CA SiteMinder®

Policy Server Release Notes

r12.5

Second Edition

CA Technologies Product References

This document references the following CA Technologies products:

- CA DLP™
- CA IdentityMinder (formerly Identity Manager)
- CA Single Sign–On
- SiteMinder
- CA SiteMinder® Web Services Security (formerly CA SOA Security Manager)

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Contents

Chapter 1: Policy Server Release Notes

This document contains information on Policy Server and the SiteMinder Administrative UI features, operating system support, installation considerations, known issues, and fixes.

Chapter 2: New Features

This section contains the following topics:

Agent Discovery

The Agent Discovery feature discovers instances of different types and versions of CA SiteMinder agents. Once discovered, you can view agent-specific details such as version, state, and so on. You can also view a list of agents deployed on various hosts in your enterprise and delete the unwanted agent instance entries from the list.

Any SiteMinder agent, irrespective of the version, that communicates with the Policy Sever regularly comes under the purview of Agent Discovery.

Note: For more information about Agent Discovery, see the *Policy Server Configuration Guide* and *Web Agent Configuration Guide*.

Authentication Context Support

In access control request processing, the authentication phase processes information about user identity and the authorization mechanism. This information that is taken together is named the authentication context.

In previous releases of SiteMinder, the duration of the authentication context was limited to the authentication phase. In this release, you can optionally store the authentication context as sessions variables in the session store. Administrators can configure responses and policies to use session variables.

Note: For information about authentication context support, see the *Policy Server Configuration Guide*.

Administrative Scoping Using Workspaces

SiteMinder Administrators are assigned rights to one or more security categories that define their administrative authority in the Administrative UI, such as managing authentication schemes.

In previous r12.x releases, you could limit the scope of rights to manage domains or applications to specific domains and applications. Otherwise, an administrator had access to every policy store object related to their other assigned security categories.

This release introduces *Workspace* objects which allow you to define a subset of policy store objects in any of the following categories:

- Administrator
- Agent
- Agent Configuration
- Agent Group
- Agent Type
- Application
- Authentication Scheme
- Domain
- Host Configuration
- Legacy Administrator
- Password Policy
- SQL Query Scheme
- Trusted Host
- User Directory
- Workspace

You assign a workspace to one or more Administrators to filter the objects that are available to them, further scoping their administrative authority. An administrator whose administrative authority is restricted by an assigned workspace is therefore known as a *scoped administrator*.

Note: Scoped Application Admin and Domain Admin security category rights grants defined in earlier releases are honored in this release and shown for existing administrators. New scoped grants are not possible. Existing scoped grants can be deleted but not modified.

CA Directory Session Store Support

CA Directory is supported as a session store.

Note: For more information about configuring CA Directory as a session store, see the *Policy Server Installation Guide.* For more information about supported versions, see the r12.5 SiteMinder Platform Support Matrix.

CA DLP Integration

If you have integrated with CA DLP, you can apply CA DLP content classifications to Enterprise Policy Management (EPM) applications. Content classifications extend applications to include the type of content a user is requesting. The Policy Server can use the results of a CA DLP content analysis to make content–aware authorization decisions.

Note: For more information about integrating with CA DLP, see the *SiteMinder Implementation Guide*. For more information about adding content classifications to an application, see the *Policy Server Configuration Guide*.

Enhanced Directory Mapping Using Identity Mapping

Identity Mappings provide an enhanced method of mapping users from a Source Directory to a Target Directory using custom search criteria. You can use Identity Mapping for both user authorization and user validation.

Identity Mapping enables custom search and also lets you control the order of mapping rules using different identity mapping entry objects.

Note: For more information about Enhanced Directory Mapping, see the *Policy Server Configuration Guide*.

CA Identity Manager Access Roles in Policies

If you have integrated CA Identity Manager and SiteMinder, you can implement policy–based access control using CA Identity Manager roles.

- The Policy Server installation includes the required data definitions for the CA CA Identity Manager integration at the following location.

  siteminder_home\xps\dd

  siteminder_home

  Specifies the Policy Server installation path.

- The name of the file is:

  IdmSmObjects.xdd

Important! Do not import this file in to the policy store until you have completed the CA Identity Manager integration. If you import the data definitions before completing the integration, the Policy Server can reach an indeterminate state. Coordinate the integration with your CA Identity Manager administrator.

Note: For more information about integrating CA Identity Manager and SiteMinder, see the CA Identity Manager documentation. For more information about managing CA Identity Manager roles in policies, see the *Policy Server Configuration Guide.*

OpenID Authentication Scheme

This release introduces support for an OpenID authentication scheme.

The OpenID authentication scheme lets SiteMinder users submit credentials through an OpenID provider. The OpenID provider authenticates the user and sends SiteMinder an authentication response. The Policy Server verifies the authentication response, completes the authentication process, and authorizes access to the resource.

Note: For more information, see the *Policy Server Configuration Guide*.

Policy Server Log Messages Added to the Profiler Log

If Policy Server profiler is enabled, all Policy Server log messages are written to the following:

- The Policy Server log file (smps.log).
- The Policy Server profiler log. The default profiler log is smtracedefault.log.

Note: For more information about Policy Server logging and profiling, see the *Policy Server Administration Guide*.

Protecting the Administrative UI with SiteMinder

This release introduces support for protecting the Administrative UI with SiteMinder. Protecting the Administrative UI with SiteMinder requires that you configure an agent to function with a reverse proxy server and configure an eternal administrator store.

Note: For more information, see the *Policy Server Configuration Guide*.

Hardware Load Balancing for Agent to Policy Server Communication

SiteMinder now supports the use of hardware load balancers configured to expose multiple Policy Servers to SiteMinder Agents through one or more virtual IP addresses. The hardware load balancer then dynamically distributes request load between all Policy Servers associated with that VIP without the need to configure SiteMinder failover or round robin load balancing.

Note: For more information about hardware load balancing support, see the *Policy Server Administration Guide*.

Chapter 3: Changes to Existing Features

Agent to Policy Server Handshakes Added to the Profiler Log

The Policy Server Profiler has been updated to include messages associated with the following:

- Retrieving the current agent shared secret.
- Retrieving the current agent shared secret after a cache flush.
- Retrieving a previous agent shared secret.
- Marking a shared secret as used by a particular agent.

These messages include the agent name, the IP address of the agent host system, and the port the agent is using to connect to the web server.

Advanced Password Services Components

In previous releases:

- You installed the Advanced Password Services (APS) Policy Server–side components with the APS installation kit.
- APS configuration files (APS.cfg and SmPortal.cfg) only supported IPv4 addresses.
- The SmPortal configuration file could only reference servers with IP addresses.

Consider the following items:

- The Policy Server installer is enhanced to include all Policy Server–side components.

  Note: For more information about enabling the Policy Server–side APS components, see the *CA SiteMinder Advanced Password Services Guide*.

- The installer installs all APS server files to the same location as did the APS installer.
- The installer installs the smaps shared library to the following items:
  - (Windows) *siteminder_home*\bin
  - (UNIX) *siteminder_home*/lib

  siteminder_home

  Specifies the Policy Server installation path.

- APS configuration files support IPv4 and IPv6 addresses.

  Note: Some APS user directory attributes store an IP address. APSAdmin allows 15 characters for an IP address entry. If an IPv6 address is longer than 15 characters, it is truncated to fit and prefixed with a "T".

- The SmPortal configuration file can reference servers with fully qualified domain names and IP addresses.
- A Policy Server upgrade retains all LANG (translation), CFG (configuration), and mail files. The default r12.5 versions of the files are installed to *siteminder_home*\samples.

  siteminder_home

  Specifies the Policy Server installation path.

Arcot Integration and Confidence Levels

In previous releases, you could apply a confidence level to authorization decisions in both access management models:

- If you were protecting resources using policies, you could apply a confidence level to an active policy expression.
- If you were protecting resources using EPM applications, you could apply a confidence level to an application role.

Support for confidence levels is now extended to include:

- Policy realms
- Enterprise Policy Management application components

Note: Using an active policy expression or an application role to apply a confidence level remains enabled by default. Using a policy realm or an application component to apply a confidence level must be enabled. For more information about enabling confidence level support, see the *SiteMinder Implementation Guide*. For more information about applying a confidence level to policies and applications, see the *Policy Server Configuration Guide*.

CGI and JSP Password Services Support

CGI and JSP–based password services support is deprecated.

- If you are deploying a new r12.5 environment, SiteMinder supports password services using a forms credential collector (FCC) and customizable FCC forms.

  Note: For more information about configuring agents for FCC–based password services, see the *Web Agent Configuration Guide*. For more information about managing password policies, see the *Policy Server Configuration Guide*.

- If you are upgrading to r12.5 and are managing CGI or JSP–based password services consider the following:
  - All related documentation is available in a Support knowledge base article, *CGI and JSP Password Services*.
  - The web agent upgrade does not remove existing executables, forms, properties files, templates, or any other required password services component.
  - The related samples are no longer installed with the web agent. If necessary, SiteMinder Support can provide all related samples.

EPM Application Role Definition by Selecting Groups, Organizations, and User Attributes

Application roles define the set of users who have access to a resource or group of resources defined in an Application object.

In previous r12.x releases, roles were defined by manually specifying a named or unnamed expression.

In this release, roles can also be defined by selecting groups, organizations, and users with matching user attributes from configured user directories.

Execution Time Added to the Profiler Log

In previous releases, it was not possible to determine the execution time of requests without correlating multiple messages.

This release introduces the execution time (ExecutionTime) data field in the Policy Server profiler.This data field returns the execution time of any selected component to the trace log. The trace log contains the execution time of each function, including the main process request, for the transaction.

Note: For more information about the Policy Server Profiler, see the *Policy Server Administration Guide*.

Federation Security Services UI

In previous r12.x releases, you manage a federated environment using the Federation Security Services UI (FSS Administrative UI). This UI is the applet–based UI installed with the Policy Server and is the only way to configure and manage legacy federation.

The *Federation Security Services Guide* explains how to manage a federated environment using the FSS Administrative UI.

The r12.5 release:

- Ports all legacy federation functionality (formerly Federation Security Services) to the SiteMinder Administrative UI. You manage all legacy federation functionality using the Administrative UI.
- Includes the FSS Administrative UI to facilitate the transition of managing legacy federation using the Administrative UI. Consider the following items:
  - After you upgrade the policy store to r12.5, run the XPS Sweeper utility to manage legacy federation objects originally configured in the FSS Administrative UI. For more information, see the *SiteMinder Upgrade Guide*.
  - This release, including all cumulative releases and service packs, is the last major release that includes the FSS Administrative UI.
  - Support is available for the FSS Administrative UI, but fixes are at the discretion of CA.
- The *Federation Manager Guide: Legacy Federation* explains how to manage a federated environment using the Administrative UI. All references to the FSS Administrative UI are removed from the r12.5 SiteMinder bookshelf. If you want to use the FSS Administrative UI, see the r12.0 SP3 SiteMinder bookshelf.

Important! Do not refer to the r12.0 SP3 documentation for future legacy federation features released in the Administrative UI.

Information Card Authentication Scheme

The ICAS implementation is:

- Extended to support the Federal Identity, Credentialing, and Access Management Identity Metasystem Interoperability 1.0 Profile (ICAM IMI 1.0 Profile) specifications. The specifications are based on the White List of issuers and LOA authorization.
- Enhanced to write the encrypted and decrypted Information Card tokens into the trace files.

Note: For more information, see *Policy Server Configuration Guide* and *Web Agent Configuration Guide*.

Importing Default Policy Store Objects

In previous releases, a SiteMinder data interchange file contained the default policy store objects. You used the smobjimport utility to import:

- The default policy store schema to configure a new policy store. The file was named:

  `smpolicy.smdif`

- An upgrade file to upgrade a policy store.

This release introduces the smpolicy.xml file. This file contains the default policy store objects. You use the XPSImport utility to import this file to configure a new policy store and to upgrade an existing policy store.

Note: For more information about configuring a policy store, see the *Policy Server Installation Guide*. For more information about upgrading a policy store, see the *SiteMinder Upgrade Guide*.

Password Policies and Active Directory Password History

In previous releases, if a user tried to reuse an old password as new, the Policy Server could not interpret the Active Directory error code. As a result, the Policy Server returned a general password failure message. The user was not informed that the old password could not be reused.

Password Services is enhanced to recognize the error code that Active Directory sends when a password cannot be reused. As a result, the Policy Server can return the password reuse message.

Consider the following:

- The DisallowForceLogin registry key must be enabled to return the password reuse message. If the key is not enabled, the Policy Server returns a general password failure message.

  Note: For more information about enabling the key, see the *Policy Server Configuration Guide*.

- You can customize the password reuse message using the FCC properties template (smpwservicesUS–EN.properties). The properties file is located in *web_agent_home*\samples\forms.

  web_agent_home

  Specifies the web agent installation path.

Password Services and User Store Error Handling

In previous releases, Password Services mapped:

- Some error codes that a user store returned for authentication failure to one SiteMinder authentication reason.
- Some error codes that a user store returned for authentication failure to more than one SiteMinder authentication reason.

Basic Password Services error handling is enhanced to distinguish these error codes better and return a distinct authentication reason code.

Important! This enhancement can affect existing customized Password Services implementations.

More information:

Customized Password Change Messages (see page 34)

Removed Agent Requests and the Policy Server Log

In previous releases, the Policy Server could remove agent requests from the processing queue, but did not log the details.

The Policy Server log (smps.log) has been enhanced to include informational messages that detail the following:

- The number of aged agent requests that the Policy Server removed within a specific period:
  - The minimum period is 30 seconds.
  - If the Policy Server takes longer than 30 seconds to remove all requests, the log reports the total time.
- The time at which the Policy removed the requests.

Note: For more information about Policy Server logging, see the *Policy Server Administration Guide*.

Report Server

In previous releases, CA Business Intelligence installed SAP BusinessObjects Enterprise XI 2.1 as a stand–alone component. This stand–alone component is known as the Report Server.

In this release, CA Business Intelligence installs SAP BusinessObjects Enterprise XI 3.1 SP3 as a stand–alone component.

Note: For more information about installing the Report Server, see the *Policy Server Installation Guide*. For more information about upgrading the Report Server, see the *SiteMinder Upgrade Guide*.

Requests and Queuing Time Added to the Profiler Log

In previous releases, you were unable to track web agent requests through the process queue.

The Policy Server profiler has been enhanced to let you track:

- When a web agent request arrives at the Policy Server and is enqueued in the process queue.
- The time the request spent in the queue.
- When the request was dequeued.

The profiler log includes the IP address and port of each request.

Enabling this functionality requires that you add the following to your profiler settings:

- The Server component.
- The execution time (ExecutionTime) data field.

Note: For more information about the Policy Server profiler, see the *Policy Server Administration Guide*.

SiteMinder Key Database

In previous releases, a SiteMinder smkeydatabase stored private key/certificate pairs and standalone certificates. SiteMinder used these keys and certificates for signing, verification, encryption and decryption functions. Each Policy Server in the deployment accessed a local version of the smkeydatabase.

This release replaces the need for multiple, local smkeydatabases with a single certificate data store. By default, the certificate data store is automatically configured and co–located with the policy store. All Policy Servers that share a common view into the same policy store have access to all certificates and keys in the environment.

Note: For more information about managing the certificate data store, see the *Policy Server Configuration Guide* and the *Policy Server Administration Guide*. For more information about migrating a smkeydatabase to the certificate data store, see the *SiteMinder Upgrade Guide*.

SiteMinder Object Export Utility

In previous releases, you used the SiteMinder object export utility (smobjexport) to export policy store data.

This release no longer includes the utility. You use the XPSExport utility to export policy store data. For more information, see the *Policy Server Administration Guide.*

Note: The SiteMinder object import utility (smobjimport) remains available to import existing smdif files into an r12.5 policy store. If you use this utility, the import does not include XPS attributes. These attributes use their default values.

XPS Trace Messages

In previous releases, all XPS log and trace messages were written to the Policy Server log (smps.log).

XPS logging has been enhanced to:

- Write all log messages to the Policy Server log.
- Write all trace messages to the Policy Server profiler log.

  Note: All XPS trace messages are written to the profiler log, regardless of whether the Policy Server profiler is enabled.

Chapter 4: Operating System Support

Before you install the Policy Server, the Administrative UI, and the Report Server, make sure that you are using a supported operating system and third-party software.

More information:

Locate the Platform Support Matrix (see page 83)

Chapter 5: System Requirements

Policy Server Requirements

The following minimum system requirements must be met for the SiteMinder Policy Server to install and run correctly.

Windows

The Windows system to which you are installing the Policy Server must meet the following minimum system requirements:

- **CPU**—x86 or x64.
- **Memory**—2 GB system RAM.
- **Available disk space**:
  - 4 GB free disk space in the install location.
  - 1 GB of free space in the temporary file location of the system.

  Note: These requirements are based on a medium size policy database of approximately 1,000 policies.

Note: For additional non–system requirements, see the *Policy Server Installation Guide*.

UNIX

The UNIX system to which you are installing the Policy Server must meet the following minimum system requirements:

- **CPU**
  - **Solaris**–SPARC.
  - **Red Hat**–x86 or x64.
- **Memory**—2 GB system RAM.
- **Available disk space**:
  - 4 GB free disk space.
  - 1 GB free disk space in /tmp.

  Note: Typically, 10 MB of free disk space in /tmp is required for the daily operation of the Policy Server. The Policy Server creates files and named pipes under /tmp. The path to which these files and pipes are created cannot be changed.

Note: For additional non–system requirements, see the *Policy Server Installation Guide*.

Administrative UI Requirements

The minimum system requirements for the Administrative UI depend on the installation option used to install the Administrative UI.

Note: For more information about the Administrative UI installation options, see the *Policy Server Installation Guide*.

Windows Stand–Alone Installation

If you are installing the Administrative UI using the stand–alone option, the Windows system must meet the following minimum system requirements:

- **CPU**—x86 or x64, 1.2 GHz or better.
- **Memory**—1 GB of system RAM. We recommend 2 GB.
- **Available disk space**—840 MB.
- **Temp directory space**—450 MB.

Note: For additional non–system requirements, see the *Policy Server Installation Guide*.

UNIX Stand–Alone Installation

If you are installing the Administrative UI using the stand–alone option, the UNIX system must meet the following minimum system requirements:

- **CPU**
  - Solaris—UltraSparc, 440 MHz or better.
  - Red Hat Linux—x86 or x64, 700 MHz or better.
- **Memory**—1 GB of system RAM. We recommend 2 GB.
- **Available disk space**—840 MB.
- **Temp directory space**—450 MB.

Note: For additional non–system requirements, see the *Policy Server Installation Guide*.

Windows Existing Application Server Installation

If you are installing the Administrative UI to an existing application server, the Windows system must meet the following minimum system requirements:

- **CPU**—x86 or x64, 1.2 GHz or better.
- **Memory**—1 GB of system RAM. We recommend 2 GB.

  Note: If you are running WebSphere, 2 GB of system RAM is required.
- **Available disk space**—540 MB.

  Note: If you are running WebSphere, 2 GB of available disk space is required.
- **Temp directory space**—2 GB.
- **JDK**—The required JDK version is installed on the system to which you are installing the Administrative UI.

Note: For additional non–system requirements, see the *Policy Server Installation Guide*.

UNIX Existing Application Server Installation

If you are installing the Administrative UI to an existing application server, the UNIX system must meet the following minimum system requirements:

- **CPU**
  - Solaris—UltraSparc, 440 MHz or better.
  - Red Hat Linux—x86 or x64, 700 MHz or better.
- **Memory**—1 GB of system RAM. We recommend 2 GB.

  Note: If you are running WebSphere, 2 GB of system RAM is required.
- **Available disk space**—540 MB.

  Note: If you are running WebSphere, 2 GB of available disk space is required.
- **Temp directory space**—2 GB.
- **JDK**—The required JDK version is installed on the system to which you are installing the Administrative UI.

Note: Additional non–system requirements exist in the *Policy Server Installation Guide*.

Report Server Requirements

The following minimum system requirements must be met for the Report Server to install and run correctly.

Windows

The Windows system to which you are installing the Reports Server must meet the following minimum system requirements:

- **CPU**—Intel® Pentium™ 4–class processor, 2.0 GHz.
- **Memory**—2 GB of RAM.
- **Available disk space**—10 GB.

  Note: This requirement is the space that is required to install the Report Server. This requirement does not account for the disk space that is required to store reports.
- **Temp directory space**—1 GB.

Note: For additional non–system requirements, see the *Policy Server Installation Guide*.

UNIX

The UNIX system to which you are installing the Reports Server must meet the following minimum system requirements:

- **CPU**
  - (Solaris) SPARC v8plusSparc
  - (Red Hat Linux) Intel Pentium 4–class processor, 2.0 GHz.
- **Memory**—2 GB of RAM.
- **Available disk space**—10 GB.

  Note: This requirement is the space that is required to install the Report Server. This requirement does not account for the disk space that is required to store reports.
- **Temp directory space**—1 GB.

Note: For additional non–system requirements, see the *Policy Server Installation Guide*.

Chapter 6: Installation and Upgrade Considerations

Upgrade Information Page

In addition to the *SiteMinder Upgrade Guide*, CA Support Online includes valuable upgrade information. For more information, see the CA r12.5 Upgrade Information page.

Java Virtual Machine Installation Error on Solaris can be Ignored (149886)

Symptom:

You are doing a console mode installation of a SiteMinder product on a Solaris platform. The following error message displays: "Unable to install the Java Virtual Machine included with this installer."

Solution:

Ignore this error message. The error is a third-party issue and it has no functional impact.

Administrative UI and Internet Explorer 9 (149209)

If you are using Internet Explorer (IE) 9 to view the Administrative UI, run the Administrative UI in compatibility mode to submit the forms.

Installation Media Names

The following tables identify the installation executables for the following SiteMinder components:

- Documentation
- Policy Server
- Administrative UI
- Report Server

Note: Information appears by platform. For more information about supported operating systems, see the r12.5 SiteMinder Platform Support Matrix on the Technical Support site.

Documentation

The SiteMinder bookshelf is available on the Support site. The bookshelf does not require an installer. For more information, see Locate the Bookshelf (see page 83).

Policy Server

Platform	Installation Executable
Linux	ca-ps-12.5-*cr*-linux.bin
Solaris	ca-ps-12.5-*cr*-sol.bin
Windows	ca-ps-12.5-*cr*-win32.exe

cr

Specifies the cumulative release number. The base r12.5 release does not include a cumulative release number.

Important! If you are running this wizard on Windows Server 2008, run the executable file with administrator permissions. Use these permissions even if you are logged in to the system as an administrator. For more information, see the release notes for your SiteMinder component.

Administrative UI

Platform	Installation Executable
Linux	■ (Prerequisite) adminui-pre-req-12.5-*cr*-linux.bin ■ (Administrative UI) ca-adminui-12.5-*cr*-linux.bin

Platform	Installation Executable
Solaris	■ (Prerequisite) adminui-pre-req-12.5-*cr*-sol.bin ■ (Administrative UI) ca-adminui-12.5-*cr*-sol.bin
Windows	■ (Prerequisite) adminui-pre-req-12.5-*cr*-win32.exe ■ (Administrative UI) ca-adminui-12.5-*cr*-win32.exe

cr

Specifies the cumulative release number. The base r12.5 release does not include a cumulative release number.

Important! If you are running this wizard on Windows Server 2008, run the executable file with administrator permissions. Use these permissions even if you are logged in to the system as an administrator. For more information, see the release notes for your SiteMinder component.

Report Server

Platform	Installation Executable
Linux	■ (Report Server) cabiinstall.sh ■ (Report Server Configuration Wizard) ca-rs-config-12.5-*cr*-linux.bin
Solaris	■ (Report Server) cabiinstall.sh ■ (Report Server Configuration Wizard) ca-rs-config-12.5-*cr*-sol.bin
Windows	■ (Report Server) cabiinstall.exe ■ (Report Server Configuration Wizard) ca-rs-config-12.5-*cr*-win32.exe

cr

Specifies the cumulative release number. The base r12.5 release does not include a cumulative release number.

Important! If you are running this wizard on Windows Server 2008, run the executable file with administrator permissions. Use these permissions even if you are logged in to the system as an administrator. For more information, see the release notes for your SiteMinder component.

More information:

Locate the Platform Support Matrix (see page 83)

Password Policy Message and Active Directory

If you are upgrading to r12.5, the Password Services forms credential collector can present a password change message that users are not familiar with. If the following criteria are met, Active Directory users receive the password reuse message:

- The DisallowForceLogin registry key is enabled.

  Note: For more information, see the *Policy Server Configuration Guide*.
- An Active Directory user directory is bound to a password policy.
- The SiteMinder password policy is not tracking password history.
- The Active Directory service is tracking password history and reuse.

This message states that a password change failed because an old password cannot be reused as new.

You can customize the password reuse message using the FCC properties template (smpwservicesUS–EN.properties). The template is located in *web_agent_home*\samples\forms.

web_agent_home

Specifies the web agent installation path.

Customized Password Change Messages

If Password Services is customized to send authentication failure messages based on SiteMinder authentication reason codes, we recommend that you verify that your implementation handles all password message values (PasswordMsg) that the SiteMinder SDK defines.

Password Services error handling is enhanced to:

- Better distinguish error codes that a user store returns for an authentication failure.
- Return a distinct SiteMinder authentication reason code.

This enhancement can result in users receiving messages that they are unfamiliar with.

More information:

Password Services and User Store Error Handling (see page 24)

Certificate Revocation List Issuer

If you are upgrading to r12.5 and a CRL is stored in an LDAP directory service, consider the following items:

- SiteMinder no longer requires that the issuer of the CRL is the same CA that issued the corresponding root certificate.
- SiteMinder no longer performs this check. This behavior is consistent with the requirements for a text–based CRL.

Deprecated SiteMinder Key Tool Options

If you are using key tool options in automated scripts, consider that the following options are deprecated:

- createDB

  This option is not being replaced and does not work with the accessLegacyKS argument. If a script uses this option:

  - The option executes to maintain backwards compatibility, but does not create a smkeydatabase.
  - A message states that the option is deprecated.

  Note: If a script also attempts to verify that a smkeydatabase was created successfully, the script fails. A smkeydatabase directory does not exist in an r12.5 Policy Server installation.

- deleteDB

  This option is deprecated. The removeAllCertificateData replaces this option. If a script uses the deleteDB option:

  - The option executes to maintain backwards compatibility. All certificate data in the certificate data store, not a smkeydatabase, is removed.
  - A message states that the option is deprecated.

- changePassword

  This option is not being replaced. If a script uses this option:

  - The option executes to maintain backwards compatibility, but does not change a password.
  - A message states that the option is deprecated.

Upgrading a Policy Store

In previous releases, you used the smobjimport utility to import an upgrade SiteMinder data interchange format (smdif) file. Importing an upgrade file, instead of the smpolicy file (smpolicy.smdif), prevented existing default objects that were modified from being overwritten.

This release no longer requires an upgrade file. You use the XPSInstall utility to import the smpolicy.xml file. When you import this file as part of an upgrade, it does not overwrite existing default objects that were modified.

Note: For more information about upgrading a policy store, see the *SiteMinder Upgrade Guide*.

Considerations for Upgrading r6.x to r12.x

If your Policy Server and policy store are operating in mixed-mode during an upgrade to r12.5, the following error message appears when you start the Policy Server:

```
[8114/21][Fri Oct 15 2010 09:10:26][CA.XPS:LDAP0014][ERROR] Error occurred during
"Modify" for
xpsParameter=CA.XPS::$PolicyStoreID,ou=XPS,ou=policysvr4,ou=siteminder,ou=netegri
ty,dc=PSRoot",text: Object
class violation

[8114/21][Fri Oct 15 2010 09:10:26][CA.XPS:XPSIO024][ERROR] Save Policy Store ID
failed.
```

This message is expected behavior and does not affect the SiteMinder environment.

This message occurs because the r6.x policy store is not upgraded. Part of the upgrade process includes importing the policy store data definitions. The error appears in the SiteMinder Policy Server log because the data definitions are not available in the policy store.

Considerations for Existing LDAP User Directory Connections Over SSL

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

The Policy Server requires that the certificate database files be in the Netscape cert8.db file format. Use the Mozilla Network Security Services (NSS) certutil application installed with the Policy Server to convert existing cert7.db certificate database files to cert8.db format.

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

Important! Before running a SiteMinder utility or executable on Windows Server 2008, open the command-line window with administrator permissions. Open the command-line window this way, even if your account has administrator privileges.

To convert the certificate database file

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

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

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

2. Enter the following command:

   `certutil -L -d certificate_database_directory [–p prefix_name] -X`

   -d *certificate_database_directory*

   Specifies the directory that contains the certificate database files to convert.

   -p *prefix_name*

   (Optional) Specifies any prefix used when creating the existing cert7.db file (for example, my_cert7.db).

   Certutil converts the existing cert7.db file to cert8.db format.

Considerations for Localized Installations

There are a number of limitations and considerations for installations of localized versions of SiteMinder.

Consider the following before installing the SiteMinder Policy Server on a system with a non–English operating system:

- Localized versions of SiteMinder must be installed on a corresponding operating system.

  For example, you must install a Japanese version of the SiteMinder Policy Server on a Japanese operating system. A Japanese version of the Policy Server will not run properly on an English operating system.

Limitations include the following:

- SiteMinder cannot be installed using the silent installation mode in a directory with a name that uses multi-byte characters.
- The Administrative UI cannot be installed in any mode (silent, command line, GUI) in a directory with a name that uses multi–byte characters.
- Windows 2008 lets you set different regional and language settings for individual user accounts. However, the System and other service accounts must be set to use the default Japanese locale or the component you are installing will not initialize.

  To set the locale for the System or other service accounts, see the Microsoft documentation.

ETPKI Library Installation

The Policy Server and Web Agent installations include a CA ETPKI library.

For Windows operating environments, if a CA ETPKI library exists on the machine to which you are installing the Policy Server or Web Agent, the installer upgrades the existing ETPKI library to the version shipped with the component. The CA ETPKI library remains in its current location.

For UNIX operating environments, the installer will install the CA ETPKI library to the *installation_location*/ETPKI directory, even if another CA ETPKI library exists elsewhere on the UNIX file system.

Upgrading a Collocated Policy Server and Web Agent

Valid on Windows

Symptom:

If a Policy Server and Web Agent are installed to the same host system, after you upgrade the Policy Server, the IIS web server fails to start and an error is logged in the Event Viewer.

Solution:

Upgrade the Web Agent. The IIS web server starts after you upgrade the Web Agent.

Modify a Customized JVMOptions File

During a Policy Server upgrade, the existing JVMOptions.txt file is renamed to JVMOptions.txt.backup. A new JVMOptions.txt file is created.

If the original file included customized parameters, be sure to modify the newly created file to include these customized parameters.

For any Apache-based agents, add the SiteMinder/resources directory to the CLASSPATH in the JVMOptions.txt file, as shown in the following example:

```
-Djava.class.path=C:/Program Files (x86)/CA/siteminder/resources;
```

Connection Between PS on UNIX and SQL Server

When attempting to connect a SiteMinder Policy Server on Red Hat or Solaris to a Microsoft SQL Server 2008 database, you should correctly define the paths to the TraceFile, TraceDll and InstallDir parameters specified in the [ODBC] section of the system_odbc.ini file. Failure to do so may result in connectivity errors.

Character Restriction for Passwords in Installations (72360)

When installing the Policy Server, the CA Report Server, and the Administrative UI, you are asked to specify passwords for various components. Consider the following:

Policy Server

When entering password information, do not use the following characters as they are reserved or restricted:

- (Windows only) A percent sign (%)
- (Reserved by InstallAnywhere) A dollar sign ($)
- (UNIX only) An apostrophe (’)
- (UNIX only) Quotation marks (“”)

CA Report Server

When entering password information, do not use the following characters as they are reserved or restricted:

- (Reserved by InstallAnywhere) A dollar sign ($)
- (UNIX only) An apostrophe (’)
- (UNIX only) Quotation marks (“”)

Administrative UI

When entering password information, do not use the following characters as they are reserved or restricted:

- (UNIX only) An apostrophe (’)
- (UNIX only Quotation marks (“”)

Distributed CA Directory Server Policy Store

If you are using multiple DSAs to function as a policy store, ensure that host information of the router DSA is listed first in the Policy Server Management Console. If you do not list the router DSA host information first, an error occurs when you attempt to install the policy store data definitions.

Note: For more information on configuring CA Directory Server as a policy store, refer to the *Policy Server Installation Guide*.

Importing Event Handler Libraries

Consider the following before upgrading a Policy Sever to r12.5:

- If the Policy Server Management Console Advanced tab does not contain event handler libraries, the XPSAudit event handler library (XPSAudit.dll) is added to the Event Handlers field. No further action is required.
- If the Policy Server Management Console Advanced tab does contain event handler libraries, complete the following after upgrading the Policy Server:

1. Open the Policy Server Management Console and click the Advanced Tab.
2. In the Event Handlers field, replace the path to the current event handler library with the path to the XPSAudit event handler library.

   Note: The default location of the XPSAudit event handler library is *policy_server_home*\bin.

   policy_server_home

   Specifies the Policy Server installation path.

3. Click Apply.

   The path to the event handler library is saved. The Event Handlers field appears disabled.

   Note: By default, the only event handler library that appears in the Advanced tab is XPSAudit.dll.

4. Use the XPSConfig utility to set additional event handler libraries, previously used or otherwise, to the XPSAudit list.

   Note: More information on using the XPSConfig utility to set event handler libraries exists in the *Policy Server Administration Guide*.

Upgrading a Japanese Policy Server

The r12.5 version of the Policy Server is not localized for the Japanese language. Upgrading the Policy Server to r12.5 results in a version that is not localized.

MDAC Versions

It is required that the MDAC versions installed on the client and server sides are compatible.

Note: More information exists in the Microsoft MDAC documentation.

Multi-Mastered LDAP Policy Stores

LDAP directories using multi-master technology may be used as SiteMinder policy stores. The following configuration is recommended when configuring an LDAP policy store in multi-master mode:

- A single master should be used for all administration.
- A single master should be used for key storage.

  This master does not need to be the same as the master used for Administration. However, we recommend that you use the same master store for both keys and administration. In this configuration, all key store nodes should point to the master rather than a replica.

  Note: If you use a master for key storage other than the master for administration, then all key stores must use the same key store value. No key store should be configured to function as both a policy store and a key store.

- All other policy store masters should be set for failover mode.

Due to possible synchronization issues, other configurations may cause inconsistent results, such as policy store corruption or Agent keys that are out of sync.

Contact SiteMinder Support for assistance with other configurations.

Multi–Mastered LDAP User Store Support Limitations (53677)

The multi–mastered LDAP enhancement has the following limitations:

- The Policy Server only supports multi–mastered user stores in a backup capacity. Because Password Services makes frequent writes to the user store, you cannot simultaneously update user information in multiple master instances. In addition, the LDAP implementation could produce out–of–date information or data loss due to delayed replication.
- Multi–mastered support does not extend to custom code such as custom authentication schemes.

Compatibility with Other Products

To ensure interoperability if you use multiple products, such as CA Identity Manager and CA SiteMinder® Web Services Security check the Platform Support Matrices for the required releases of each product. The platform matrices exist on the Technical Support site.

Updated snmptrap File

This release includes an updated snmptrap.conf file. Before installation, back up and save the original snmptrap.conf file, located in *siteminder_installation*\config.

Windows Considerations

The following considerations apply to supported Windows operating environments:

DEP Error during Policy Server Installation

Symptom:

A Data Execution Prevention (DEP) error can prevent the Policy Server from installing on Windows 2008 SP2.

Solution:

1. Configure DEP for essential Windows programs and services only.
2. Run the Policy Server installer.

To configure DEP for essential programs and services

1. Right–click My Computer and select Properties.

   The System Properties dialog appears.
2. Click Advanced.

   The Advanced tab opens.
3. Under Performance, click Settings.

   The Performance Options dialog appears.
4. Click Data Execution Prevention and select Turn on DEP for essential Windows programs and services only.
5. Click OK.

   A message prompts you to restart the system.

Note: After you have successfully installed the Policy Server, you can revert the DEP settings for all programs and services.

Windows Server 2008 System Considerations

For Windows Server 2008, the User Account Control feature helps prevent unauthorized changes to your system. When the User Account Control feature is enabled on the Windows Server 2008 operating environment, prerequisite steps are required before doing any of the following tasks with a SiteMinder component:

- Installation
- Configuration
- Administration
- Upgrade

Note: For more information about which SiteMinder components support Windows Server 2008, see the SiteMinder Platform Support matrix.

To run SiteMinder installation or configuration wizards on a Windows Server 2008 system

1. Right–click the executable and select Run as administrator.

   The User Account Control dialog appears and prompts you for permission.

2. Click Allow.

   The wizard starts.

To access the SiteMinder Policy Server Management Console on a Windows Server 2008 system

1. Right–click the shortcut and select Run as administrator.

   The User Account Control dialog appears and prompts you for permission.

2. Click Allow.

   The Policy Server Management Console opens.

To run SiteMinder command–line tools or utilities on a Windows Server 2008 system

1. Open your Control Panel.
2. Verify that your task bar and Start Menu Properties are set to Start menu and *not* Classic Start menu.
3. Click Start and type the following in the Start Search field:

   ```
   Cmd
   ```

4. Press Ctrl+Shift+Enter.

   The User Account Control dialog appears and prompts you for permission.

5. Click Continue.

   A command window with elevated privileges appears. The title bar text begins with Administrator:

6. Run the SiteMinder command.

More information:

Contact CA Technologies (see page 3)

Deploying SiteMinder Components

If you are deploying SiteMinder components on Windows 2008 SP2, we recommend installing and managing the components with the same user account. For example, if you use a domain account to install a component, use the same domain account to manage it. Failure to use the same user account to install and manage a SiteMinder component can result in unexpected behavior.

Solaris Considerations

The following considerations apply to Solaris.

Solaris 10 Support

The Policy Server and Web Agent are certified for global and non-global zones.

Note: More information on Solaris 10 support exists in the *Policy Server Installation Guide*.

Errors in the SMPS Log due to a gethostbyname() Error (54190)

Network connectivity errors appear in the smps log when gethostbyname() is called. These errors appear even though the directories are available on the network. This was a Solaris issue, which according to Sun bug ID 4353836, has been resolved.

Sun lists the following patches for Solaris 9:

Solaris 9

- 112874-16 (libc)
- 113319-12 (libnsl)
- 112970-05 (libresolv)
- 115545-01 (nss_files)
- 115542-01 (nss_user)
- 115544-01 (nss_compat)

Upgrading a Solaris Policy Server (57935)

Symptom:

If your license file is older than January 2005, the Policy Server may experience problems reading the license file after an upgrade. You may receive a message stating that a valid end-user license cannot be found.

Solution:

Contact Technical Support, and request a new license file.

Report Server Required Patch Clusters

The *Policy Server Installation Guide* contains the system requirements required to install the Report Server. SAP BusinessObjects Enterprise provides additional patch specifications. Before installing the Report Server:

1. Go to *temporary_location*/docs.

   temporary_location

   Specifies the location to which you copied the installation media.

2. Open *SAP BusinessObjects Enterprise XI 3.1 SP3 for Solaris – Supported Platforms* (supported platforms SP3 - Solaris.pdf).

3. Review the Solaris 9 or 10 patch requirements.

Use this resource for Solaris 9 and 10 patch requirements only. This document also provides supported operating system and hardware requirements that SiteMinder does not support. For supported operating systems, see the SiteMinder r12.5 Platform Support Matrix. For system requirements, see the *Policy Server Installation Guide*.

Red Hat Enterprise Linux AS and ES Considerations

The following considerations apply to Red Hat Enterprise Linux AS and ES.

Red Hat Enterprise Linux AS Requires Korn Shell (28782)

A Policy Server installed on Red Hat AS requires the Korn shell. If you do not install a Korn shell on Red Hat AS, you cannot execute the commands that control the Policy Server from a command line, such as start-all and stop-all.

Excluded Features on Red Hat Enterprise Linux AS

The following features are not supported by the Policy Server on Red Hat AS:

- Safeword authentication scheme
- SiteMinder Test Tool

Apache 2.0 Web Server and ServletExec 5.0 on Red Hat Enterprise Linux AS (28447, 29518)

To use Apache 2.0 Web Server and ServletExec 5.0 on Red Hat AS

1. Run the ServletExec 5.0 AS installer against Apache 1.3.x.

   The ServletExec AS Java instance is created.

2. Run ServletExec and Apache 1.3.x, and make sure you can run /servlet/TestServlet.

3. Shutdown Apache 1.3.x, but leave ServletExec running.

4. Using anonymous FTP, access ftp://ftp.newatlanta.com/public/servletexec/4_2/patches and download the latest zip.

5. Extract the following from the zip:

   `mod_servletexec2.c`

6. Edit the httpd.conf file of your HP-Apache 2.x so that it contains the necessary ServletExec-specific directives.

   Note: The directives are also present in the httpd.conf file of your Apache 1.3.x if you allowed the ServletExec installer to update the httpd.conf during installation. For more information on editing the httpd.conf file, refer to the New Atlanta Communication ServletExec documentation.

7. Start Apache 2.x.

8. Test the Web Server with ServletExec by accessing:

   `/servlet/TestServlet`

Report Server Required Patch Clusters

The *Policy Server Installation Guide* contains the system requirements required to install the Report Server. SAP BusinessObjects Enterprise provides additional patch specifications. Before installing the Report Server:

1. Go to *temporary_location*/docs.

   temporary_location

   Specifies the location to which you copied the installation media.

2. Open *SAP BusinessObjects Enterprise XI 3.1 SP3 for Linux – Supported Platforms* (supported platforms SP3 - Linux.pdf).

3. Review the Red Hat 5 patch requirements.

Use this resource for Red Hat 5 requirements only. This document also provides supported operating system and hardware requirements that SiteMinder does not support. For supported operating systems, see the SiteMinder r12.5 Platform Support Matrix. For system requirements, see the *Policy Server Installation Guide*.

Chapter 7: General Considerations

Application Objects Appear in the Policy Server User Interface

If you are using Enterprise Policy Management in a 6.0 SP5 environment, application-related objects you create using the Administrative UI also appear in the Java applet-based Policy Server User Interface. Do not modify these objects from the Policy Server User Interface. You should only modify application-related objects using the Administrative UI.

IdentityMinder Object Support in Policy Stores (29351)

Policy Servers that have not been enabled for IdentityMinder cannot be connected to policy stores that contain IdentityMinder objects. Policy Servers that have been enabled for IdentityMinder 5.6 SP2 can be connected to r12.5 policy stores that contain IdentityMinder objects.

Note: For more information about configuring and deploying IdentityMinder, see the *IdentityMinder Web Edition Installation Guide*.

NTLM Authentication Scheme Replaced by Windows Authentication Scheme

This release does not include an NTLM authentication scheme template. This authentication scheme type has been replaced by the Windows Authentication template. Support for NTLM authentication is now provided through the new authentication scheme template.

Performance Issues Using SQL Query Schemes on Non-Unicode Databases (144327)

Symptom:

Performance is impacted when using a SQL query scheme to find user data in a non-Unicode database. The performance degradation is because default Policy Server behavior is to append an "N" to the SQL query to enable Unicode searching.

Solution:

This is no longer an issue. To prevent performance degradation when using an SQL query scheme to find user data in a non-Unicode database, use the following procedure to disable Unicode searching:

1. Create the following registry setting:

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

2. Set the value of the setting to 1.

   Unicode searching is disabled.

STAR Issue: 20517732-01

Unsupported Features

SiteMinder does not support the following features:

- An external administrator user store with an Administrative UI configured with WebSphere
- SafeWord authentication scheme on Red Hat AS
- SiteMinder Test Tool on Red Hat AS
- Password services with Microsoft Active Directory Global Catalog
- Password services with the Microsoft Active Directory 2008 fine grained password policy feature
- Enhanced LDAP referrals with Novell eDirectory
- SiteMinder only supports enhanced LDAP referrals with Siemens DirX for searches and writes:
  - Password services write referrals is supported.
  - Enhanced referrals for binds and, thus authentication, is not supported.

System Management Limitations

The following system management limitations exist:

Pop-up Blockers May Interfere with Help

Certain pop-up blockers or Web browsers may prevent the Administrative UI help window from opening. Many pop-up blockers allow the pop-up if you press CTRL while you click the link. You can also set your Web browser to allow pop-ups from the Administrative UI.

Registry Setting No Longer Required for Setting the Maximum Number of Connections (27442)

In previous versions of the Policy Server, two ODBC connections were created for each Policy Server service. The following registry setting overrode the default value and indicated the maximum total number of ODBC connections created by the Policy Server for all services:

```
Netegrity\SiteMinder\CurrentVersion\Database\UserDirectoryConnections
```

For r12.5 Policy Servers, the maximum number of connections is determined dynamically, based on five times the maximum number of threads specified in the Policy Server Management Console. (See the Performance group box of the Settings tab in the Management Console.)

If you are upgrading to the r12.5 Policy Server from a 5.x Policy Server, remove the UserDirectoryConnections registry setting. If you do not, and the value specified by the setting is less than the maximum number of threads calculated by the Policy Server, your Policy Server logs will contain many error messages. These messages will indicate that the value of the registry setting overrides the maximum number of connections calculated by the Policy Server.

Policy Server Limitations

The following Policy Server limitations exist:

Leading Spaces in User Password May Not Be Accepted (27619)

A user whose password includes leading spaces may not be able to authenticate under the following combination of circumstances:

- The Policy Server is running on Solaris.
- The password with leading spaces is stored in an LDAP User Store.

Note: A password policy may or may not be enabled.

Error Changing Long Password When Password Services is Enabled (26942)

If the Policy Server has Password Services enabled, changing the password may fail if the old password length exceeds 160 UTF8 octets and the new password length exceed 160 UTF8 octets.

Certificate Mappings Issue with certain Policy Stores (27027, 30824, 29487)

Certificate mappings do not work when the IssuerDN field is longer than 57 characters for policy stores that are installed on the following directories:

- Novell eDirectory
- Active Directory

Handshake Errors with Shared Secret Rollover Enabled (27406)

In the Policy Server error log, you may see an occasional handshake error related to the shared secret, followed by a successful connection. This may occur if the shared secret rollover feature was enabled for the Web Agent communicating with the Policy Server. This behavior is expected as part of a normal shared secret rollover. You can ignore these errors.

Internal Server Error When Using SecureID Forms Authentication Scheme (39664)

When using the SecureID forms authentication scheme, if users do not enter their passwords correctly during their initial login, they are not granted access to resources despite providing correct credentials in subsequent tries. The Policy Server presents users with an internal server error and these users must restart the Web browser to continue.

X.509 Client Certificate or Form Authentication Scheme Issue (39669)

The Policy Server's X.509 Client Certificate or Form authentication scheme is not working properly when using an alternate FCC location.

Certain User Name Characters Cause Authenticating or Authorizing Problems (39832)

When the Policy Server is using an LDAP user store, users with characters such as &, * , \, and \\ in their user names are not getting authenticated and authorized properly. For example, the Policy Server does not authenticate or authorize these sample users:

- use&r1
- use*r2
- use\r3
- use\\r4

DEBUG Logging With SafeWord Authentication Causes Policy Server to Fail (42222, 43051)

On Solaris, when resources are protected by SafeWord authentication schemes, if you enable DEBUG or ALL logging in the SmSWEC.cfg SafeWord configuration file, the Policy Server fails. As a result, do not enable DEBUG or ALL logging for SafeWord authentication schemes. The SafeWord server is PremierAccess server, using protocol 200 or 201.

Active Directory Integration Enhancement For LDAP Namespace (43264, 42601)

This limitation is related to this new AD feature from 6.0 SP 2:

"Enhanced User Account Management and Password Services Integration with Active Directory (SM5504) (28460) (23347) (24047) (25816)"

When following the instructions in section "Enabling Active Directory Integration Enhancement", be aware that this feature is only supported for the LDAP and not the AD namespace.

Policy Server Does Not Support Roll Over of Radius Log (44398) (43729) (42348)

The Policy Server does not have the capability to roll over the radius log. Prior to the 6.0 release, you could roll over the radius log by running the smservauth -startlog command.

smnssetup Tool Deprecated (44964) (45908) (46489)

The smnssetup tool was removed from distribution in 6.0 SP 4. You should use the Policy Server Configuration Wizard (ca-ps-config) to configure:

- OneView Monitor GUI
- SNMP support
- Policy stores

The wizard gives you the option of using either a GUI or a console window. For more information, see the *Policy Server Installation Guide*.

Option to Create Copies of Existing Policy Server Objects

When creating Policy Server objects in the Administrative UI, you have the option of creating a copy of an existing object of the same type. The copy option is not available for the following objects:

- Agent Type
- AuthAz Directory Mapping
- AuthValidate Directory Mapping
- Certificate Mapping
- User Directory
- Application
- Application Resource
- Domain
- Policy
- Realm
- Response
- Response Attribute
- Rule
- Global Policy
- Global Response
- Global Rule
- Password Policy
- Administrator

User Directory Limitations

The following user directory limitation exists:

ODBC User Store Failover

Given

A Policy Server is configured on Solaris to use two Oracle-based user stores: one is the primary user store and the other is the secondary user store.

Result

The time for the Policy Server to failover from the primary to the secondary, in the event of a network failure, may be as long as 8 minutes.

Solution

This time can be reduced by setting the TCP/IP setting, tcp_ip_abort_interval, to the desired time.

Perl Scripting Interface Limitations

The following Perl scripting interface limitations exist:

Perl use Statement for PolicyMgtAPI Must Come Before Use Statement for AgentAPI (24755)

On Solaris, a core dump results if you call use for AgentAPI before you call use for PolicyMgtAPI. If you are calling use for both modules, do so in the following order:

- use Netegrity::PolicyMgtAPI;
- use Netegrity::AgentAPI;

Methods that Return Arrays May Return undef in a One-Element Array (28499)

With methods that return an array, undef should be returned if an error occurs or there is nothing to return. However, these methods may incorrectly return a one-element array with the first element set to undef.

Perl Scripting Interface and Multi-valued Agent Configuration Parameters (37850)

The Perl Scripting Interface does not support setting multi-valued Agent configuration parameters.

Japanese Policy Server Limitations

The following Japanese Policy Server limitation exists:

Agent Shared Secrets are Limited to 175 Characters (30967, 28882)

A Shared Secret for a SiteMinder Agent in a Japanese operating system environment may have no more than 175 characters.

Chapter 8: Known Issues

Known Issues in 12.51

The following are known issues in r12.5:

Importing Policy Store Data that is in Clear–Text (161395)

Symptom:

If a file contains sensitive data in clear–text, the SiteMinder object import utility lets you import it without using a required argument. The following option is required when importing data in clear–text:
-c

Importing the data without the required argument can result in a corrupted policy store.

Solution:

The *Policy Server Administration Guide* includes a warning about using the required option when importing a file that contains sensitive data in clear–text.

Report Without Data (145002)

Symptom:

My report has no data. I did not see an error message.

Solution:

This problem occurs if the end time for the report occurs *earlier* the start time for the report. Verify that the end time occurs later than the start time and run the report again.

First Tab in Group Appears in Administrative UI When Switching from View to Modify (146508)

Symptom:

I was viewing an object in the Administrative UI, but after I clicked Modify, the first tab appeared instead of the tab I was viewing.

Solution:

The first tab in a group appears after clicking Modify. This behavior is expected.

OCSPUpdater Does Not Support the SHA-224 Algorithm (150477,150474)

The OCSPUpdater used for federation certificate validity checking cannot sign OCSP requests using the SHA-224 algorithm. The updater can only sign with the SHA-256, SHA-384, and SHA-512 algorithms.

smpolicysrv_snmp.log Not Generated (147959)

If SNMP is configured for auditing and the Policy Server fails to start–up, SiteMinder generates the SmStartupEvents.audit file. However, no SNMP events are generated. SiteMinder records the start–up events in the reference log file.

Report Server Configuration (150327,119313)

With SiteMinder r12.5, you cannot configure the report server on a non–default port. The report server requires port 6400.

Browser Refresh and Back Buttons Cause Resubmission of Data (149633)

Symptom:

When you select the browser refresh or back button, the dialog where you have entered values gets resubmitted. The repeat operation puts the object that you are configuring into an invalid state.

Solution:

Avoid using the refresh and back buttons on the browser when using the Administrative UI.

Agent Discovery and IIS Web Agents (134318)

If a web agent is installed on a Microsoft IIS web server, the agent discovery feature does not identify the agent for the first–time until the agent intercepts a user request and passes it to the Policy Server.

Subsequent updates to the timestamp of the agent instance are dependent on how IIS is configured. If IIS is configured to shut down idle worker processes, the timestamp is not updated until the web server receives a subsequent request.

This is normal expected behavior. The behavior is a result of how the IIS web server functions.

Uninstalling the Report Server Leaves Files and Registry Entries

Valid on Windows

Symptom:

When I uninstall SAP BusinessObjects Enterprise, some files and registry entries remain.

Solution:

These items are left behind deliberately. These items are required if a user wants the information available for a new installation.

To remove the files and registry entries on Windows 32–bit platforms

1. After uninstalling SAP BusinessObjects Enterprise, delete all files in the installation directory.

   Note: The default installation directory is C:\Program Files\CA\SC\CommonReporting3.

2. Delete the following registry entries:

   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Shared\CommonReporting3
   HKEY_CURRENT_USER\Software\Business Objects
   HKEY_USERS\.DEFAULT\Software\Business Objects
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BOE120*SIASIANODENAME*
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BOE120MySQL
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\BOE120Tomcat
   HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun 2.0\BOE120SIA<SIANODENAME>HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun 2.0\BOE120Tomcat
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\Folders*INSTALLDIR*

   The leftover files and registry entries are removed.

To remove the files and registry entries on Windows 64–bit platforms

1. After uninstalling SAP BusinessObjects Enterprise, delete the following directory:

   installation_directory\CommonReporting3.

   Note: The default installation directory is C:\Program Files(x86)\CA\SC\CommonReporting3.

2. Delete the following registry entry:

   `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432NODE\Business Objects`

   The leftover files and registry entries are removed.

Cache Time Limit while Creating a Response Attribute

While creating a response attribute in a response group, you can configure a time for which the cache is valid. Although the Administrative UI lets you enter any value, the maximum time allowed is 3600 seconds.

Active Directory Synchronization (115248)

When integrating Microsoft Active Directory with SiteMinder, Active Directory user stores that are clustered or configured for round robin load balancing may not synchronize correctly between each use. As a result, some fields may not behave as expected. The unexpected behavior is associated with known Active Directory synchronization limitations.

Contact Microsoft to resolve problems associated with replication and synchronization.

STAR issue: 19249325–01

Windows Server 2008 System Considerations

For Windows Server 2008, the User Account Control feature helps prevent unauthorized changes to your system. When the User Account Control feature is enabled on the Windows Server 2008 operating environment, prerequisite steps are required before doing any of the following tasks with a SiteMinder component:

- Installation
- Configuration
- Administration
- Upgrade

Note: For more information about which SiteMinder components support Windows Server 2008, see the SiteMinder Platform Support matrix.

To run SiteMinder installation or configuration wizards on a Windows Server 2008 system

1. Right–click the executable and select Run as administrator.

   The User Account Control dialog appears and prompts you for permission.

2. Click Allow.

   The wizard starts.

To access the SiteMinder Policy Server Management Console on a Windows Server 2008 system

1. Right–click the shortcut and select Run as administrator.

   The User Account Control dialog appears and prompts you for permission.

2. Click Allow.

   The Policy Server Management Console opens.

To run SiteMinder command–line tools or utilities on a Windows Server 2008 system

1. Open your Control Panel.
2. Verify that your task bar and Start Menu Properties are set to Start menu and *not* Classic Start menu.
3. Click Start and type the following in the Start Search field:

   ```
   Cmd
   ```

4. Press Ctrl+Shift+Enter.

   The User Account Control dialog appears and prompts you for permission.

5. Click Continue.

   A command window with elevated privileges appears. The title bar text begins with Administrator:

6. Run the SiteMinder command.

More information:

Contact CA Technologies (see page 3)

Oracle RAC Propagation Window Results in SiteMinder Errors

Symptom:

The Oracle RAC nodes propagate changes within 7 seconds. SiteMinder could read and write objects to a policy store, user store, session store, or audit store more often. As a result, the default Oracle RAC propagation window can result in SiteMinder errors. These SiteMinder errors occur because the write operation was made into one node and the read operation was made to another node.

Solution:

Configure the following setting in the Oracle RAC cluster:

MAX_COMMIT_PROPAGATION_DELAY=0

Note: For more information about configuring this setting, see the Oracle documentation.

Policy Server may Fail to Insert Audit Events into the Audit Database

Symptom:

Under heavy load, the Policy Server may fail to insert queued audit events into the audit store. If the failure occurs, the SiteMinder Policy Server log (smps.log) displays the following error:

[INFO] Failed attempt to bulk insert audit message: Code: -1044. DB Code: 2

Solution:

Two registry keys determine when the Policy Server inserts audit events into the audit database: SQLBulkInsertFlushInterval and SQLBulkInsertFlushRowCount:

- SQLBulkInsertFlushInterval determines the frequency in which the Policy Server inserts queued audit events into the audit database. The default value of this registry key is 60 seconds. If 60 seconds elapses before the value defined by the SQLBulkInsertFlushRowCount is reached, the Policy Server inserts all queued audit events into the audit database.
- SQLBulkInsertFlushRowCount determines how many audit events occur before the Policy Server inserts audit events into the audit database. The default value of this registry key is 1,000. If 1,000 audit events are queued before the value defined by SQLBulkInsertFlushInterval is reached, the Policy Server inserts all queued audit events into the audit database.

Modify the SQLBulkInsertFlushRowCount registry key to resolve the error message.

To modify 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\Reports\NamespaceProviders.
   - (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. Increase the value of the SQLBulkInsertFlushRowCount registry key.

   Increase the value to be at least twice as large as the number of audit events that were created, per second, when the error appeared in the SiteMinder Policy Server log.

   Example: If 1,500 audit events occurred when the error appeared, increase the value to 3,000.
3. Do one of the following:
   - (Windows) Save the registry key and exit the Registry Editor.
   - (UNIX) Save the sm.registry file.
4. Restart the Policy Server.

Policy Server Performance with a Sun Java System Directory Server EE Policy Store

Symptom:

The Policy Server takes an exceedingly long time to start when version 6.0 of Sun Java System Directory Server EE is functioning as the policy store.

Solution:

A known indexing issue with version 6.0 results in the performance problem. Regenerate the existing policy store indexes.

Note: Version 6.3.1 of Sun Java Systems Directory Server EE contains fixes that affect the behavior of indexes. These fixes prevent the problem.

Important! The suffix DN is unavailable when you re–index the policy store.

To re–index the policy store

1. Log into the directory server host.
2. Navigate to the *directory_server_install*\bin and run the following command:

   ```
   dsadm reindex -b -t xpsNumber -t xpsValue -t xpsSortKey -t xpsCategory -t
   xpsParameter -t xpsIndexedObject
   -t xpsTombstone instance_path policysvr4
   ```

   directory_server_install

   Specifies the Sun Java System Directory Server EE installation path.

   instance_path

   Specifies the path to the directory server instance functioning as the policy store.

   Note: For more information about dsadm command, see your vendor–specific documentation.
3. Restart the directory server instance.

Sun Java System Directory Server EE Logs Warn that the Search is Not Indexed

Symptom:

I have configured version 6.3.1 of Sun Java System Directory Server EE as a policy store. The directory logs contain warnings stating that the search is not indexed.

Solution:

This is expected behavior and SiteMinder performance is not affected. Restart the directory server instance to stop the warnings.

Searches for Many Policy Objects (63721)

When searching on many policy objects using the Administrative UI, the connection between the Administrative UI and the Policy Server can time out, the Policy Server tunnel buffer can become corrupt, or both. In such cases, the Administrative UI displays a connection timeout error and no search results are returned. To eliminate this problem, adjust the Administrative UI Policy Server connection timeout and create a registry key for the Policy Server tunnel buffer size.

To adjust the Policy Server connection timeout

1. Log in to the Administrative UI.
2. Click Administration, Admin UI, Modify Administration UI Connection, Search to open the Policy Server connection object.

3. Select the appropriate Policy Server and click Submit.
4. Set the Timeout field in the Advanced section to a large value, such as 2,000 seconds.

The Policy Server connection timeout is now increased.

To create a registry key for the tunnel buffer size

1. Create the following Policy Server registry key:

   HKLM\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\PolicyServer\
   Max AdmComm Buffer Size
2. Set this registry key to a large value, such as 2,097,000 KB.
3. Save the changes and exit the registry.

Note: Restart the Administrative UI if these symptoms persist following the connection timeout and buffer size changes.

XPSExport Creates Read Only File (65035)

XPSExport creates read only output XML files, which XPSImport cannot use. To correct this problem, change the permissions on the output XML file to read/write before running XPSImport.

Windows LDAP Driver Version and FIPS/IPv6 Support

For the initial release of the SiteMinder r12.5 Policy Server, Windows LDAP directory drivers for policy stores and user stores have configuration limitations related to IPv6 and/or FIPS 140:

- The LDAP drivers do not support IPv6 connections, so while a Windows-based Policy Server may be configured to service Agent IPv6 connections, if it accesses LDAP stores, the LDAP connections must be configured for IPv4.
- When a Windows Policy Server is configured for FIPS-only operation and is using LDAP-over-SSL for Policy/User Stores, it does not restrict SSL to FIPS-only algorithms.

  Customers wishing to strictly observe all FIPS-140 algorithm restrictions may modify the SSL configuration files accordingly and deploy FIPS-compliant certificates.

Trial Version of Policy Server Supports Only FIPS-compatibility and FIPS-migration Mode (64416)

Problem:

A trial version of the SiteMinder Policy Server can operate in FIPS-compatibility and FIPS-migration modes. Setting the Policy Server to operate in FIPS-only mode results in the Policy Server rejecting the trial license because the license was encrypted using algorithms that are not FIPS compliant.

Solution:

Ensure that the SiteMinder Policy Servers you want to migrate to FIPS-only mode are using a valid SiteMinder license and not a trial license.

Reports and SiteMinder Performance

Under certain circumstances, running analysis and audit-based reports may slow SiteMinder performance. We recommend analyzing the load patterns in your environment to determine the best time to run reports.

IPv6 ODBC Data Sources

Do not use brackets around the IP address when using IPv6 ODBC data sources or the connection fails.

Example: use fec0::9255:20c:29ff:fe47:8089 instead of [fec0::9255:20c:29ff:fe47:8089]

Note: More information on IPv6-supported databases exists in the SiteMinder Platform Support Matrix.

Searching CertSerialNumbers in a Custom Certificate Mapping Fails (59352)

Symptom:

(LDAP) The default Policy Server behavior is to treat a CertSerialNumber as a broken string of numbers. This behavior causes a custom certificate mapping to fail if the user directory stores the CertSerialNumber as an unbroken string of numbers. The Policy Server fails to lookup the user because the default LDAP search contains spaces.

Solution:

Enable the NoSpacesinCertNumbers registry setting. Enabling the registry setting causes the Policy Server to treat certificate serial numbers as an unbroken string of numbers for all serial number comparisons.

Location:
HKEY_LOCAL_MACHINE/SOFTWARE/Netegrity/Siteminder/CurrentVersion/PolicyServer/NoSpacesInCertSerialNumbers

Values: 0 (disabled) 1 (enabled)

Default Value: 0

Mixed Certificate-Based Authentication Schemes (27997)

The following authentication schemes are affected by the value of the Web Agent parameter for FCC Compatibility Mode (FCCCompatMode):

- Certificate or HTML Forms
- Certificate and HTML Forms

Note: For more information about how FCC Compatibility Mode affects the listed authentication schemes, see the *Web Agent Configuration Guide*.

Password Change Fails if UserDN Equal to or Greater than 1024 Characters (52424)

A password change fails and the user receives an error message prompting them to contact the Security Administrator or Help Desk if the combination of the new password; old password; and user identity, which is comprised of the userID, Client IP and time stamp is equal to or exceeds 1024 characters.

Passwords for User Accounts Stored in Active Directory cannot be Locked (48125)

SiteMinder continues to let users change their passwords when the “User cannot change password" feature is enabled for the accounts.

Linux Policy Server Does Not Delete Oracle Session Store Sessions (39143)

Symptom:

A Linux Policy Server may not immediately delete sessions from an Oracle session store when the idle timeout setting for the realm is reached.

Solution:

The Policy Server does begin to delete sessions shortly after the idle timeout setting is reached. For example, if the idle timeout setting is 30 minutes, the Policy Server may begin deleting sessions at 45 minutes.

Single Logout Services Log Errors if ODBC/SQLError Component Enabled (41324)

If the ODBC/SQLError component is enabled in the Policy Server trace log, Single Logout Services can cause the following errors to be written to the trace log:

```
[13:42:44.0] [CSmDbODBC.cpp:189] [CSmDbConnectionODBC::MapResult] [] [][-1]
[Microsoft] [ODBC]
```

The error is expected behavior. The data is ultimately written to the session store database.

Manually Create the webadapter.properties File (72353)

Problem:

The file webadapter.properties is not created in ServletExec's configuration folder, as expected. As a result, OneView Monitor does not work.

Solution:

After configuring OneView Monitor on an RHAS 4.0 platform with a supported web server, manually create the webadapter.properties file in ServletExec's configuration folder. The ServletExec adapter uses the properties in this file to rout HTTP requests from the web server to a ServletExec Application Server (AS) instance.

The webadapter.properties file contains the following properties:

servletexec.aliasCheckInterval

Specifies a minimum number of seconds for the ServletExec adapter to poll the ServletExec AS instance.

Note: Setting this property to a positive number ensures that the ServletExec adapter polls the AS instance for the specified interval of time. As a result, the adapter is automatically updated when the instance's web application data is modified.

Examples:

servletexec.aliasCheckInterval=10

servletexec.aliasCheckInterval=-1

Use this value to disable polling.

instance_name

Specifies the name of a ServletExec AS instance.

servletexec.*instance_name*.hosts

Specifies one or more host names or IP addresses separated by commas.

Note: These are the hosts for which the specified ServletExec AS instance is configured to process requests.

Examples:

servletexec.*instance_name*.hosts=www.abc.com:9090,www.ca.com

servletexec.*instance_name*.hosts=192.168.200.17,192.168.200.43:8000

servletexec.*instance_name*.hosts=all

Specifies that this ServletExec AS instance is configured to process requests from all hosts.

servletexec.*instance_name*.instances

Specifies the IP address and port number of a ServletExec AS instance.

Note: This IP address and port number are used by the ServletExec adapter when forwarding HTTP requests from the web server to the specified ServletExec AS instance. Each instance must have a unique IP address/port number pair.

Example:

servletexec.*instance_name*.instances=127.0.0.1:8888

Specifies default values for the IP address and port number.

servletexec.*instance_name*.pool-increment

Specifies the number of connections that can be added to the connection pool when a connection is needed and the pool is empty.

Note: These connections are used by the ServletExec adapter to communicate with the specified ServletExec AS instance.

Example:

servletexec.*instance_name*.pool-increment=5

servletexec.*instance_name*.pool-max-idle

Specifies the maximum number of idle connections that can be present in the connection pool at any one time.

Note: This number applies to the connections that are used by the ServletExec adapter to communicate with the specified ServletExec AS instance.

Example:

servletexec.*instance_name*.pool-max-idle=10

Using the webadapter.properties file, the ServletExec adapter applies the following algorithm to each HTTP request:

1. Locate all ServletExec AS instances that are configured for the host specified in the HTTP request.
2. Find a match between the URL in the HTTP request and the .instances property of one of the instances located in step 1.
3. Forward the HTTP request to the resulting ServletExec AS instance.

Edit or Delete Responses and Response Groups

Problem:

Responses and response groups cannot be edited or deleted in the context of a Create Domain or Modify Domain task.

Solution:

Edit and delete responses and response groups by clicking the Policies tab, Domains, and Response or Response Group.

Enterprise Policy Management (EPM) Limitations

Each EPM application can have multiple resources that are associated with it. However, each resource can have only one response that is associated with it.

Password Change Behavior with Active Directory (AD) User Stores (82607)

Setting the password change flag for a particular user in an Active Directory (AD) user store invalidates the user's old password. When the password change flag is set, entering any password on the login dialog redirects the user to the password change dialog. To create the new password, however, the user must match the old password in the field on the password change dialog.

This behavior results from password policies that are part of the AD user store and not from SiteMinder password policies and cannot be changed. Because the policies are integral to the AD user store, changing the namespace from AD to LDAP has no effect on this behavior.

Policy Analysis Reports Return No Results (82275)

Valid for Active Directory user directory connections configured over the LDAP namespace.

Symptom:

My Policy analysis reports are not returning user records.

Solution:

Use the Administrative UI to define an alias mapping between the inetOrgPerson attribute and the respective attribute in Active Directory.

Example: If the respective attribute is “user”, create an alias attribute mapping named inetOrgPerson and define the alias as “user”.

Note: For more information on attribute mapping, see User Attribute Mapping in the *Policy Server Configuration Guide*.

Creating a SiteMinder Administrator in CriticalPath IDS 4.2.5 Fails (84995)

Problem

Sun Microsystems' Logical Domains (LDOMS) 1.1 returns a host ID value of 00000000 to SiteMinder. SiteMinder uses this value to create the IDs of policy server objects. When SiteMinder uses the value of 00000000 to create the object ID of the administrator, the resulting object ID is invalid, and the newly-created administrator fails to log in to the server.

Solution

Contact Sun Microsystems for a patch that corrects the host ID value returned to SiteMinder.

Star Issue: 17982871-1

Oracle Issues

The following Oracle issues exist:

Administrative UI and Oracle Policy Store Objects (65782)

When you are using an Oracle policy store and you make changes to policy store objects in the Administrative UI, the changes are effective immediately; however, they may not be visible in the Administrative UI for up to 5 minutes.

SiteMinder Query Timeout and Oracle User Directories (68803)

The SiteMinder Query Timeout is not supported when the Policy Server is connected to an Oracle user directory. You may encounter this limitation when the Oracle response time is very slow.

Policy Server Issues

The following Policy Server issues exist:

Policy Server May Fail to Start due to a Dynamically Updated system_odbc.ini File (55265)

Symptom:

(Linux) The Policy Server may fail to start because the system_odbc.ini file is dynamically updated.

Solution:

After the Policy Server installation, save the file as Read-Only.

Error Message Appears When Starting the Policy Server (127332) (135676)

Symptom:

If your Policy Server and policy store are operating in mixed-mode during an upgrade to r12.5, the following error message appears after the Policy Server starts:

```
[CA.XPS:LDAP0014][ERROR] Error occurred during "Modify" for
xpsParameter=CA.XPS::$PolicyStoreID,ou=XPS,ou=policysvr4,ou=siteminder,ou=netegri
ty,dc=PSRoot
,text: Object class violation

[CA.XPS:XPSIO024][ERROR] Save Policy Store ID failed.
```

Solution:

This message is expected behavior and does not affect the SiteMinder environment.

This message occurs because the r6.x policy store is not upgraded. Part of the upgrade process includes importing the policy store data definitions. The error appears in the SiteMinder Policy Server log because the data definitions are not available in the policy store.

STAR issue: 19759432–01 and 20134656–01

Solaris Issues

The following Solaris issues exist:

Password Screen does not Prompt for Multiple SafeWord Authenticators (56766)

Users are unable to access protected resources when a SafeWord authentication scheme requires both fixed and token-based authenticators. The password screen only prompts users for one authenticator. Therefore, the user is unable to provide both types of credentials and cannot access the protected resource.

Federation Encryption Issue with JCE on Solaris (71293)

Symptom:

An issue occurs with the Java Cryptography Extension (JCE) and legacy federation (formerly Federation Security Services) encryption. This issue happens when an legacy federation Policy Server on Solaris is using certain versions of the JRE. When the Policy Server is acting as an IdP, SAML assertion encryption could possibly fail. If the Policy Server is acting as an SP, SAML assertion decryption could possibly fail.

Solution:

Modify the java.security file in *jre_root*/lib/security so that the sun.security.provider.Sun provider is registered as the first provider.

Note: Other supported platforms with different versions of Java could possibly exhibit this problem. Apply the same solution.

Chapter 9: Defects Fixed

Web Agent or Web Agent Option Pack Not Initializing (53329/160562)

Symptom:

Web Agent or Web Agent Option Pack does not initialize when the first Policy Server listed in the HCO is down, if the HCO is configured in the round-robin mode.

Solution:

This issue has been fixed.

Policy Server terminates abruptly (55611/160506)

Symptom:

Policy Server terminates abruptly when the username has a special character (%).

Solution:

This issue has been fixed.

STAR Issue: 21697579-01

Administrative UI fails to handle ACS data (55802/160501)

Symptom:

Administrative UI fails to handle a large amount of indexed Assertion Consumer Service (ACS) data.

Solution:

This issue has been fixed.

STAR Issue: 21610816-01

Error while Exporting Workspace Entries (79748/160505)

Symptom:

XPSExport utility terminates abruptly when you export workspace entries.

Solution:

This issue has been fixed.

STAR Issue: 21857023-01

Issue with deleting Web Agent Response Attribute (98975/160503)

Symptom:

If a web agent response attribute is deleted, the remaining attributes are not sent in the response during authentication unless the Policy Server is restarted.

Solution:

This issue has been fixed.

STAR Issue: 21837663-1

ETPKI must be upgraded (160568)

Symptom:

ETPKI must be upgraded to the 4.3.8 release.

Solution:

This issue has been fixed. ETPKI has been upgraded to ETPKI 4.3.8 release.

Data Direct Drivers must be upgraded (160679)

Symptom:

Data Direct drivers must be upgraded for all platforms.

Solution:

This is no longer an issue. The Data Direct drivers have been upgraded to version 7.1.5 across all the platforms.

Information about Accessing Administrative UI Help

Symptom:

Information about accessing the Administrative UI Help to know more about the settings to configure the OpenID Authentication Scheme was unavailable.

Solution:

This is no longer an issue. The *Policy Server Configuration Guide* has been updated.

STAR Issue: 21324374-1

Oracle Versions that Support Asynchronous Call

Symptom:

Information about the versions of Oracle that supports asynchronous call was incorrect.

Solution:

This is no longer an issue. The *Policy Server Configuration Guide* has been updated.

STAR Issue: 21313001

Information about Supported OpenID Versions

Symptom:

Information about the versions of OpenID and OpenID Attribute Exchange that SiteMinder supports was unavailable.

Solution:

This is no longer an issue. The *Policy Server Configuration Guide* has been updated.

STAR Issue: 21294111-1

Test Tool Basic Playback Mode Does Not Work with a FIPS-only Policy Server (154109)

Symptom:

If the Policy Server is running in FIPS Only mode, the basic play back mode of the SiteMinder Test Tool does not work.

Solution:

Incorrect ServletExec Reference (161421)

The *Policy Server Installation Guide* has been updated with the correct reference to ServletExec.

STAR Issue: 21123153;2

SQL Server Authentication Information for Report Servers (161427)

The *Policy Server Installation Guide* has been updated to include SQL Server authentication mode considerations for the Report Servers.

STAR Issue: 21123153;2

Extending Policy Store Schema Documentation (161413)

Symptom:

The *SiteMinder Upgrade Guide* incorrectly stated that the policy store schema must be upgraded.

Solution:

The documentation has been revised to state that policy store schema must be extended for policy store objects that 12.5 requires. A schema upgrade is not required.

STAR Issue: 21101867

Policy Store Upgrade Documentation (160518)

Symptom:

The *SiteMinder Upgrade Guide* was missing policy store upgrade steps.

Solution:

The documentation has been revised to state that:

- You are required to stop all Policy Servers before beginning a policy store upgrade.
- You are required to start all Policy Servers after completing a policy store upgrade.

STAR Issue: 21132271

RadiantOne Incorrectly Listed as Supported

Symptom:

The Implementation Guide incorrectly listed the Radiant Logic, Inc. RadiantOne™ Virtual Directory Server

Solution:

The incorrect reference no longer appears in the guide.

STAR issue: 21123716–1

MySQL File Location Incorrect (159256)

The *Policy Server Installation Guide* has been updated with the correct location for the MySQL.sql file.

Chapter 10: Documentation

This section contains the following topics:

SiteMinder Bookshelf

Complete information about SiteMinder is available from the SiteMinder bookshelf. The SiteMinder bookshelf lets you:

- Use a single console to view all documents published for SiteMinder.
- Use a single alphabetical index to find a topic in any document.
- Search all documents for one or more words.

View and download the SiteMinder bookshelf from the CA Technical Support site. You do not need to log in to the site to access the bookshelf.

If you plan to download the documentation, we recommend that you download it before beginning the installation process.

Release Numbers on Documentation

The release number on the title page of a document does not always correspond to the current product release number; however, all documentation delivered with the product, regardless of release number on the title page, supports the current product release.

The release number changes only when a significant portion of a document changes to support a new or updated product release. If no substantive changes are made to a document, the release number does not change. For example, a document for r12 can still be valid for r12 SP1. Documentation bookshelves always reflect the current product release number.

Occasionally, we must update documentation outside of a new or updated release. To indicate a minor change to the documentation that does not invalidate it for any releases that it supports, we update the edition number on the cover page. First editions do not have an edition number.

Command Line Scripting (CLI) Documentation

The guidance and reference information for the Perl CLI API has been combined into the Perl Programming Guide, which is available on the SiteMinder Bookshelf. The Perl POD format for the CLI reference is no longer supported.

Chapter 11: Platform Support and Installation Media

This section contains the following topics:

Locate the Platform Support Matrix

Use the Platform Support Matrix to verify that the operating environment and other required third-party components are supported.

Follow these steps:

1. Go to the CA Support site.
2. Click Product Pages.
3. Enter the product name and click Enter.
4. Open popular links and click Informational Documentation Index.
5. Click Platform Support Matrices.

Note: You can download the latest JDK and JRE versions at the Oracle Developer Network.

Technology Partners and CA Validated Products

The latest list of partners and their validated products.

Locate the Bookshelf

The SiteMinder bookshelf is available on the Technical Support site.

Follow these steps:

1. Go to the Technical Support site.

   Note: You do not have to log in.

2. (Optional) If the Get Support tab is not pulled to the front, click Get Support.

3. Under Find Product News and Support, click Product Pages.

   The Support by Product page appears.

4. Enter SiteMinder in the Select a Product Page field and press Enter.

   The SiteMinder product page appears.

5. Click Bookshelves.

6. Click the link for the release that you require.

   The SiteMinder bookshelf main page appears.

Locate the Installation Media

If you need a base release, follow these steps:

1. Go to the CA Support site and click Product Pages.
2. Enter the product name and click Enter.
3. Open Quick Access and click Download Center.
4. Log in.
5. Locate your product in the Use the Select a Product list.
6. Select a release and gen level. Click Go.
7. Save the installation zip locally and extract the kit to a temporary location.

If you need a cumulative release (cr), follow these steps:

1. Go to the CA Support site and click Product Pages.
2. Enter the product name and click Enter.
3. Open Quick Access and click Hotfix/Cumulative Release Index.
4. Log in.
5. Click the release you want.
6. Save the installation zip locally and extract the kit to a temporary location.

Appendix A: Third–Party Software Acknowledgments

SiteMinder incorporates software from third–party companies. For more information about the third–party software acknowledgments, see the SiteMinder Bookshelf main page.

Appendix B: Accessibility Features

CA Technologies is committed to ensuring that all customers, regardless of ability, can successfully use its products and supporting documentation to accomplish vital business tasks. This section outlines the accessibility features that are part of CA SiteMinder.

Product Enhancements

SiteMinder offers accessibility enhancements in the following areas:

- Display
- Sound
- Keyboard
- Mouse

Note: The following information applies to Windows-based and Macintosh-based applications. Java applications run on many host operating systems, some of which already have assistive technologies available to them. For these existing assistive technologies to provide access to programs written in JPL, they need a bridge between themselves in their native environments and the Java Accessibility support that is available from within the Java virtual machine (or Java VM). This bridge has one end in the Java VM and the other on the native platform, so it will be slightly different for each platform it bridges to. Sun is currently developing both the JPL and the Win32 sides of this bridge.

Display

To increase visibility on your computer display, you can adjust the following options:

Font style, color, and size of items

Lets you choose font color, size, and other visual combinations.

Screen resolution

Lets you change the pixel count to enlarge objects on the screen.

Cursor width and blink rate

Lets you make the cursor easier to find or minimize its blinking.

Icon size

Lets you make icons larger for visibility or smaller for increased screen space.

High contrast schemes

Lets you select color combinations that are easier to see.

Sound

Use sound as a visual alternative or to make computer sounds easier to hear or distinguish by adjusting the following options:

Volume

Lets you turn the computer sound up or down.

Text-to-Speech

Lets you hear command options and text read aloud.

Warnings

Lets you display visual warnings.

Notices

Gives you aural or visual cues when accessibility features are turned on or off.

Schemes

Lets you associate computer sounds with specific system events.

Captions

Lets you display captions for speech and sounds.

Keyboard

You can make the following keyboard adjustments:

Repeat Rate

Lets you set how quickly a character repeats when a key is struck.

Tones

Lets you hear tones when pressing certain keys.

Sticky Keys

Lets those who type with one hand or finger choose alternative keyboard layouts.

Mouse

You can use the following options to make your mouse faster and easier to use:

Click Speed

Lets you choose how fast to click the mouse button to make a selection.

Click Lock

Lets you highlight or drag without holding down the mouse button.

Reverse Action

Lets you reverse the functions controlled by the left and right mouse keys.

Blink Rate

Lets you choose how fast the cursor blinks or if it blinks at all.

Pointer Options

Let you do the following:

- Hide the pointer while typing
- Show the location of the pointer
- Set the speed that the pointer moves on the screen
- Choose the pointer's size and color for increased visibility
- Move the pointer to a default location in a dialog box

Keyboard Shortcuts

The following table lists the keyboard shortcuts that CA SiteMinder supports:

Keyboard	Description
Ctrl+X	Cut
Ctrl+C	Copy
Ctrl+K	Find Next
Ctrl+F	Find and Replace
Ctrl+V	Paste
Ctrl+S	Save
Ctrl+Shift+S	Save All
Ctrl+D	Delete Line
Ctrl+Right	Next Word
Ctrl+Down	Scroll Line Down
End	Line End