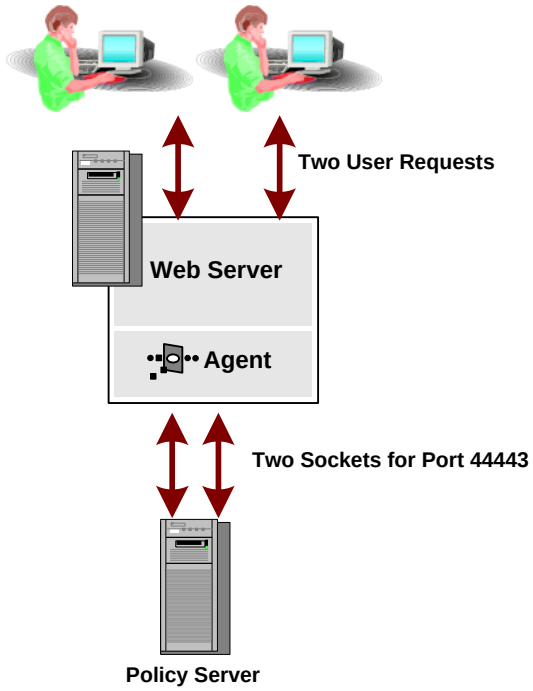
The number of concurrent users a Web Agent can support depends on several factors, including the number of *TCP/IP sockets* the Web Agent has available. Other factors that affect the number of users a Web Agent can support include:

- The amount of memory available to the Web Agent's Web Server
- The processor speed of the Web Agent's Web Server
- How cache is configured

How Requests are Handled

When a user request, such as a GET, PUT, or POST, is received by a Web Agent, the Web Agent forwards the request to the Policy Server. The Web Agent uses multiple threads to provide high performance processing of many requests. The Policy Server must provide enough sockets (one for each thread) to support communication with the Web Agent.

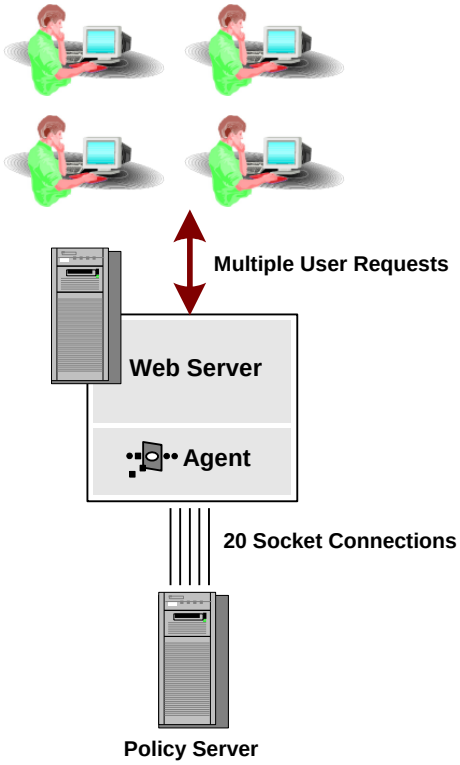
The Policy Service combines the Authentication, Authorization, and Accounting functions in to one service that listens, by default, on port 44443 for Web Agent requests. By default, a Web Agent requires two sockets to communicate with the Policy Server on port 44443.



Note: The Policy Server Management Console lists the default ports of 44442, 44443, and 44441 for Authentication, Authorization, and Accounting, respectively, for 5.x Web Agent mixed-mode compatibility with the Policy Server. A 5.x Web Agent opens sockets across all three ports to communicate with a Policy Server service.

The total number of sockets used by the Web Agent is one factor you must consider when determining how many Web Agents a Policy Server can support. More information exists in How to Determine When to Add Policy Servers (see page 216).

When the load requirements increase as more users attempt to access the resource protected by the Web Agent, the Web Agent uses more socket connections for each port. By default, the maximum number of socket connections that the Web Agent can sustain through port 44443 is 20.



Maximum Available Sockets for a Web Agent

By default, each Web Agent can sustain 20 sockets to each of the Policy Server. If the number of requests exceeds the open sockets at any given time, requests are placed in a queue.

How the Queue Works

The queue is designed to hold a maximum of 300 requests. For example, if the default Web Agent configuration values were not modified, 20 requests could be sent to the Policy Server at once. An additional 300 requests could then be placed in a queue. Therefore, using the default settings, the Web Agent could support 320 requests at any given moment.

By caching user information, Web Agents can support more than 320 requests at any given moment, even if you do not modify the default configuration options. However, in almost all deployments, far fewer than 320 simultaneous requests are required between a single Web Agent and the Policy Server.

Once placed in a queue, requests remain pending until one of the following takes place:

- A socket is made available and the request is sent to the Policy Server.
- The request times out.

Increase the Request Timeout

If the amount of time allocated for the request expires, the request is removed from the queue, and the user must re-attempt to access the resource. To avoid this situation when a Web Agent is experiencing a heavy load, the request timeout setting should be set to a greater amount of time. This value is defined in the Host Configuration Object which resides on the Policy Server. The default value is 60 seconds (60000 milliseconds).

Increase the Available Sockets for Web Agents

To handle a heavier load of requests, you can increase the default maximum number of sockets that the Web Agent can sustain for the port. The value is defined by the MaxSocketsPerPort setting in the Host Configuration Object.

Configure Web Agents Under Heavy Loads

For Web Agents in environments where there is heavy traffic between the Web Agents and the Policy Servers, modify the appropriate configuration settings identified below in the Host Configuration Object.

Sockets Usage

In this section, connections discussed are from the Web Agent to the Policy Server service listening on the default port of 44443. Therefore, if **nofiles(descriptors)** is set to 1024, that means that the Policy Server service has 1024 file descriptors available.

Netscape / Sun Java Systems web servers are assumed to be configured for the default of single-process mode (**MaxProcs** set to 1). Sun Java Systems (formerly iPlanet) v6 runs in multi-process mode by default.

Sockets and IIS/Sun Java Systems Web Agents

For Web Agents installed on IIS or Sun Java Systems Web Servers, the **MinSocketsPerPort** and **MaxSocketsPerPort** settings, in the host configuration object, determine the minimum and maximum number of sockets that will be open from the Web Agent to the Policy Server. When the Web server, with an installed and enabled SiteMinder Web Agent, starts, the Agent opens the number of sockets specified by the **MinSocketsPerPort** setting as defined in the host configuration object for the Agent.

As load increases, the number of sockets also increases, up to the number of sockets specified in the **MaxSocketsPerPort** setting in the host configuration object. If the Web Agent receives more requests than the number specified in **MaxSocketsPerPort**, then the overflow requests are placed in a queue.

Note: The queue for overflow requests has a limit of 300.

Each request uses a socket, but not all requests open new sockets. If all sockets from the connection pool are in use, then the Agent opens additional sockets as needed. New sockets are opened in groups defined by the number specified in the **newsocketstep** setting of the host configuration object. The Agent will continue to open new sockets as needed until the maximum limit specified in the **MaxSocketsPerPort** setting is reached. Only a single request can be executed on a socket, meaning that a socket is utilized until a reply comes back from the Policy Server. Once a request is completed, the socket is placed into a connection pool so that it can be used to service another request.

Once a socket is opened, it will not be closed. Exceptions include communication errors between the Agent and the Policy Server, and the idling out of connections by the Policy Server. Socket(s) will be closed by the Policy Server if they are unused for the length of time specified by the TCP Idle Session Timeout for the associated service (specified in the Policy Server Management Console).

Sockets and Apache Web Agents

Unlike the other Agents, Apache Web Agents do not use connection pooling. Apache is multi-processed and has a drastically different architecture from IIS and iPlanet Web servers, which are multi-threaded. Apache spawns child processes to handle requests, and uses a configuration setting called **MaxClients** to determine the maximum number of child processes that it will fork to handle load. The number of child processes is managed by Apache settings in the httpd.conf file. Each child process has its own independent socket connection(s) to the Policy Server. When the Apache parent process forks a child, an initial connection is opened to each Policy Server for the default Agent. The total number of sockets opened from an Apache server at maximum will equal the value of **MaxClients** times the number of trusted hosts.

Note: This connection model may have major implications for the Web Agent to Policy Server ratio (depending on the version of the Policy server being used), as the limiting factor often becomes connections between the agent and Policy Server, rather than the number of transactions per second. Before deploying Web Agents on Apache, it is very important to ensure that the Policy Server can handle the maximum number of connections that may be opened by all Web Agents that connect to it.

More information:

Sample Calculations for Sockets and Maximum Connections (see page 223)

Increase the Number of Sockets per Port

If the number of user requests will exceed 60 (20 requests being processed and 40 requests in queue) at any given moment, increase the Web Agent's MaxSocketsPerPort setting to a more suitable value. However, if you have multiple Trusted Hosts in the SiteMinder installation, and you increase the Max Sockets Per Port value for each Trusted Host, you may need to modify the Max Sockets setting in the Policy Server Management Console (Settings tab), as well.

More information:

How to Determine When to Add Policy Servers (see page 216)

Configure Dynamic Load Balancing or Failover

If the Web Agent works with multiple Policy Servers, configure dynamic load balancing to let the Web Agent distribute requests across all of the Policy Servers. Dynamic load balancing provides faster access to Policy Servers and therefore, more efficient user authentication and authorization.

Failover and load balancing considerations differ based on the type of Web server on which you install your Web Agents.

Failover/LoadBalancing for IIS or Sun Java Systems Web Agents

If you configure your environment for failover or load-balancing between Policy Servers, then the Web Agent opens the minimum number of sockets to each Policy Server at startup. Connections to a load-balanced Policy Server occur in the same way as connections to a single Policy Server, although fewer sockets may be opened to each Policy Server, since each is getting half of the total requests.

If configured for failover, and an error occurs between the Web Agent and the primary Policy Server, then connections to the failover Policy Server will be used. Failover occurs per service, so there may be active connections to both the primary and the failover Policy Servers at once. Once the primary Policy Server comes back up, the sockets opened to the failover server remain. All new sockets will be opened to the primary Policy Server. Failover is inherently part of load balancing; if one of the load balancing Policy Servers becomes unavailable, normal failover takes place.

Failover/LoadBalancing for Apache Web Agents

The Apache agent opens the same number of connections to all configured Policy Servers, whether or not failover has occurred. Since each child process has its own connection(s) to the Policy Server, failover occurs independently for each child. This can result in a 500 error for each socket as failover takes place. Once the primary Policy Server comes back up, the sockets opened to the failover server remain. All new sockets will be opened to the primary Policy Server. Failover is inherently part of load balancing; if one of the load balancing Policy Servers becomes unavailable, normal failover takes place.

Increase the Request Timeout

Modify the default value of 60000 milliseconds (60 seconds) if the network connections are slow or you expect a large number of users.

Note: Cache can also be increased to improve Web Agent performance, however, increasing cache is usually more appropriate for sites that are not experiencing a large number of policy changes, as described in the section below.

Improve Performance in More Stable Environments

For environments that are not subject to frequent policy changes, you can modify the following configuration parameters. Changing these values will improve performance by decreasing the amount of communication between Web Agents and Policy Servers. Therefore, Web Agents will not retrieve information about policy changes on a frequent basis.

Decrease the Policy Server Poll Interval

This parameter field determines how often the Web Agent retrieves information about policy changes from the Policy Server. A higher interval decreases traffic between the Policy Server and Web Agent. By default, the Web Agent polls the Policy Server every 30 seconds.

Modify the Maximum User Session Cache Size

This parameter specifies the size of the user cache, in megabytes, where the Web Agent caches information about authenticated users. When the cache fills to capacity, the Web Agent replaces the oldest user in the cache with a new user. The size of the cached information for each user entry will vary depending on resource usage requirements. You can increase performance by increasing the size of the cache according to your system's available memory.

Increase the Resource Cache Timeout

This parameter specifies the amount of time that resource entries remain in the cache. After the timeout expires, the Web Agent removes cached entries and contacts the Policy Server if the user attempts to access the protected resource again. By default, this value is set at 600 seconds (10 minutes).

How to Determine When to Add Policy Servers

Each Policy Server in the SiteMinder environment must have adequate resources to perform its tasks. As user populations grow and resources are added to the environment, the demands placed on each Policy Server within the environment grow. If the demands placed on the Policy Server exceed the capabilities of the server, performance suffers.

By default, the Policy Server provides 256 sockets for port 44443 (authorization, authentication, and accounting) when installed on either Windows NT or UNIX. Each socket can remain open for an unlimited period of time.

Two general factors can help you determine when to add Policy Servers to your environment:

- Determining the number of sockets a Web Agent opens to the Policy Server
- Determining the number of Web Agents a Policy Server supports

Determine the Number of Sockets Opened to a Policy Server

The Policy Server combines the following functions into one service:

- Authentication
- Authorization
- Accounting

By default this Policy Server service listens for Web Agent requests on port 44443.

Note: The Policy Server Management Console lists the default ports of 44442, 44443, and 44441 for Authentication, Authorization, and Accounting, respectively, for 5.x Web Agent mixed-mode compatibility with the Policy Server. A 5.x Web Agent can open sockets across all three ports to communicate with a Policy Server service.

The number of sockets a Web Agent opens to the Policy Server port is dependent on the following:

- The socket configuration settings in the Web Agent's host configuration object
- The web server's mode of operation and configuration
  - single-process/multi-threaded
  - multi-process/single-threaded
  - multi-process/multi-threaded

    Note: Refer to your vendor-specific documentation to determine the mode of operation in which your web server is operating.
- The Web Agent version

Host Configuration Object Socket Parameters

The number of sockets a Web Agent opens to a Policy Server is defined in the Host Configuration Object (HCO). The settings include:

MaxSocketsPerPort

Specifies the total number of sockets that a Web Agent can open to the port on which the Policy Server service is listening.

Default: 20

MinSocketsPerPort

Specifies, on start up, the minimum number of sockets that a Web Agent opens to the port on which the Policy Server service is listening.

Default: 2

NewSocketSetup

Specifies the increment to which new sockets are created. New sockets are created up to the number specified by MaxSocketsPerPort.

Default: 2

Single-Process/Multi-Threaded Web Server

A single-process/multi-threaded web server creates multiple threads to handle client requests. Each thread requires the Web Agent to open a socket to the Policy Server port on which the service is listening.

Note: You configure the maximum number of threads a process creates in the web server's configuration file. Consider the expected load on the web server when configuring this setting. Refer to your vendor-specific documentation for more information.

All three HCO parameters, MaxSocketsPerPort, MinSocketsPerPort, and NewSocketSetup, apply to a Web Agent installed on a single-process/multi-threaded web server.

Example: 5.x Web Agent

Using the default socket settings in the HCO on startup, a 5.x Web Agent opens two sockets to each port, 44441, 44442, and 44443, as specified by MinSocketsPerPort. As needed, the Web Agent opens additional sockets on each port as specified by NewSocketSetup up to the number specified by MaxSocketsPerPort.

The maximum number of sockets a 5.x Web Agent opens to communicate with each Policy Server listed in its HCO is 60:

(**MaxSocketsPerPort**)	x	(**Number of Ports on which Service Listens**)	=	(**Max Sockets**)
20	x	3	=	60

Example: 6.x Web Agent

Using the default socket settings in the HCO on startup, a 6.x Web Agent opens two sockets to port 44443, as specified by MinSocketsPerPort. As needed, the Web Agent opens additional sockets on port 44443 as specified by NewSocketSetup up to the number specified by MaxSocketsPerPort.

The maximum number of sockets a 6.x Web Agent opens to communicate with each Policy Server listed in its HCO is 20.

(**MaxSocketsPerPort**)	x	(**Number of Ports on which Service Listens**)	=	(**Max Sockets**)
20	x	1	=	20

Multi-Process/Single-Threaded Web Server

A multi-process/single-threaded web server creates multiple, concurrent single-threaded processes to handle client requests. Each thread requires the Web Agent to open a socket to the port on which the Policy Server service is listening.

Note: You configure the maximum number of processes the web server creates in the web server's configuration file. Consider the expected load on the web server when configuring this setting. Refer to your vendor-specific documentation for more information.

The MinSocketsPerPort setting in the HCO is the only applicable socket parameter to a Web Agent installed on a multi-process/single-threaded web server because the web server handles each request with a separate process. A Web Agent never has to handle more than one thread per process. As such, the Web Agent only needs to open one socket on start-up and does not need to open further sockets.

Note: CA recommends changing the MaxSocketsPerPort, MinSocketsPerPort, and NewSocketSetUp default settings to 1 to prevent Web Agents from opening unnecessary sockets. More information on modifying the default HCO settings exist in the *Policy Design Guide*.

Example: 5.x Web Agent

In this example, the Web Server is configured for 150 concurrent processes. Your environment may differ.

Using a MinSocketsPerPort setting of 1 on startup, a 5.x Web Agent opens one socket to each Policy Server port: 44441, 44442, and 44443. The maximum number of sockets a 5.x Web Agent opens to communicate with each Policy Server listed in its HCO is 450.

(**Max Processes**)	x	(**MinSocketsPerPort**)	x	(**Number of Ports on which Service Listens**)	=	(**Max Sockets**)
150	x	1	x	3	=	450

Example 6.x Web Agent

In this example, the Web Server is configured for 150 concurrent processes. Your environment may differ.

Using a MinSocketsPerPort setting of 1 on start-up, a 6.x Web Agent opens one socket to port 44443. The maximum number of sockets a 6.x Web Agent opens to communicate with each Policy Server listed in it HCO is 150:

(**Max Processes**)	x	(**MinSocketsPerPort**)	x	(**Number of Ports on which Service Listens**)	=	(**Max Sockets**)
150	x	1	x	1	=	150

Multi-Process/Multi-Threaded Web Server

A multi-process/multi-threaded web server creates multiple, concurrent multi-threaded processes to handle client requests. Each thread requires the Web Agent to open a socket to the port on which the Policy Server service is listening.

Note: You configure the maximum number of processes the web server creates and the maximum number of child threads for each process in the web server's configuration file. Consider the expected load on the web server when configuring these setting. Refer to your vendor-specific documentation for more information.

All three HCO parameters, MaxSocketsPerPort, MinSocketsPerPort, and NewSocketSetup, apply to a Web Agent installed on a multi-process/multi-threaded web server.

Example: 5.x Web Agent

In this example, the web server is configured for 150 concurrent processes. Your environment may differ.

Using the default socket settings in the HCO on startup, a 5.x Web Agent opens two sockets to each port, 44441, 44442, and 44443, as specified by MinSocketsPerPort. As needed, the Web Agent opens additional sockets on each port as specified by NewSocketSetup up to the number specified by MaxSocketsPerPort. The maximum number of sockets a 5.x Web Agent opens to communicate with each Policy Server listed in its HCO is 9000.

(**MaxSocketsPerPort**)	x	(**Number of Ports on which Service Listens**)	x	(**Max Processes**)	=	(**Max Sockets**)
20	x	3	x	150	=	9000

Example: 6.x Web Agent

In this example, the web server is configured for 150 concurrent processes. Your environment may differ.

Using the default socket settings in the HCO on startup, a 6.x Web Agent opens two sockets to port 44443, as specified by MinSocketsPerPort. As needed, the Web Agent opens additional sockets as specified by NewSocketSetup up to the number specified by MaxSocketsPerPort. The maximum number of sockets a 6.x Web Agent opens to communicate with each Policy Server listed in its HCO is 3000:

(**MaxSocketsPerPort**)	x	(**Number of Ports on which Service Listens**)	x	(**Max Processes**)	=	(**Max Sockets**)
20	x	1	x	150	=	3000

Determine the Number of Web Agents a Policy Server Can Support

The load requirements of the Policy Server depend upon how many Web Agents are configured to use the Policy Server, and how many requests each Web Agent supports. The sockets required by the Web Agents that the Policy Server serves must not exceed the maximum number of sockets that Policy Server provides. Socket requests are fulfilled by the Policy Server on a first come, first served basis.

For example, by default, the Policy Server provides a maximum of 256 sockets. By default, a Web Agent uses a maximum of 20 sockets. Therefore, if you do not modify the default values of either the Policy Server or the Web Agent, the Policy Server can support 12 Web Agents:

12(agents) x 20(sockets) = 240(sockets)

This configuration is acceptable because the total sockets required (240) is less than the 256 maximum default threshold. Adding another Web Agent would increase the socket requirement to 260, which the Policy Server could not support.

If you increase the sockets per port parameter for the Web Agent, the Policy Server would support fewer Web Agents, unless you modified the number of sockets the Policy Server provided.

For example, if the Policy Server provided 256 sockets, it would also support the following configuration:

4(agents) x 25(sockets) +
10(agents) x 15(sockets) = 250(sockets)

The total number of sockets used (250) would be less than the maximum number of sockets provided by the Policy Server. The four Web Agents configured to use 25 sockets could protect heavily used sites, where as the ten Web Agents using only 15 sockets could protect sites that experience lower traffic.

If the number of sockets required by the Web Agents exceeds the maximum provided by the Policy Server, you must do one of the following:

- Increase the number sockets provided by the Policy Server, as described in the following section, or
- Add another Policy Server to the configuration

Modify the Number of Connections Provided by Policy Servers

Modify the number of connections the Policy Server supports by changing the Max Connections value on the Settings tab of the Policy Server Management Console for each of the Policy Server.

Generally, there is no reason to decrease the default number of connections (256). You should only increase the value if the Web Agents served by the Policy Server require additional connections.

The maximum number of connections that the Policy Server can support is determined by the following settings:

- On UNIX: the kernel limit on open file descriptors. For more information about how to set this parameter, see the Policy Server installation instructions for UNIX in the Policy Server Installation Guide.
- On Windows: the number of open handles

A proper nofiles(descriptors) setting is required on Solaris Policy Servers to accommodate the sockets being opened by the Web Agents. This configures the ulimit or the number of file descriptors available to each Policy Server service. The ulimit should be set to at least 1024, and may be higher depending on the system needs and the version of Solaris being used. To set nofiles(descriptors) to 1024, for example, run ulimit –n 1024; this command usually is placed in smuser's .profile file so that it runs whenever smuser logs in (su – smuser). The nofiles(descriptors) value determines the maximum number of sockets and files which may be used at the same time by the process, which may include, besides connections to the agent, connections to such objects as the user directory and log files.

The Maximum Connections value may be increased up to just below the ulimit.

Note: There is a theoretical MaxConnections maximum of 32,000. However, CA recommends setting MaxConnections no higher than 10,000, which is the maximum tested value.

Note that some room must be left when setting Maximum Connections. For example, if it is calculated that there could be up to 1024 Web Agent connections, you should use the Settings Tab to set Maximum Connections to a slightly higher value, such as 1256.

Sample Calculations for Sockets and Maximum Connections

The following sections provide examples of how to calculate the needed number of sockets for Agents and the maximum connections for Policy Servers.

IIS and Sun Java Systems Examples

If there is one Web Agent, and thus one trusted host, connecting to the Policy Server, and the MaxSocketsPerPort setting is 20, then there will be a maximum of 20*1 = 20 open sockets. Even if multiple Agent identities are created within that Web Agent, as long as there is only one smhost.conf file, only one set of sockets will be opened to the Policy Server. If there are any Web Agents using the Policy Server for failover, then MinSocketsPerPort for each trusted host must also be added (except for Apache – see below). You should also calculate the total number of sockets needed on the Policy Server if all of the Agents failover completely.

By default, the maximum number of Agent connections is 256. If the number of client connections exceeds the number that the Policy Server can accept, the Policy Server will refuse additional connections. If this occurs, then with debug tracing enabled on the Policy Server, the following message appears in the debug log for the affected service:

```
"Rejected connection request. Too many server threads (256) or server is
shutting down."
```

In addition, 500 errors appear in the browser making the request.

Apache Examples

In Apache, the number of connections is calculated as one connection per Apache child process, per trusted host. For example, if you have a maximum of 150 child processes (value of MaxClients in httpd.conf) and 1 trusted host, then there will be a maximum of 150 * 1 = 150 connections from that Agent. The maximum number of child processes (Apache agents) / MinSocketsPerPort (other agents) for other Web Agents using the Policy Server for failover must also be added to that total.

If this occurs, then with debug tracing enabled on the Policy Server, the following message appears in the debug log for the affected service:

```
"Rejected connection request. Too many server threads (256) or server is
shutting down."
```

In addition, 500 errors appear in the browser making the request.

IIS and Sun Java Systems Recommendations

For IIS and Sun Java Systems Web Agents, if all sockets in the connection pool are being used, then this usually indicates that there is a bottleneck in the back end (Policy Server, user directory, and so on). For that reason, and to limit the number of connections to the Policy Server, CA recommends against increasing MaxSocketsPerPort above the default of 20. With the default MaxSocketsPerPort (Web Agent) and Maximum Connections (Policy Server) settings, 10-15 Agent identities may connect to a single Policy Server. You must ensure that the maximum number of sockets that can be opened does not exceed the capacity of the Policy Server to accept those connections.

Apache Recommendations

For Apache Web Agents, the suggested ratio of Web Agents to Policy Servers is of 2-4 Agent identities per Policy Server, depending on the Maximum Connections setting on the Policy Server and the MaxClients setting on each Apache instance, and the number of agent identities. You must ensure that the maximum number of sockets that can be opened does not exceed the capacity of the Policy Server to accept those connections.

How the Policy Server Threading Model Works

The Policy Server worker thread pool consists of two separate thread pools that independently process High Priority and Normal Priority messages. A reactor thread receives all incoming Web Agent requests and depending on the message type, passes them to either the High Priority or Normal Priority queue. High Priority messages include Agent connection requests. Normal Priority messages include user messages, such as authentication and authorization requests.

- **High Priority messages**—the default number of worker threads in the thread pool available for High Priority messages is five and the maximum number is 20. You can change the default value by adding and setting the PriorityThreadCount registry key.
- **Normal Priority messages**—the default number of worker threads in the thread pool available for Normal Priority messages is eight. You can add additional worker threads by modifying the Maximum Threads setting field on the Data tab in the Policy Server Management Console.

Note: For more information, see the Policy Server Management Console Reference in this guide.

The maximum number of worker threads available to Normal Priority messages depends on the operating system on which the Policy Server is installed and on the amount of memory available to the system. See your vendor-specific documentation for more information about thread usage.

Varying the size of the thread pool to improve performance is an iterative process that is largely dependent on the specific environment in use.

How to Configure Policy Servers Under Heavy Loads

If the load requirements of the Policy Server serving your site are large (any number that requires a great deal of CPU usage), you can:

- Turn Off Logging—Unless you are tracking log information for a specific reason, such as troubleshooting or monitoring usage, turn off logging. Logging may have an adverse affect on performance.
- Add Memory—Add more memory to the servers hosting the Policy Server. This will enable you to set a higher number of maximum sockets for the Policy Server.
- Add Additional Policy Servers—Adding additional Web servers for more Policy Servers enables the site to support more users and resources. Each Policy Server can be configured to use the same policy store. The Web Agents in the site can then be configured to use different Policy Servers, which spreads the load requirements among the multiple Policy Servers and improves performance.

Turn Off Logging

Unless you are tracking log information for a specific reason, such as troubleshooting or monitoring usage, turn off logging. Logging may have an adverse affect on performance.

Add Memory

Add Additional Policy Servers

Adding additional Web servers for more Policy Servers enables the site to support more users and resources. Each Policy Server can be configured to use the same policy store. The Web Agents in the site can then be configured to use different Policy Servers, which spreads the load requirements among the multiple Policy Servers and improves performance.

Dynamic Host Configuration Object (HCO) Updates

You can add Policy Servers to and remove them from an existing Policy Server cluster or the default cluster when no cluster is configured. Without dynamic HCO updates, the Web Server must be rebooted and the Host Configuration Object initialized by the Web agent for Policy Server changes to take effect.

With dynamic HCO updates, you can add and remove Policy Servers without needing to reboot the Web Server for the changes to take effect. The Web agent picks up the Policy Server changes dynamically and the Host Configuration Object is updated after a delay that depends on the internal polling interval.

Note: You cannot add or remove Policy Server clusters or modify other HCO parameters without rebooting the Web Server.

Enable Dynamic Host Configuration Object (HCO) Updates

With dynamic HCO updates, you can add Policy Servers to and remove them from an existing Policy Server cluster without needing to reboot the Web Server for the changes to take effect.

To enable dynamic Host Configuration Object (HCO) updates

1. Open the following file with a text editor:
   web_agent_home\config\SmHost.conf

   web_agent_home

   Specifies the directory where the Web Agent is installed.
2. Add or update the following line in the file:
   enableDynamicHCO="YES"
3. Save and close the SmHost.conf file.
4. Restart the Web Server.

Dynamic HCO updates are enabled.

Note: For more information, see the *Web Agent Installation Guide*.

Database and Directory Considerations

See the following guidelines for information related to tuning databases and directories.

Replication Considerations

Replicating databases is a process of creating and managing duplicate versions of a directory or database. Replicating databases and directories enables you to make changes to one directory, such as importing a policy store, and mirror the changes in the replicated database or directory.

Replicate databases and directories to:

- Improve performance in geographically distributed environments. For example, if there is a Policy Server in London, England and a Policy Server in Boston, Massachusetts, and the policy store is in Boston, you could replicate the policy store database and provide the London office with the replica. By replicating the policy store, both Policy Servers would be accessing the same data. However, the Policy Server in London could now access the replicated policy data faster, while creating less network traffic.
- Safeguard data. Replicating databases enables you to configure failover. If one database is taken off-line to be backed up or fails to respond to a request, the replicated database can be used in its place.

Netscape LDAP Directory Tuning

When using a Netscape LDAP directory for the policy store or user directory, follow these guidelines:

- Configure a primary and secondary directory, and configure the Policy Server to failover to the secondary directory. Configuring a backup directory ensures that if the primary directory fails, the secondary directory can be used in its place.
- Modify the LDAP directory timeout value to a number that is less than the Web Agent request timeout. For example, if the Web Agent request timeout is 60 seconds, set the LDAP timeout to 50 seconds. Setting a smaller timeout for the LDAP directory will avoid waiting for the LDAP directory to respond.
- Increase the size limit in entries. Specifies the maximum number of entries to return from a search operation.
- Increase the look thru limit entries. Specifies the maximum number of entries that are checked in response to a candidate search request.
- Increase max entries in cache. Specifies the number of entries the directory server will maintain in cache. Increasing this number uses more memory but can substantially improve search performance.
- Increase the DB cache size in bytes. Specifies the size in bytes of the in-memory cache. Increasing this number uses more memory but can substantially improve server performance, especially during modifications or when the indexes are being built. However, do not increase this number beyond the available resources for your machine.

For more information, see your LDAP documentation.

UNIX Server Tuning

To improve the performance of a UNIX server, follow these guidelines:

- Minimize the paging of memory to disk. Server performance often suffers if paged memory is used.
- Decrease size of buffers servicing requests. HTTP traffic found at Web sites is typically smaller than default buffer sizes.

General Considerations

nofiles Parameter

The nofiles parameter defines the total number of sockets and file descriptors that the shell and its descendants have been allocated. By default, this parameter is set to 64 on UNIX servers. Increasing this value increases the number of sockets you can use. For more information, see the *Web Agent Installation Guide*.

File Descriptors

The maximum number of file descriptors available to a Policy Server must match or exceed the sum of the maximum numbers of connections configured for each Web Agent talking to this Policy Server. However, in the case of Apache Web Agents, each child process may potentially use up to the maximal number of connections as well.

Therefore, it is recommended that the maximum number of file descriptors is set to unlimited on the Policy Server side. The maximum number of file descriptors can be configured by running the ulimit -n <value> command, where <value> is a positive integer or the word "unlimited".

Timezone Considerations

Policy and rule time restrictions are based on the local time defined on the server hosting the Policy Server. For example, if the Policy Server resides in Portland, Oregon, and a rule is configured to fire between 9 am and 5 pm, the rule would actually fire in Boston, Massachusetts between noon and
8 pm.

However, to configure Agent key rollovers, you must specify the time using Greenwich Mean Time (GMT). Using GMT ensures that all the keys rollover at the same time, regardless of the geographical location.

Note: For more information, see the *Web Agent Guide.*

More information:

Policy Server Encryption Keys Overview (see page 49)

Appendix C: Using the Policy Server as a RADIUS Server

This section contains the following topics:

Use the Policy Server as a Radius Server

Remote Authentication Dial-In User Service (RADIUS) is a protocol that enables you to exchange session authentication and configuration information between a Network Access Server (NAS) device and a RADIUS authentication server. You can use the Policy Server as the RADIUS authentication server.

The RADIUS protocol is often used by NAS devices that serve as:

- Proxy services for Internet Service Providers (ISP)
- Firewalls
- Corporate dial-up security services

The RADIUS Client/Server Architecture

RADIUS is designed to simplify security by separating the communication technology provided by a NAS device from the security technology provided by the authentication server. RADIUS security protects remote access to networks and network services using a distributed client/server architecture. The Policy Server is the RADIUS server. The RADIUS client is the NAS device.

A NAS device performs one of the following:

- Supports dial-in protocols, such as SLIP or PPP, authenticates users by using the RADIUS authentication server, and routes the user onto the network; or
- Supports direct connections to the network through a firewall, authenticates users by using the RADIUS authentication server, and grants network access.

The Policy Server can serve as the RADIUS authentication server when configured as described in this chapter. As the RADIUS server, the Policy Server authenticates RADIUS users using a RADIUS authentication scheme and a pre-defined user directory.

Note: To use RADIUS accounting, you must configure a separate RADIUS accounting server. The Policy Server will satisfy the NAS device by sending the ACK response to the accounting server. However, you can log accounting information to files.

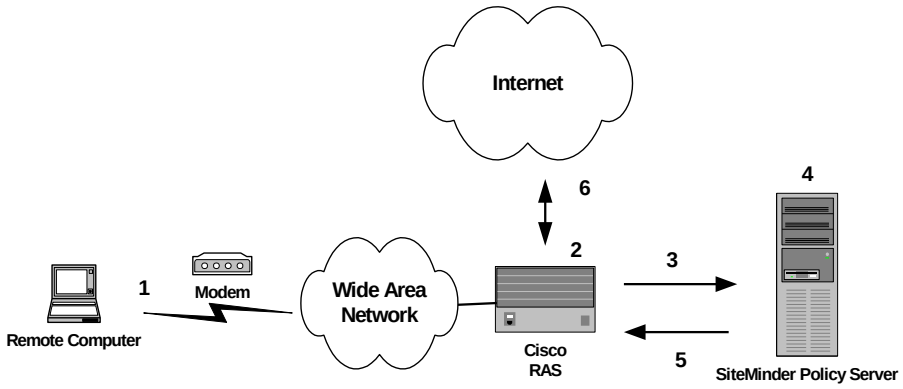
More information:

Generate RADIUS Logs for Accounting and Debugging (see page 267)

How RADIUS Authentication Works with the Policy Server

The Policy Server authenticates users through a series of communications with the NAS device. When SiteMinder authenticates a user, the NAS provides that user with access to the appropriate network services.

This authentication process is depicted in the following graphic:



1. A user dialing in from a modem attempts to open a connection to the Cisco RAS (a NAS device), which will enable the user to access the Internet.
2. The RAS determines that it must use a RADIUS user profile to authenticate the user.
3. The RAS sends the user connection request to the Policy Server.

4. The Policy Server obtains the user's name and password using one of the following methods:
   - Authenticates using Password Authentication Protocol (PAP)

     PAP is a PPP authentication protocol that provides a simple method for a host to establish its identity in a two-way handshake. Authentication takes place only upon initial link establishment and does not use encryption.
   - Authenticates using Challenge Handshake Authentication Protocol (CHAP)

     CHAP is also a secure PPP authentication protocol. CHAP provides a way to periodically verify the identity of a host using a three-way handshake and encryption. Authentication takes place upon initial link establishment. The RAS can repeat the authentication process any time after the connection takes place.
   - Authenticates using Security Dynamics ACE/Server or Secure Computing SafeWord server.
5. The Policy Server sends an authentication response to the RAS.
6. One of the following takes place:
   - If authentication is unsuccessful, the RAS refuses the connection.
   - If authentication is successful, the RAS receives a list of attributes from the SiteMinder response that fires upon authentication of the user. The attributes are used as a user profile, which configures the user's network session.

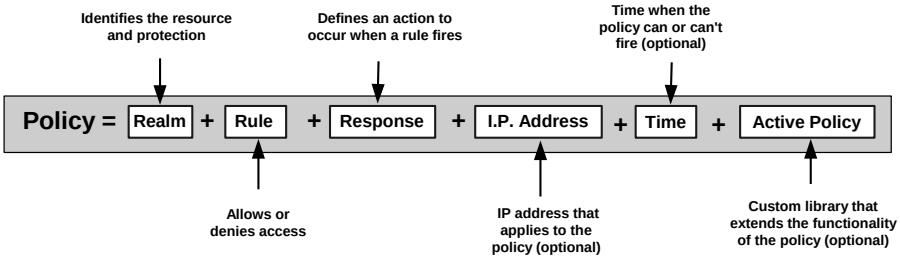
     The RAS notifies the Policy Server that the session has begun and when the session ends.

Policies in RADIUS Environments

A SiteMinder RADIUS policy is enforced by a RADIUS Agent and is created by binding the following elements together:

- An authentication rule
- A response
- A user or user group, and
- Optionally, an IP address, Time, and an active policy.

The basic structure of a policy is shown in the following diagram.



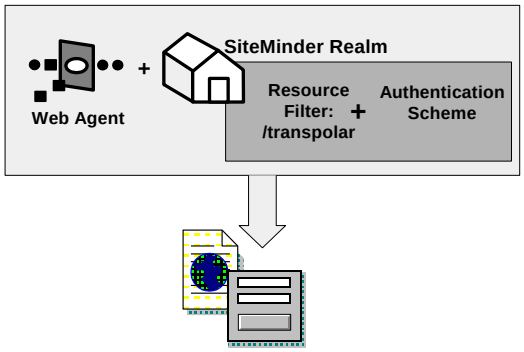
Although RADIUS policies are composed of the same elements that are contained in policies used by SiteMinder Agents, RADIUS Agents interpret the components differently. Rules, realms, and responses perform different functions, as shown in the following table.

Policy Component	In a RADIUS Policy, this item:	In a SiteMinder Agent Policy, this item:
Realm	■ Identifies the Agent. ■ Identifies the authentication scheme. ■ Defines session timeouts.	■ Defines the resource filter (directory within the domain that the SiteMinder Agent will govern). ■ Identifies the Agent. ■ Identifies the authentication scheme. ■ Defines the state (protected or unprotected) of the resource. ■ Identifies which events (authentication or authorization) to process. ■ Defines session timeouts.
Rule	■ Authenticates only. ■ Allows or denies access. ■ Defines time or active rule restrictions.	■ Defines the resource filter. ■ Defines the action (Web Agent action, authorization event, or authentication event. ■ Allows or denies access. ■ Authorizes and authenticates. ■ Defines time or active rule restrictions.

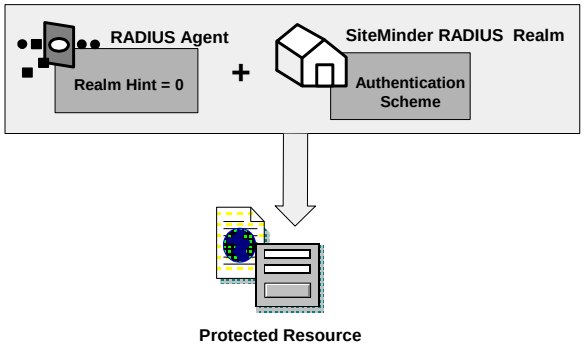
Policy Component	In a RADIUS Policy, this item:	In a SiteMinder Agent Policy, this item:
Response	■ Defines the values to return for authentication events.	■ Defines the value to return for an authorization event. ■ Defines the values to return for authentication events. ■ Defines the values to return for authorization reject events. ■ Defines the values to return for authentication reject events.

RADIUS vs. Non-RADIUS Resources

The elements of a RADIUS policy are treated differently in part because of how resources are identified in a RADIUS environment. In a SiteMinder Agent environment, specific resources are identified using a resource filter in the definition of the realm. The resource filter identifies the directory location of the resources. The realm definition also identifies the Web Agent and the authentication scheme, as shown in the following diagram:



As shown in the following diagram, protected resources are located differently in a RADIUS environment. Instead of the realm identifying the resource using a filter, the RADIUS Agent identifies the resource using a *realm hint*. A realm hint is an attribute that enables the Policy Server to establish the domain in which to authenticate users. The realm hint either identifies a specific realm that the Agent protects or signifies that the Agent must protect the entire NAS device.



Use Realm Hints

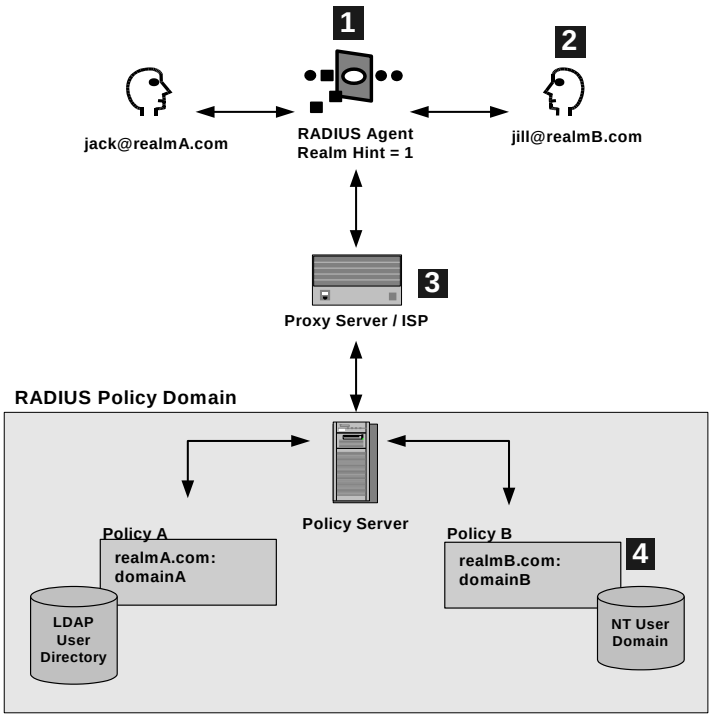
How does a RADIUS Agent protect a NAS device that must authenticate users in different domains, such as domainA and domainB? A realm hint is a RADIUS attribute that enables SiteMinder to determine the correct domain in which to authenticate a user. You must provide a RADIUS Agent with one of the following realm hint values:

- 0--(Default) Signifies that there is only one realm in the policy domain and therefore, a hint is not needed. The realm is bound to the NAS device directly.
- 1--(RADIUS User-Name attribute) SiteMinder parses the realm name from the user name in this attribute, then finds the associated domain, as explained below.
- An attribute that contains the actual name of the domain. This attribute is not available for all NAS devices. see your NAS device product documentation for more information.

When the realm hint is set to 1, the realm name is parsed from the user name attribute. The user_name-realm separator must be “@” or “/”.

- If the separator is “@” then the element following the “@” is the realm name. For example, in jack@realmA.com, the realm is realmA.com.
- If the separator is “/” then the element preceding the “/” is the realm name. For example, in x5/jack, the realm is x5.

The following diagram and explanation shows how a proxy server determines the correct SiteMinder domain in which to authenticate a user.



1. One RADIUS agent protects both SiteMinder domains. The RADIUS Agent is configured with the realm hint value of 1.
2. When Jill tries to access the ISP's proxy server, the RADIUS agent intercepts the request and forwards Jill's user name attribute jill@realmB.com to the Policy Server.
3. The Policy Server parses the user_name and realm_name from the user name attribute.

   Example: jill@realmB.com, where jill is the user_name and realmB.com is the realm_name.

   The Policy Server identifies the domain associated with the realm_name. The domain associated with realmB.com is domainB.
4. The Policy Server authenticates the user_name in the appropriate directory. The user_name jill is authenticated in the NT user domain defined for Policy B: realmB.com:domainB.

Responses in RADIUS Policy Domains

SiteMinder responses can be used to return RADIUS attributes to the NAS device if the user is authenticated. Attributes configure the characteristics of the session once the user is authenticated and define the user profile of the authenticated user. The user profile can be used by the NAS device. For example, using attributes in a response, you can define time limits for the RADIUS user session.

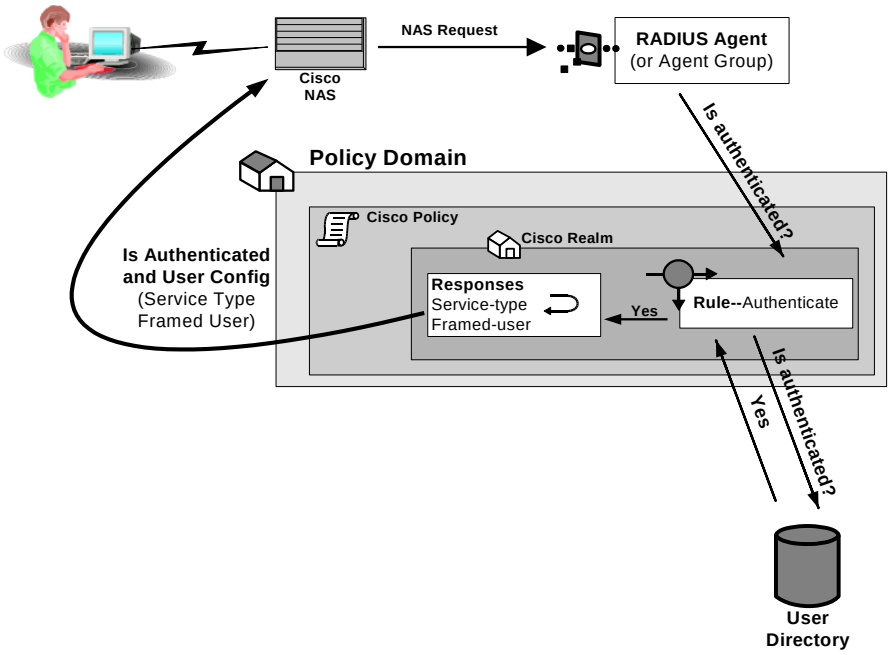
Using responses, you can provide the NAS device with user profile information that assigns privileges to the user. For example, you could allow one user unlimited access to a resource, yet limit another user's access to the same resource. Used in this way, responses give you the ability to authorize users even though RADIUS is primarily only a mechanism for authentication.

Note: If the NAS specifies authentication only, by default, SiteMinder does not return RADIUS attributes. To return RADIUS attributes when the NAS specifies authentication only, follow the instructions in Configure SiteMinder to Always Return RADIUS Attributes (see page 241).

How Responses Work

RADIUS responses are paired with rules that authenticate. If a rule authenticates a user successfully, the RADIUS response is triggered. If the rule does not authenticate the user, the response is not triggered.

If a response is triggered, the Policy Server sends the attributes contained in the response to the NAS device. This information is used to customize the user's session, as shown in the following diagram:



Attribute Types

You can use the following attributes in responses:

- User attributes
- DN attributes
- Active response attributes
- Radius attributes

User Attributes

These attributes return information associated with a user in an LDAP, WinNT, or ODBC user directory. User attributes are retrieved from the user directory and can used to modify the behavior of the RADIUS device.

Note: For more information about user attributes and how to configure user attributes, see the *Policy Design* guide.

DN Attributes

These attributes return profile information associated with an LDAP directory object related to the user. For example, the DN attribute could return information about LDAP objects such as the user's group or organizational unit (OU).

Note: For more information about DN attributes and how to configure DN attributes, see the *Policy Design* guide.

Active Response Attributes

These attributes return values from a custom library that was developed using the SiteMinder Authorization API. An active response is generated when SiteMinder invokes a function in the custom library.

For more information about active response attributes, see the *Policy Design* guide.

RADIUS Attributes

These attributes return values defined by the following Agent type attributes:

RADIUS

Generic RADIUS attributes, as defined by the RADIUS Protocol specification, *Request for Comment (RFC) 2138.* The identifiers for these attributes include 1-25 and 27-63. Some of these attributes may be used multiple times in the same response.

Any RADIUS Agent type can return a response that includes generic RADIUS attributes.

RADIUS Extended

Attributes defined in the Dictionary file of the NAS device. These attributes define values that are not defined by generic RADIUS attributes and are specific to the type of NAS device in use. The unique identifiers for these attributes extend beyond the range reserved for generic RADIUS attributes, starting with 64. For example, Lucent provides an extended RADIUS attribute called *Ascend-Disconnect-Cause,* which uses the identifier 195.

Only Agent types that match the vendor type of the extended RADIUS attribute can use the attribute. For example, a Shiva Agent type can use the extended RADIUS attributes defined for Shiva, but a Cisco Agent type cannot use Shiva extended attributes in a response. The extended attributes that are used in a response must match the attributes defined in the Dictionary file of the RADIUS client.

By default, SiteMinder provides pre-defined RADIUS extended attributes for some Agent Types that use these attributes, such as Ascend (Lucent). You can also define additional RADIUS extended attributes for any of the RADIUS Agent types, if necessary.

Vendor-Specific

Attributes defined in the Dictionary file of the NAS device, which use 26 as an identifier. Vendor-specific attributes enable you to define attributes for values that are not provided by the generic RADIUS attributes. Some vendors use vendor-specific attributes in place of or in addition to RADIUS extended attributes. For example, Cisco does not use RADIUS Extended attributes; however, this NAS device supports several vendor-specific attributes, such as *Cisco-AVpair* and *Account-Info*.

You can use vendor-specific attributes to pass information to other protocols. For example, you can define a vendor specific attribute for the Cisco-AV Pair attribute to pass TACACS+ information to a TACACS+ server.

Vendor-specific attributes can only be defined in responses that match the vendor type of the RADIUS client.

By default, SiteMinder provides pre-defined vendor-specific attributes for some Agent Types that use these attributes, such as the Network Associates' Sniffer Agent type. You can also define additional RADIUS extended attributes to any of the RADIUS Agent types, if necessary.

Note: For more information about RADIUS attributes, see *Request for Comment (RFC) RADIUS Protocol 2138.*

More information:

Create Attributes for Agent Types (see page 242)

Configure SiteMinder to Always Return RADIUS Attributes

Some NAS devices always expect RADIUS responses in the Access-Accept, even if the NAS specifies authentication only. If the NAS specifies authentication only, by default, SiteMinder does not return RADIUS attributes.

To always return RADIUS attributes to a NAS device, create a new registry value with the following parameters:

- Value type--DWORD
- Value Name--HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Authentication\AlwaysReturnRadiusAttrs
- Value Data--A numeric value greater than zero

Note: The install program does not create a registry entry for AlwaysReturnRadiusAttrs. Until you create and set the entry, SiteMinder uses the default value of 0.

After you set AlwaysReturnRadiusAttrs to a value greater than zero, the following message will appear in the Authentication Server's debug log:

> Radius Attributes will be returned regardless of RA_SERVICE_TYPE_AUTHENTICATE_ONLY

Create Attributes for Agent Types

Before you can use an attribute in a response, the attribute must be made available to the Agent type returning the response. Attributes are made available to Agent types by defining the attributes in Agent types. Although many Agent types are pre-configured with vendor-specific and RADIUS extended attributes, you can add additional extended RADIUS, generic RADIUS, and vendor-specific attributes to Agent types, as needed.

Define Multiple Instances of an Attribute

You can define multiple instances of a vendor-specific attribute for the same Agent type. When you define multiple instances of a vendor-specific attribute, you can send a different value to the NAS device for each instance of the attribute. For example, for a Cisco Agent, you could define the following vendor-specific attributes, all using the same identifier (26):

- Cisco-AVpair
- Account-Info
- Command-Code

The settings that define the number of times an attribute can be used within a response are located on the Properties tab of the Agent Attribute Properties dialog box.

To configure the attribute to be used multiple times, the Access Accept value must be set to Zero or Many.

The type of attribute that you define must match the vendor type of the Agent returning the response. For example, a vendor-specific Cisco attribute can only be returned by a Cisco Agent.

When the response is returned by the Agent, the packet structure of the response reflects the type of RADIUS Agent that sent the response. For example, the packet structure of a response returned by a Cisco Agent would include the vendor ID and the length of the string.

To define an attribute for an Agent type

1. In the Policy Server User Interface, choose Agent Types from the View menu.

   The Agent Types icon appears in the System Configuration list in the left pane.

2. Click the Agent Types icon.

   The SiteMinder Agent types List appears.

3. Double click the Agent type for which you want to configure a vendor-specific, RADIUS, or extended RADIUS attribute.

   The Agent Type Properties dialog box appears.

4. Select the Agent Type Attributes tab to move it to the front.

5. Click the Create button to create a new attribute.

   The SiteMinder Agent Attribute dialog box appears.

6. From the RADIUS Type drop-down list, select the appropriate type of attribute (Vendor specific, RADIUS Extended, or RADIUS).

   Note: More information about attribute types exists in Attribute Types (see page 239).

7. From the Data Type drop-down list, select the type of data the attribute contains.

8. In the Identifier field, enter one of the following attribute identifiers:

   - Generic RADIUS-- enter the attribute id as defined in the RADIUS protocol specification. For example, to create an attribute for the Callback-Id variable, enter 20.

     Although it is possible to overwrite the identifier of a Generic RADIUS attribute, you should generally retain the pre-defined Generic RADIUS attribute definitions, which match the RADIUS specification (*RFC 2138*).

   - RADIUS Extended--enter the attribute identifier as defined by the vendor documentation. For example, to create an attribute for the Ascend-Callback attribute, enter 246.

   - Vendor-Specific--enter 26. For example, to create an attribute for a Cisco Agent that enables the Agent to use TACACS+, enter 26.

   Note: For more information about the attribute identifiers, see your RADIUS vendor documentation.

9. In the RADIUS Behavior group box, define the RADIUS codes using the following fields:

Access Request

Provides information used to determine whether or not a user is allowed access to a specific NAS. The Access Request packets also provide information for any special services requested for that user.

Access Accept

Provides specific configuration information necessary to begin delivery of service to the user.

Note: You must set the Access Accept value to Zero or One, Zero or Many, or One and Only One in order to use the attribute in a response.

Access Reject

Sends information if any value of the received Attributes is not acceptable. This code is often used for reply messages.

Access Challenge

Sends information if the NAS device has been configured for challenge/response.

Accounting Request

Describes the type of service being delivered and the user to whom it is being delivered.

Accounting Response

Sends information if the Accounting Request was recorded successfully. A RADIUS Accounting-Response is not required to have any attributes in it.

For each code, you can define one of the following occurrences:

Not allowed

Attribute cannot be used in a response.

Zero or One

One instance or no instances of the attribute can be returned in the same response. If this value is selected, and you use the attribute in a response, the attribute will be removed from the Attribute drop-down list after you have used the attribute in a response.

Zero or Many

Multiple instances or no instances of the attribute can be returned in the same response.

One and Only One

One instance of the attribute must be returned in a response. If this value is selected, and you use the attribute in a response, the attribute will be removed from the Attribute drop-down list after you have used the attribute in a response.

10. If you selected Number from the Data Type drop-down list, click on the Value tab to assign possible values to the attribute.

    Use this tab to define a list of pre-defined values from which the user can choose when configuring the attribute in a response. The values are used in the Response Attribute dialog box, which is used when configuring a response.

    By mapping the symbolic names to the values, it is easier to use the attribute in a response, rather than having to remember the actual numeric values.

11. Click the Create button to define a value in the Agent Attribute Value dialog box.
12. In the Name field, enter the symbolic name of the attribute.
13. In the Numeric Value field, enter the actual numeric value of the attribute.
14. Click OK to save the attribute definition.
15. Click OK to save the attribute and close the Agent Attributes Properties dialog box.

    The attribute is added to the Agent Type Attributes list.

16. Click OK to save the Agent Type definition.

    The attribute is added to the properties of the Agent type. When you configure a response for this Agent type, you can use this attribute by selecting it from the Response Editor dialog box shown.

17. Define the attribute in the response.

More information:

Define the Response (see page 253)

Modify Existing Attributes

You can modify attributes that you created and attributes that have been pre-defined for a RADIUS Agent. For example, you can modify the pre-defined Ascend-PPP-Address attribute for the Ascend Agent type.

Note: When you modify an existing attribute, the attribute is not updated dynamically in responses that already use the attribute. If an attribute is used in a response, you must recreate the response using the updated attribute.

All RADIUS Agent types have been pre-configured to use the generic RADIUS attributes, as defined in *RFC 2138*. These attributes are available to be used by each RADIUS Agent type. You can configure responses to use the generic attributes from the Response Attribute dialog box.

Although the generic RADIUS attributes listed in the Attribute drop-down list do not appear in the Agent Attribute Properties dialog box, you can modify the values of the generic RADIUS attributes by overwriting the attributes using new attributes of the same name. For example, to modify the value of the generic RADIUS attribute Filter ID, define a new attribute called Filter ID for the appropriate RADIUS Agent type (Cisco, Shiva, etc.).

Important! If you overwrite a generic attribute or define a new attribute in the Generic RADIUS Agent, the change is applied to *all* RADIUS Agents. For example, if you modify the Filter ID attribute in the Generic RADIUS Agent, the modification is also made to all of the other RADIUS Agent types, such as Cisco, Shiva, Livingston, Ascend, Checkpoint, etc.

To modify attributes

1. In the Policy Server User Interface, select the Advanced menu and select Show Agent Types.

   The SiteMinder Agent types appear in the Agent Type List.
2. Double click the Agent type for which you want to modify a vendor-specific, RADIUS, or extended RADIUS attribute.

   The Agent Type Properties dialog box appears.
3. Select the Agent Type Attributes tab to move it to the front.
4. Select an existing attribute and click the Edit button.

   The SiteMinder Agent Attribute dialog box appears.
5. Modify the values as necessary and click OK to save the changes.

More information:

Create Attributes for Agent Types (see page 242)

Deploy SiteMinder in a RADIUS Environment

SiteMinder can be setup to provide authentication services in a variety of different RADIUS environments:

- A homogeneous environment composed of only one NAS device, such as a Cisco RAS, and only one user directory. This environment is discussed in How to Authenticate Users in a Homogeneous RADIUS Environment (see page 248).
- A heterogeneous environment composed of multiple NAS devices, such as a Checkpoint firewall and a Cisco RAS, and one user directory. This environment is discussed in Authenticate Users in Heterogeneous RADIUS Environments with One User Directory (see page 255).
- A heterogeneous environment composed of multiple NAS devices, such as a Checkpoint firewall and a Cisco RAS, and multiple user directories. This environment is discussed in How Authenticating Users in Heterogeneous RADIUS Environments with Two User Directories Works (see page 259).

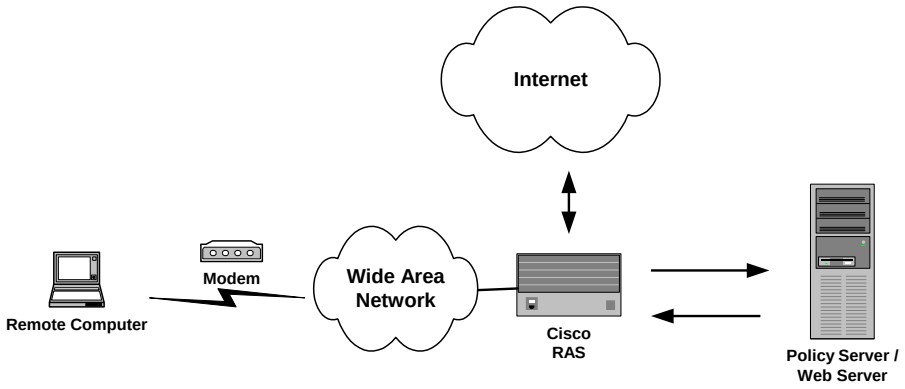
Guidelines for Protecting RADIUS Devices

Before deploying SiteMinder in a RADIUS environment, note the following guidelines:

- Realm names in the same policy domain must be unique.
- Only one type of RAS device can be protected within one policy. A single policy cannot protect more than one RADIUS device because each vendor uses a separate Dictionary file. The responses in a single policy must interpret return attributes identically. If the environment is heterogeneous and includes a variety of RAS devices, define a separate policy for each type of RADIUS device.
- Multiple user directories can be defined within one policy domain. When multiple user directories are defined, specify a search order.
- You can combine RADIUS Agents for different NAS vendors in a single generic RADIUS Agent group, and then use the same Agent group in a separate policy for each type of RADIUS Agent. For example, if the Agent group contained a Shiva Agent and a Cisco Agent, you would create a Shiva policy and a Cisco policy. The same rule and realm would be added to each policy, which saves time. However the response associated to each instance of the same rule would differ; the Cisco policy would associate a Cisco response to the generic rule and the Shiva policy would associate a Shiva response to the generic rule.

How to Authenticate Users in a Homogeneous RADIUS Environment

A homogeneous RADIUS environment is the most simple to protect. You can protect the RADIUS device using just one policy. This type of environment includes only one RADIUS device, such as a Cisco RAS, and one user directory, as shown in the following graphic:



To setup SiteMinder in a homogeneous RADIUS environment

1. Configure the system:
   a. Define the RADIUS Agent, as explained in Define the RADIUS Agent (see page 249).
   b. Setup a user directory against which to authenticate RADIUS users, as explained in Set Up the User Directory (see page 250)
   c. Optionally, you can also define administrative users and modify the authentication schemes.
2. Configure the policy domain:
   a. Create a RADIUS authentication scheme (CHAP or PAP), as explained in Create the Authentication Scheme (see page 251).
   b. Define a realm that identifies the RADIUS Agent and the RADIUS authentication scheme, as explained in Define the Realm (see page 251).
   c. Define a rule that enables authenticated users to access the realm protected by the RADIUS Agent, as explained in Define the Rule (see page 252).
   d. Define a response that provides the user profile to the NAS device and configures the characteristics of the session using response attributes, as explained in Define the Response (see page 253).
   e. Create a policy that binds the rule and response with the user directory, as explained in Create the Policy (see page 254).

More information:

How RADIUS Authentication Works with the Policy Server (see page 232)

Define the RADIUS Agent

In this example, only one RADIUS Agent will be defined, and it will protect only one domain. However, if the NAS device, such as a proxy server, services multiple domains, configure the Agent with a realm hint.

To define the RADIUS Agent

1. Start the Policy Server User Interface.
2. In the System tab, right click Agent and select Create Agent.

   The SiteMinder Agent Dialog box appears, as shown in the following graphic.
3. In the Name field, enter the name of the Agent.

   Use a name that is intuitive, such as the name of the NAS device.
4. Optionally, in the Description field, enter a description of the Agent, such as its purpose.
5. In the Agent Type group box, do the following:
   a. Select the RADIUS radio button.
   b. Select the appropriate vendor name from the drop-down list, such as Cisco.
6. In the IP Address field, enter the IP address of the NAS device.

   Use the DNS Lookup button to search for an IP address using a hostname.
7. In the Shared Secret group box, do the following:
   a. In the Secret field, enter the secret that is used by the NAS device.

      The secret is used by the Policy Server to authenticate requests from a NAS. Depending on the type of NAS device you are using, there may be some restrictions on the number of characters you can use; however, SiteMinder supports the RADIUS protocol specification which allows for 0-128 characters to be used in a shared secret.

      see your NAS device product documentation for more information.
   b. In the Confirm Secret field, re-enter the secret.

8. In the Realm Hint Attribute field, enter one of the following:
   - 0 if only one realm is going to be defined in the policy domain.
   - 1 if multiple realms are defined in the policy domain.
   - An attribute that contains the actual name of the realm, if such an attribute is available for the NAS device.
9. Click OK to save the settings and exit the dialog box.

   The RADIUS Agent definition is added to the Agent List.

More information:

Use Realm Hints (see page 236)

Set Up the User Directory

You can authenticate RADIUS users using any user directory that is supported for the NT or UNIX platform you are using.

If the user directory contains information about user privileges, you can create responses using user attributes. When the user attributes are sent back to the RADIUS device, the attributes are used to configure the user session.

You can use the following directories:

- ODBC-enabled database
- NT Domain
- Netscape or NDS LDAP

Note: For specific information about setting up a user directory, see the *Policy Design* guide.

Set up the Policy Domain

The policy domain must identify one or more user directories that contain the names of the RADIUS users, the names of the Administrators who can modify the domain, and the realm that the RADIUS Agent is protecting.

Note: For more information about setting up a policy domain, see the *Policy Design* guide.

Create the Authentication Scheme

You can use any of the following authentication schemes:

- Password Authentication Protocol (PAP)

  PAP is a PPP authentication protocol that provides a simple method for a host to establish its identity in a two-way handshake. Authentication takes place only upon initial link establishment and does not use encryption.

- Challenge Handshake Authentication Protocol (CHAP)

  CHAP is also a secure PPP authentication protocol. CHAP provides a way to periodically verify the identity of a host using a three-way handshake and encryption. Authentication takes place upon initial link establishment. The RAS can repeat the authentication process any time after the connection takes place.

- Security Dynamics ACE/Server or Secure Computing SafeWord server.

Note: For more information about creating an authentication scheme, see the *Policy Design* guide.

Define the Realm

By default, when you create a realm that is protected by a RADIUS Agent, the realm is protected. Therefore, you do not need to define rules for the realm that deny users access. If users do not match the criteria of the rule that enables access to the realm, they are automatically denied access.

In this example, there is only one realm, therefore, the RADIUS Agent that is protecting the realm was not configured with a realm hint.

To define the realm

1. In the Policy Server User Interface, select the Domain tab.
2. Right click the policy domain for the RADIUS device and select Create Realm.

   The SiteMinder Realm Dialog box appears.
3. In the Name field, enter a name for the Realm.

   Note: The name cannot contain the characters * or &.
4. Optionally, in the Description field, enter a description of the Realm.
5. Under the Resource tab, select the name of the RADIUS Agent from the Agent drop-down list.
6. From the Authentication Scheme drop-down list, select the appropriate authentication scheme.

   Note: Only authentication schemes that you have already created will be displayed in this drop-down list. If you have not created any schemes, this list will be blank.

7. Select the Session tab to move it to the front.
8. Under the Session tab, do the following:
   a. Optionally, in the Session Timeouts group box, specify the maximum amount of time that a session can remain active and the maximum amount of time that a session can remain idle.

      SiteMinder provides the NAS device with these session limitations. Once these time constraints have been met, the NAS device ends the session.

   b. Optionally, select the Synchronous Auditing check box to require that all authentication and auditing requests are successfully logged to the auditing log before the user is allowed access.

      The RADIUS auditing log is configured on the Debug tab of the Policy Server Management Console.
9. Click OK to save the realm definition and exit the dialog box.

Define the Rule

In this example only one rule is necessary. This rule will allow users to authenticate. When you define rules to authenticate RADIUS users, you can set time restrictions, which will configure the time limits of the session.

To define a rule to enable access

1. In the Domain tab, right click the Realm that will contain the rule and select Create Rule Under Realm.

   The SiteMinder Rule Dialog box appears.
2. In the Name field, enter a name for the rule.

   Note: Typically, you should name rules according to the action they perform. Using an intuitive naming strategy will make it easier to manage large groups of rules. The name cannot contain the characters * or &.
3. Optionally, in the Description field, enter a description of the rule.
4. In the Realm and Resource group box, select the appropriate realm from the Realm drop-down list.
5. In the Allow/Deny and Enable/Disable group box, do the following:
   - Select the Allow Access radio button to allow access when the user is authenticated.
   - Select the Enabled check box to enable the rule.

6. Optionally, in the Advanced group box, do any of the following:
   - Under the Time Restrictions tab, set time restrictions.
   - Under the Active Rule tab, define an active rule.
7. Click OK to retain the rule definition and exit the SiteMinder Rule Dialog box.

   The new rule appears in the Rule List.

Define the Response

By default, all users are prohibited from accessing a resource unless they are authenticated. Therefore, it is usually only necessary to define responses that allow access.

The following procedure assumes you have defined the attributes that you will use for the response.

Note: More information about defining attributes to use in responses exists in Create Attributes for Agent Types (see page 242).

To define a response

1. In the Domain tab, right click Responses and select Create Response.

   The SiteMinder Response Dialog box appears.
2. In the Name field, enter a name for the response.

   Note: Typically, you should name responses according to the action they perform. Using an intuitive naming strategy will make it easier to manage large groups of responses. The name cannot contain the characters * or &.
3. Optionally, in the Description box, enter a description of the response.
4. In the Agent Type group box, do the following:
   a. Select the RADIUS radio button.
   b. In the drop-down list, select the vendor name of the RADIUS device, such as Cisco.
5. To add RADIUS attributes to the Response, click Create in the Attribute List group box.

   The Response Attribute dialog box appears.

6. Under the Syntax Entry tab, do one of the following:
   - To add RADIUS attributes, do the following:
   a. Select the Static radio button.
   b. From the Attribute drop-down list, select the appropriate RADIUS attribute.
   c. Depending on the type of attribute you selected, either enter a value for the attribute in the dialog box that appears or enter a value for the attribute in the Variable Value field.
   d. To add additional attributes to the response, repeat steps a-c.
   - To add a user attribute, select the User Attribute radio button.
   - To add a DN attribute, select the DN Attribute radio button.
   - To add an active response, select the Active Response radio button.

   Note: For more information, see the *Policy Design* guide.
7. Click OK when you have finished adding attributes to the response.

   The attribute and value are listed in the Attribute List of the SiteMinder Response Dialog box.
8. In the Response Properties dialog box, click OK.

   The response definition is added to the Response List.

More information:

Responses in RADIUS Policy Domains (see page 238)

Create the Policy

Once you have created the RADIUS Agent, a realm, a rule, and a response, you can bind these components with the RADIUS user directory to create a policy. The policy will protect the RADIUS device.

To create the policy

1. In the Domain tab, right click Policies and select Create Policies.

   The SiteMinder Policy Dialog box appears.
2. In the Name field, enter a name for the policy.

   The name cannot contain the characters * or &.
3. Under the Users tab, add users to or remove users from the policy, by clicking the Add/Remove button.

   Note: For more information about excluding users and defining user directories, see the *Policy Design* guide.

4. Under the Rules tab, do the following:
   a. Click the Add/Remove Rules button.

      The Available Rules dialog box appears.
   b. In the Available Members box, select the rule.
   c. Click the left arrow to move it to the Current Members box.
   d. Click OK.

      The Available Rules dialog box closes.
5. Under the Rules tab, highlight the rule and click the Set Response button.

   The Available Responses dialog box appears.
6. Select the response you created and click OK.

   The Set Response dialog box closes and the response appears in the Rules tab.
7. If necessary, add IP Address, time, and active policy restrictions to the policy.

   Note: For more information about these restrictions, see the *Policy Design* guide.
8. When the policy is complete, click OK in the SiteMinder Policy dialog box.

   The policy is added to the Policy List. SiteMinder can now be used to authenticate users for the NAS device.

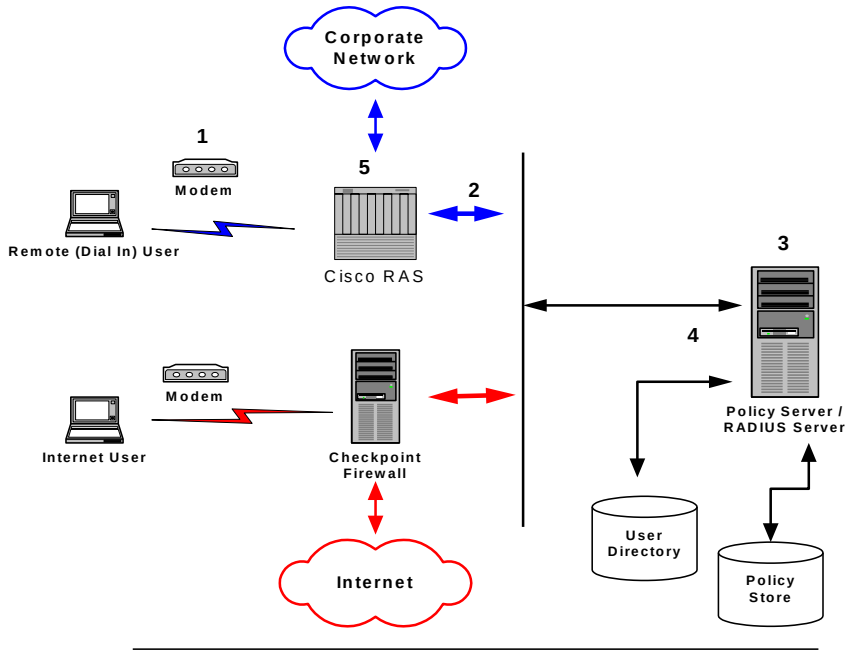
Authenticate Users in Heterogeneous RADIUS Environments with One User Directory

A more powerful and complex deployment of the Policy Server in a RADIUS environment is one that includes multiple realms administered by multiple NAS devices. In this scenario, the Policy Server can serve as the RADIUS authentication server for multiple RADIUS clients at once.

The advantage of using a heterogeneous configuration is that you save time by using the same RADIUS authentication server (that is, the Policy Server) for each RADIUS client.

How Users are Authenticated in Heterogeneous, Single Directory Environments

An example of a heterogeneous configuration is illustrated in the following graphic:



In the network topology shown in the previous diagram, the Policy Server authenticates users of two NAS devices: a Cisco RAS and a Checkpoint Firewall. The Policy Server uses one user directory to authenticate the users.

Each NAS device has its own RADIUS Agent, which has been configured with a realm hint. When the Policy Server receives a request to authenticate the user, it uses the RADIUS Agent's realm hint to determine the resource (domain) that the authenticated user can access.

The process of authentication when one user directory is used is as follows:

1. The remote user dials in from a modem and the Cisco RAS determines that it must use a RADIUS user profile to authenticate the user.
2. The RAS sends the user connection request to the Policy Server.
3. The Policy Server enacts the policy defined for the RAS, and the RADIUS Agent associated with the Cisco RAS does the following:
    a. Determines the user's domain using a realm hint.
    b. Obtains the user's name and password using the authentication scheme configured for the Agent.

4. The Policy Server evaluates the user information against the user directory and policy store.
5. The Policy Server sends an authentication response to the Cisco RAS and one of the following takes place:
   - If authentication is unsuccessful, the RAS refuses the connection.
   - If authentication is successful, the RAS receives a list of attributes from the user profile in the RADIUS server's database and establishes network access for the caller.

     The RAS notifies the Policy Server that the session has begun and when the session ends.

When the Internet user attempts to dial into the Internet Service Provider via the Checkpoint Firewall, a similar process of authentication occurs. Using the realm hint, the RADIUS Agent defined for the Checkpoint Firewall determines which domain the Internet user has access to. If the user is authenticated, the Policy Server passes the Firewall the correct attributes to establish the session.

User information for both NAS devices is stored in the same user directory. Each time the Policy Server receives an authentication request, it authenticates the user using the same data directory.

System and Policy Domain Configuration

This system configuration differs from the homogeneous environment; you must now create two Agents.

Within the policy domain there is one policy that includes rules and responses for the Cisco Agent and the Checkpoint Agent.

To setup SiteMinder in the heterogeneous, single directory environment described above, you must:

1. Configure the system:
   a. Define two RADIUS Agents, as described in Define Agents for a Heterogeneous, Single Directory Environment (see page 258).
   b. Setup a user directory against which to authenticate RADIUS users, as described in Configure the User Directory (see page 259).
   c. Create one policy domain, as described in Create the Policy Domain (see page 259).
   d. Create an authentication scheme, as described in Create the Authentication Scheme (see page 251).

2. Configure the policy domain:

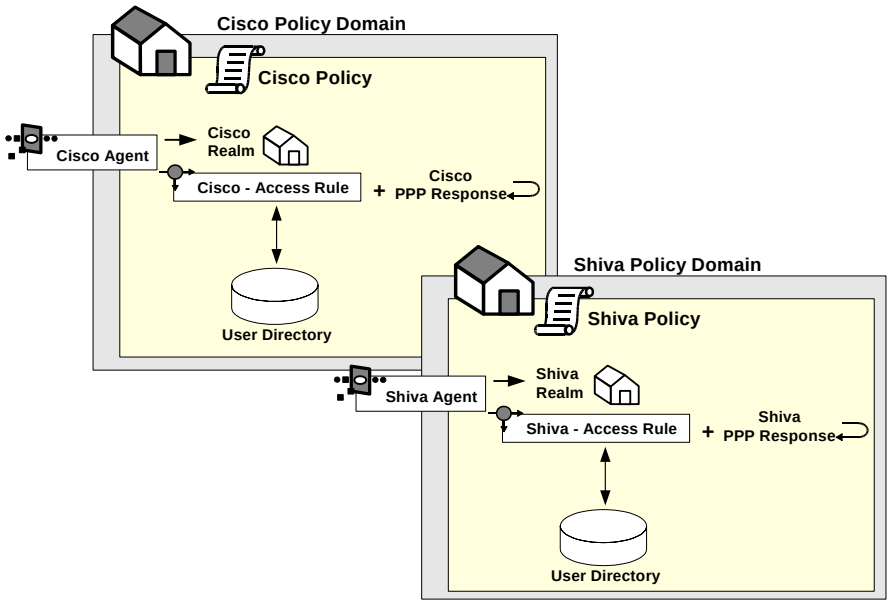
   a. Define two realms--one realm for the Cisco RAS and one realm for the Checkpoint firewall. Each realm binds a RADIUS Agent with a RADIUS authentication scheme.

   b. Define two rules that allow authenticated users to access the appropriate realm. Each rule binds a realm with an allow or deny access event.

   c. Define two responses that provide the user profile to the NAS device and configure the characteristics of the session using response attributes. A separate response must be defined for each NAS device because each device uses a different Dictionary file.

   d. Create one policy that binds the Cisco rule with the Cisco response and the Checkpoint rule with the Checkpoint response. This policy also binds the components of the policy domain (the rule and response groupings) with the RADIUS user directory.

A diagram of this policy domain is shown in the following graphic:



Define Agents for a Heterogeneous, Single Directory Environment

For this environment, you must configure two RADIUS Agents:

- One Agent must be associated with the Cisco RAS.
- One must be associated with the Checkpoint Firewall.
- Both RADIUS Agents must use 1 as the realm hint, which enables each Agent to identify the correct domain to protect.

Configure the User Directory

The Policy Server can authenticate users using the same user directory for both NAS devices.

More information:

Set Up the User Directory (see page 250)

Create the Policy Domain

The policy domain must identify the user directory that contains the names of the RADIUS users, the names of the Administrators who can modify the domain, and the realm that the RADIUS Agent is protecting. A RADIUS environment that uses only one user directory requires only one policy domain.

Note: For more information about setting up a policy domain, see the *Policy Design* guide.

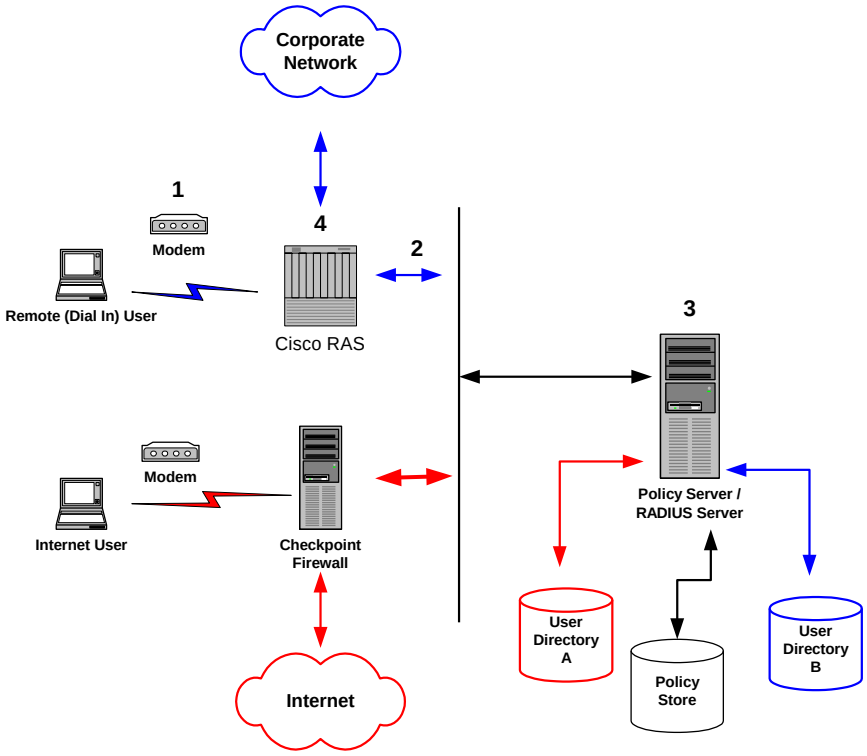
How to Authenticate Users in Heterogeneous RADIUS Environments with Two User Directories

The Policy Server can also be configured to authenticate users for multiple NAS devices when the user information for each device is located in separate user directories. The NAS devices can be of different vendor types.

There are several advantages to this configuration:

- Using two user directories in a single policy domain enables you to delegate the administration of each directory to a different person.
- By configuring the Policy Server to authenticate users for multiple RADIUS clients, you save time. You do not need to install and configure a separate authentication server for each RADIUS client.
- Using existing user directories is more efficient. You do not need to merge the user information into a single directory.

An example of a heterogeneous configuration that uses two user directories is illustrated in the following graphic:



Unlike the topology described in the previous section, this Policy Server uses *two* user directories to authenticate the users. User information for the Cisco RAS users is stored in User Directory A. User information for the Checkpoint firewall is stored in User Directory B. The Policy Server can authenticate users using both of these directories.

By dividing the configuration into two policy domains, the need for realm hints is eliminated. Each RADIUS Agent exists in a separate policy domain and is bound to only one realm.

The process of authentication when two user directories are used is as follows:

1. The remote user dials in from a modem and the Cisco RAS determines that it must use a RADIUS user profile to authenticate the user.
2. The RAS sends the user connection request to the Policy Server.
3. The Policy Server enacts the policy defined for the RAS, and the RADIUS Agent obtains the user's name and password using the authentication scheme configured for the Agent.

4. The Policy Server evaluates the user information against the user directory and policy store associated with the policy's domain.
5. The Policy Server sends an authentication response to the Cisco RAS and one of the following takes place:
   - If authentication is unsuccessful, the RAS refuses the connection.
   - If authentication is successful, the RAS receives a list of attributes from the user profile in the RADIUS server's database and establishes network access for the caller.

     The RAS notifies the Policy Server that the session has begun and when the session ends.

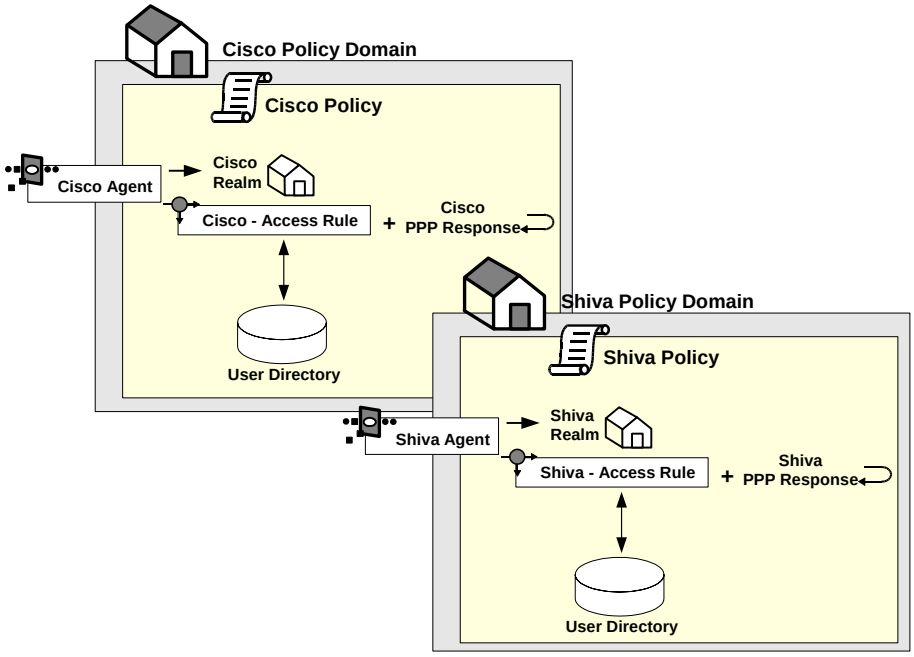
When the Internet user attempts to dial into the Internet Service Provider by using the Checkpoint Firewall, this same process of authentication occurs. However, the Policy Server evaluates the Internet user's authentication information against a different user directory.

How to Configure the System and Policy Domain

To configure the heterogeneous environment described above, which includes two user directories, you must:

1. Configure the system:
   a. Define two RADIUS Agents, as described in Define Agents for a Heterogeneous, Two Directory Environment (see page 262).
   b. Set up the user directories, as described in Set Up User Directories (see page 262).
   c. Create two policy domains, as described in Create Two Policy Domains (see page 263).
2. Configure the policy domain:
   a. Define one realm. The realm binds a RADIUS Agent with a RADIUS authentication scheme.
   b. Define a rule that enables authenticated users to access the realm. Each rule binds a realm with an allow or deny access event.
   c. Define a response that provides the user profile to the NAS device and optionally, configures the characteristics of the session using response attributes.
   d. Create a policy that binds the rule with the response. This policy also binds the rule and response with the RADIUS user directory.

A diagram of these two policy domains is shown in the following graphic:



Define Agents for a Heterogeneous Two Directory Environment

For this environment, you must configure two RADIUS Agents:

- One Agent must be associated with the Cisco RAS.
- One Agent must be associated with the Checkpoint Firewall.
- Neither RADIUS Agent requires a realm hint.

More information:

Define Agents for a Heterogeneous, Single Directory Environment (see page 258)

Set Up User Directories

Each of the user directories containing RADIUS user information must be configured in the Policy Server. Each directory will be associated with a separate policy domain so that separate administrators can be defined for each policy domain.

More information:

Set Up the User Directory (see page 250)

Create Two Policy Domains

One policy domain must be created for the Cisco RAS and one policy domain must be created for the Checkpoint firewall. When defining the policy domains, associate each domain with the appropriate user directory.

More information:

Set up the Policy Domain (see page 250)

Group RADIUS Agents

The following sections detail how to group RADIUS agents.

RADIUS Agents Group Overview

Creating a RADIUS Agent group enables you to manage multiple RADIUS Agents at once and eliminates the need to create and configure separate realms for each RADIUS Agent. Using one realm saves time because you can define the same session timeouts and the same authentication scheme for all RADIUS Agents simultaneously.

A group of RADIUS Agents could include Agents for different types of NAS devices. For instance, an Agent group could contain Agents for a Shiva LAN Rover RAS, a Checkpoint firewall, and a Cisco RAS. The Agent group containing all of these RADIUS Agents would be associated with a single realm, which defined the authentication scheme and session timeout requirements.

Agent groups are best suited for static environments that do not change often; Agent groups enable you to quickly configure SiteMinder to authenticate users of many NAS devices. If your environment is not static and frequently changes as new NAS devices are added or removed, you should probably avoid using Agent groups. Instead, it is usually easier to add and remove RADIUS Agents if they are not located in groups. If the Agents are separated and not grouped together, you can usually find specific Agents faster, and modify or remove policies more quickly.

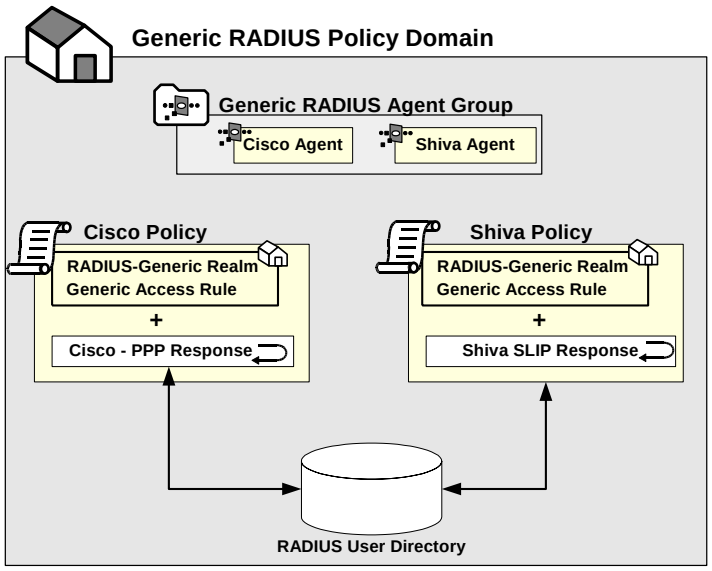
Set up RADIUS Agent Groups

When using RADIUS Agent groups, you typically setup a separate policy for each type of RADIUS Agent. By using separate policies for each type of RADIUS Agent, you can share the common elements of the policy domain, such as the realm and a rule, in each policy. Sharing these common elements saves time.

Unlike the rule and realm, the response in each policy is not shared. Each policy has its own response, which corresponds to the device type of the RADIUS Agent in the policy. The attributes in a response match the attributes provided by the Dictionary file of the NAS device. For example, a response for a Cisco RAS would need to provide attributes that the Cisco RAS could interpret using the Cisco Dictionary file.

Note: All of the NAS devices represented in a RADIUS Agent group must share the same user directory. If they do not share the same user directory, they cannot exist in the same policy domain and therefore, they cannot share the same generic realms or generic rules.

The following example depicts one RADIUS Agent group that contains both an Agent for a Cisco RAS and an Agent for a Shiva RAS. The Agent group is shared by both the Cisco policy and the Shiva policy. Both of these policies share the same generic rule to allow access and the same generic realm, which binds the Agent group to the same authentication scheme. Notice, however, that the responses for each policy are unique.



To setup a RADIUS Agent Group

1. In the System tab of the Policy Server User Interface, right click Agent Groups and select Create Agent Group.

   The SiteMinder Agent Group dialog box appears, as shown in the following graphic.

2. In the Name field, enter a name for the RADIUS Agent group.

3. Optionally, in the Description field, enter a description of the group.

   You may want to use the description to identify the RADIUS Agents contained in the group.

4. In the Agent Type group box, select the RADIUS radio button and select Generic RADIUS from the drop-down list.

5. To add the group members, do the following:

   a. Click Add/Remove.

      The Agent Group Items dialog box appears, as shown below.

   b. In the Available Members box, select a RADIUS Agent and click the left arrow.

   c. Continue adding Agents until the Current Members box contains all of the RADIUS Agents that will comprise the RADIUS Agent group.

   d. Click OK.

6. In the SiteMinder Agent Group dialog box, click OK.

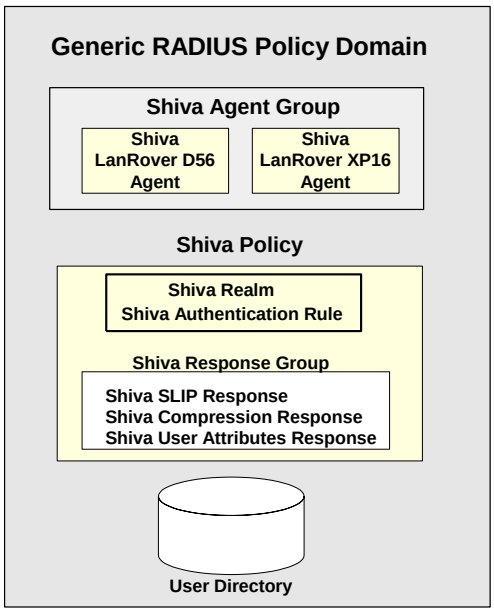
   The RADIUS Agent Group is added to the Agent Group List.

Group RADIUS Responses

A RADIUS response group is a collection of responses defined for the same type of Agent, such as Generic RADIUS. When a rule fires, all of the RADIUS responses paired with it in the response group are triggered.

The responses must be of the same Agent type in order to use the same Dictionary file. For example, you could combine two Cisco responses in the same group or two Generic RADIUS responses in the same group. However, you could not group a Generic RADIUS and a Cisco response in the same group.

The advantage of using RADIUS response groups is that it enables you to configure a policy domain using fewer policies. Instead of creating a separate realm and a separate policy for each RADIUS Agent, you could group RADIUS Agents of the same type, create one generic rule for authentication, and then group the responses for the rule. This type of configuration is shown in the following diagram:



Response groups also make it easier to add RADIUS devices to the environment. For instance, in an environment such as the one shown in the previous figure, you could quickly add another Shiva RAS to the RADIUS Agent group and this new RAS would automatically be configured with the appropriate rule and responses.

Troubleshoot and Test RADIUS

Once you have configured the Policy Server to act as a RADIUS authentication server, you can test and troubleshoot the policies using the tools described in subsequent topics.

Generate RADIUS Logs for Accounting and Debugging

RADIUS logs track debugging and accounting information generated by the Policy Server. Use the RADIUS log file to track the following:

- State of the Policy Server
- Connection attempts and session creations
- Information about each Policy Server action

Logs are turned on and off using the Policy Server Management Console from the Debug tab.

The Policy Server time stamps the log file with the date and time it was created. For example, "log.txt" can be specified as the name of the file. When the Policy Server is restarted and the Policy Server creates the log file, the date and time are added to the name, for example:

```
log.txt.08Dec1999_13_30_57
```

If you are appending logging information to the same file, the date on the file reflects the date and time it was created. The timestamp is only updated if the Policy Server is restarted.

Read RADIUS Log Files With Smreadclog

This tool is used to read RADIUS log files generated by the Policy Server. It is useful for troubleshooting the Policy Server when used as a RADIUS authentication server. Options are provided to display individual RADIUS attributes that are exchanged between NAS and SiteMinder.

Smreadclog uses the following arguments to supply information required to read RADIUS log files:

-i*<input-file>*

Specifies the filename of the log file.

-o*<output-file>*

Specifies the filename of the output file.

-s*<secret>*

Specifies the shared secret that can be used to decode RADIUS passwords.

-r

Indicates that a hex dump of an entire RADIUS packet be displayed.

-a

Indicates that RADIUS attributes should be displayed individually.

-d

Indicates that RADIUS attributes should be displayed according to their definition in the policy store. This option displays actual attribute names as well as attribute values formatted based on their attribute type. Without this option, only the attribute name and value are displayed (as a hex string).

-p*<radius-server>*

Enables you to record and replay RADIUS activity of the Policy Server service against your RADIUS server.

-m*<authentication port>*

Specifies the port used for RADIUS authentication if that port is not the default port, 1645.

-n*<accounting port>*

Specifies the port used for RADIUS accounting if that port is not the default port, 1646.

To use smreadclog

1. Navigate to one of the following locations:
   - On NT, <*siteminder_installation*>\Bin

     where <*siteminder_installation*> is the installed location of SiteMinder.
   - On UNIX, <*siteminder installation*>/bin

     where <*siteminder_installation*> is the installed location of SiteMinder.
2. Enter the following command:

   ```
   smreadclog -i<input-file> -o<output-file>
   -s<secret> -r -a -d -p<radius-server> -m<portnumber>
   -n<portnumber>
   ```

   For example,

   ```
   smreadclog -iradiuslog.txt -oradiuslog2.txt
   -ssecret -r -a -d -p123.123.12.12
   ```

How to Test using the SiteMinder Test Tool

The SiteMinder Test Tool simulates the behavior of a RADIUS authentication server. Using the Test Tool, you can test policies that authenticate RADIUS users and ensure that the response attributes you configured are returning the appropriate data.

The process of testing RADIUS policies includes the following steps:

1. Create a RADIUS policy.
2. Configure the Policy Server Management Console to use RADIUS, as explained in Configure the Policy Server Management Console (see page 269).
3. Configure the SiteMinder Test Tool to test RADIUS policies, as explained in Test RADIUS Policies (see page 269).

Configure the Policy Server Management Console

To configure the Policy Server Management console

1. Start the Policy Server Management Console.

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

2. Select the Settings tab.
3. On the Settings tab, do the following:
   a. In the RADIUS UDP Ports group box, select the Enable check box.
   b. In the Authentication field, enter 1645.
   c. In the Accounting field, enter 1646.
4. On the Status tab, restart the Policy Server to enable the Policy Server configuration changes.

   You are now ready to test the RADIUS policies using the Test Tool.

Test RADIUS Policies

To test RADIUS policies

1. Start the Test Tool.

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

2. In the SiteMinder Agent group box, do the following:
   a. Select the RADIUS radio button.
   b. In the Secret field, enter the shared secret that was defined for the RADIUS agent in the SiteMinder Administration User Interface.
3. In the User Information group box, do the following:
   a. In the User field, enter the name of a user in the RADIUS user directory whose authentication will be tested.
   b. In the Password field, enter the user's password.
   c. Select the CHAP Password check box if you are using a RADIUS CHAP Authentication scheme.
4. In the Command group box, click IsAuthenticated.

The policy is tested and the response attributes appear in the Attributes group box.

Appendix D: Log File Descriptions

This section contains the following topics:

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)

Field Name	Description	Null?	Field Type
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)
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)

Field Name	Description	Null?	Field Type
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 E: Publishing Diagnostic Information

This section contains the following topics:

Diagnostic Information Overview

The Policy Server includes a command line tool for publishing diagnostic information about a 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 SiteMinder utility or executable on Windows Server 2008, open the command line window with Administrator permissions. Open the command line window this way, even if your account has Administrator privileges. For more information, see the release notes for your SiteMinder component.

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

To 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\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 server store

Published object store information includes the type of object store 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 F: Error Messages

This section contains the following topics:

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.

Message	Function	Description
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.
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.

Message	Function	Description
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.
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.

Message	Function	Description
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.
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.

Message	Function	Description
Cannot get AceAlphanumeric	SmLoginLogoutMessage::Get-AceAlphanumericFail	Failed to find method in ACE client library.
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.

Message	Function	Description
Cannot get AceSendNextPasscode	SmLoginLogoutMessage::Ace-SendNextPasscodeFail	Failed to find method in ACE client library.
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.

Message	Function	Description
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.
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 in displayed when this parameter is missing of 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.

Message	Function	Description
FindApplicablePassword Policies - error fetching Root	SmLoginLogoutMessage::Error-FetchingApplicablePolicyRoot	Failed to fetch Root object while validating Logging attempt.
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::Password DataAttrib-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 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 use 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 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, 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 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 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.

Message	Function	Description
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.
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.

Message	Function	Description
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.
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.

Message	Function	Description
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."
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.

Message	Function	Description
Failed to stat management command channel	SmServerMessage::Stat-MangmCmd ChannelFail	(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-UpdateAg entKeys	The Administrator command that Agents update their keys could not be saved in the Policy Store.
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.

Message	Function	Description
Handshake error: Unknown client name '%1s' in hello message	SmServerMessage::Handshake-ErrorUnknownClient	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::InconsistentAgent-KeyMarker	An Agent Key record in the Policy Store has the given unrecognized key type.
Inconsistent number of agent keys (%1i)	SmServerMes-sage::InconsistentNumberOf-AgentKeys	The Policy Store contains the given incorrect number of keys for an Agent.
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.

Message	Function	Description
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.
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.

Message	Function	Description
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.
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.

Message	Function	Description
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.
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.

Message	Function	Description
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.
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.

Message	Function	Description
Unable to reset logger options dynamically	SmServerMessage::Dynamic-Logger ResetFail	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-Age ntIdentity	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-UnR esolved	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-UpdateFail ed	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.
Unexpected exception while publishing AZ Libs	SmServerMes-sage::UnexpectedExc eption-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-KeyTypeU nknown	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-ExcpP ublishAuthLibs	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.

Message	Function	Description
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 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::AdministratorDirectory-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-RealmOid	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.

Error Message	Function	Description
(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-ObjectClasses) 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-PropertiesDirObjRollbackFail	Unable to reset the properties of the object after new values were rejected. Verify the directory connection defined in the policy store.
Exception in Transact SessionTimeoutThread.	SmJavaApiMessage::Unknown-ExcpTransactSessionTimeout-Thread	An unknown error occurred while trying to process expired sessions.
Exception in Transact SessionTimeoutThread. Msg: %1s	SmJavaApiMessage::Excp-TransactSessionTimeoutThread	An error occurred while trying to process expired sessions.
Failed to create EmsSession Timeout Thread	SmJavaApiMessage::Ems-SessionTimeoutThread-CreateFail	There are not enough system resources to create a new thread.
Failed to resolve all domains	SmJavaApiMessage::Domain-ResolveFail	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-UsersDelegatedRolesFail	Unable to retrieve roles for this user. Make sure the library smobjims.dll (libsmobjims.so) is installed.
getUsersDelegatedRolesInApp failed, error = %1s	SmJavaApiMessage::IMSget-UsersDelegatedRolesInAppFail	Unable to retrieve user roles for the application. Make sure the library smobjims.dll (libsmobjims.so) is installed.
getUsersDelegatedTasks failed, error = %1s	SmJavaApiMessage::IMSget-UsersDelegatedTasksFail	Unable to retrieve tasks for this user. Make sure the library smobjims.dll (libsmobjims.so) is installed.

Error Message	Function	Description
getUsersDelegatedTasksInApp failed, error = %1s	SmJavaApiMessage::IMS-getUsersDelegatedTasksIn-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-getUsersRolesFail	Unable to retrieve roles for this user. Make sure the library smobjims.dll (libsmobjims.so) is installed.
getUsersRolesInApp failed, error = %1s	SmJavaApiMessage::IMS-getUsersRolesInAppFail	Unable to retrieve user roles for the application. Make sure the library smobjims.dll (libsmobjims.so) is installed.
getUsersTasks failed, error = %1s	SmJavaApiMessage::IMS-getUsersTasksFail	Unable to retrieve tasks for this user. Make sure the library smobjims.dll (libsmobjims.so) is installed.
getUsersTasksInApp failed, error = %1s	SmJavaApiMessage::IMS-getUsersTasksInAppFail	Unable to retrieve user tasks for the application. Make sure the library smobjims.dll (libsmobjims.so) is installed.
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.

Error Message	Function	Description
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.
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 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.

Error Message	Function	Description
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.
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 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_-ACTE XPR_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_-GLOB AL_CAEClog	The JVM encountered an internal error establishing the active expression context
SmJavaAPI: Error making global reference to class NativeCallbackError %1p	SmJavaApiMessage::MSG_E_-GLOB AL_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_-GLOB AL_CAUTHClog	The JVM encountered an internal error establishing a authentication context

Error Message	Function	Description
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 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.
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.

Error Message	Function	Description
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
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_-CAUGHT_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-AddMemberGroupDN	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::AuthenticateUserDNLd-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-LoadSecurityIntegrationFileFail	(Obsolete)
(Bind - init) Server: failed to load Security Integration secret	SmLdapMessage::BindInit-LoadSecurityIntegrationSecret-Fail	(Obsolete)
(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.

Error Message	Function	Description
(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. Check LDAP server and port.	Unable to initialize to LDAP server with SSL. Check the LDAP server and port. Make sure your LDAP server is configured for SSL.
(Bind) DN: '%1s'. Status: Error %2i . %3s	SmLdapMessage::BindDN-RequireCredentialsError	Unable to bind to LDAP server. Make sure the credentials are correct. See 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.

Error Message	Function	Description
(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.
(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-PropDNError	Failed to modify a given DN entry in an LDAP user directory. See the included LAP 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.

Error Message	Function	Description
(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.
(SmDsLdap-GetHandle) Error while parsing %1s LDAP URL.	SmLdapMessage::GetHandle-LdapURLParsingError	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.
(SmDsLdap-Referral) Error while parsing %1s LDAP URL.	SmLdapMessage::Ldap-URLParsingError	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-LdapConnMgrUnbind	Error while unbinding from the LDAP server.
CSmDsLdapConnMgr (ldap_unbind_s). Server %1s : %2ul	SmLdapMessage::Unknown-ExceptionLdapConnMgrUnbind	Internal error occurred while unbinding from the LDAP server.
CSmDsLdapProvider::Search(): Wrong syntax of LDAP search filter: %1s	SmLdapMessage::Wrong-SyntaxLdapSearchFilter	Verify if the LDAP search filter has correct syntax.

Error Message	Function	Description
CSmDsLdapProvider::Search-Binary(): Wrong syntax of LDAP search filter: %1s	SmLdapMessage::Wrong-SyntaxLdapSearchBinFilter	Verify if the LDAP search filter has correct syntax.
CSmDsLdapProvider::Search-Count(): Wrong syntax of LDAP search filter: %1s	SmLdapMessage::Wrong-SyntaxLdapSearchCountFilter	Verify if the LDAP search filter has correct syntax.
CSmObjLdapConnMgr Exception (ldap_unbind_s). Server %1s:%2ul	SmLdapMessage::Excp-CSmObjLdapConn-Mgrldap_unbind_s	The 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-DisabledUserState	SmLdapMessage::DirDisabled-FlagNotProper	The user attribute chosen to server as a Disabled Flag attribute in the user directory's setting is ill-suited for this purpose. Please reselect the attribute.
Exception (ldap_controls_free) in CSmDsLDAPConn::Create-LDAPControls	SmLdapMessage::Unknown-ExceptionFreeLDAPControls	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.
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.

Error Message	Function	Description
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.
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.

Error Message	Function	Description
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.
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.

Error Message	Function	Description
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.
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.

Error Message	Function	Description
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 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\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.
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 SiteMinder admin UI to check the sizelimit that SiteMinder will use for this LDAP server. Set this to match the server configuration.

Error Message	Function	Description
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 SiteMinder admin UI to check the sizelimit that 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 SiteMinder admin UI to check the sizelimit that 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 SiteMinder admin UI to check the sizelimit that 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.
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 SiteMinder admin UI to check the sizelimit that SiteMinder will use for this LDAP server. Set this to match the server configuration.

Error Message	Function	Description
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 SiteMinder admin UI to check the sizelimit that 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 SiteMinder admin UI to check the sizelimit that 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 SiteMinder admin UI to check the sizelimit that 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 SiteMinder admin UI to check the sizelimit that SiteMinder will use for this LDAP server. Set this to match the server configuration.
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 SiteMinder admin UI to check the sizelimit that 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 SiteMinder admin UI to check the sizelimit that SiteMinder will use for this LDAP server. Set this to match the server configuration.

Error Message	Function	Description
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 SiteMinder admin UI to check the sizelimit that 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.
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 SiteMinder admin UI to check the sizelimit that 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 SiteMinder admin UI to check the sizelimit that 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-ExceedSearchForRespAttr	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.

Error Message	Function	Description
LDAP admin limit exceeded searching for ResponseGroup entries in policy store	SmLdapMessage::AdminLimit-ExceedSearchForRespGroup	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-ExceedSearchForRootConfig	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-ExceedSearchForRule	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-ExceedSearchForRuleGroup	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.
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.

Error Message	Function	Description
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 SiteMinder admin UI to check the sizelimit that 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.
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.

Error Message	Function	Description
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 SiteMinder admin UI to check the sizelimit that 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.
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 SiteMinder admin UI to check the sizelimit that 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 SiteMinder admin UI to check the sizelimit that 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 SiteMinder admin UI to check the sizelimit that SiteMinder will use for this LDAP server. Set this to match the server configuration.

Error Message	Function	Description
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 SiteMinder admin UI to check the sizelimit that 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 SiteMinder admin UI to check the sizelimit that 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-Exceed SearchForAgentType	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.
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-LimitExceeded_AuthAzMap	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the SiteMinder admin UI to check the sizelimit that 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-LimitExceeded_CertMap	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the SiteMinder admin UI to check the sizelimit that 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-LimitExceeded_Domain	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the SiteMinder admin UI to check the sizelimit that SiteMinder will use for this LDAP server. Set this to match the server configuration.

Error Message	Function	Description
LDAP size limit exceeded searching for KeyManagement entries in policy store	SmLdapMessage::LdapSize-Limit-Exceeded_KeyManagement	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the SiteMinder admin UI to check the sizelimit that 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-LimitExceeded_ODBCQuery	Check the size limit for your specific LDAP server. (see LDAP server manual) Also, run the SiteMinder admin UI to check the sizelimit that SiteMinder will use for this LDAP server. Set this to match the server configuration.
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 SiteMinder admin UI to check the sizelimit that 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 SiteMinder admin UI to check the sizelimit that 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 SiteMinder admin UI to check the sizelimit that 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.

Error Message	Function	Description
LDAP size limit exceeded searching for PropertySection entries in policy store	SmLdapMessage::SizeLimit-Exceed SearchForProperty-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 SiteMinder admin UI to check the sizelimit that SiteMinder will use for this LDAP server. Set this to match the server configuration.
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 SiteMinder admin UI to check the sizelimit that 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.

Error Message	Function	Description
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.
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 SiteMinder admin UI to check the sizelimit that 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.

Error Message	Function	Description
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.
Length of the string supplied is more than the allowed limit.Please see LDAP store documentation for more details .	SmLdapMessage::Ldap-LengthCon strain-Violation_CertMap	The value used in the search was too long.
SmDsLdapConnMgr (ldap_search_ext_s) in PingServer : %1s	SmLdapMessage::ErrorLdap-Conn MgrPingServer	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-MgrBi ndInitFail	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-MgrBi ndSetOptionConnect-Timeout	Unable to set LDAP option. Check the error string for more information.
SmDsLdapConnMgr Bind - SSL init. Server %1s : %2ul	SmLdapMessage::LdapConn-MgrBi ndSSLInitFail	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-Conn MgrBind	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.)

Error Message	Function	Description
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?
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?

Error Message	Function	Description
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?
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.

Error Message	Function	Description
SmObjLdapConnMgr Bind. Server %1s:%2ul. Error %3i - %4s	SmLdapMessage::SmObj-LdapConnMgrBindServerError	The 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.
SmObjLdapConnMgr Exception (ldap_simple_bind_s). Server %1s:%2ul	SmLdapMessage::ExcpSm-ObjLdapConnMgrldap_simple_-bind_s	The 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-ObjLdapConnMgrldap-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-ObjLdapConnMgrldapssl_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::TerminatingServer-Processes	Shutting down server process so important reconfiguration may take place. See previous error in log.

Error Message	Function	Description
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.
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.

Error Message	Function	Description
Unexpected value of 'arg' argument in rebindproc_sm %1i	SmLdapMes-sage::UnexpectedValueArg-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::UnexpectedValueFreeit-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.
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.

Error Message	Function	Description
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.
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.

Error Message	Function	Description
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 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.
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 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 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 SiteMinder Database.
Invalid credentials or server not found attempting to connect to '%1s' server '%2s'.	SmOdbcMessage::Unable-ToConnect	Invalid credentials supplied for accessing a 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.

Error Message	Function	Description
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.

Message	Message ID	Description
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.
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.

Message	Message ID	Description
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.
Failed to find root object!	RootObjFindFail	The policy server failed to find affiliate domains. Check if affiliate objects are visible through the 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.

Message	Message ID	Description
QueryInterface (IID_IADsContainer) failed; Error %1xl. %2s	QueryInterfaceIID_IADs-Container Fail	The policy server failed to enumerate container members through the ADSI interface.
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.

Message	Message ID	Description
Unsupported function called: SmDirGetUserProperties	UnsupportedFuncCallSmDir-GetUserProperties	The SmDirGetUserProperties function is not supported by the affiliate provider library.
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

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W