CA SiteMinder®

Policy Server Release Notes

12.52

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time. This Documentation is proprietary information of CA and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2013 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

CA Technologies Product References

This document references the following CA Technologies products:

- CA DataMinder™
- CA IdentityMinder (formerly Identity Manager)
- CA Single Sign–On
- CA 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 8: Installation and Upgrade Considerations 27

Chapter 13: Defects Fixed in 12.52 123

Chapter 1: Policy Server Release Notes

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

Chapter 2: New Features in 12.52

This section contains the following topics:

Administrative UI New Look and Feel

The CA SiteMinder® Administrative UI is now refreshed to meet the CA standard for controls, fonts, colors, icons, and images. Frames now use the accordion-style navigation for simpler menu selections. The steps in the configuration wizards have a new, more colorful look. Both changes improve the navigation and ease of configuration.

Enhanced Session Assurance with DeviceDNA™

This release introduces Enhanced Session Assurance with DeviceDNA™

Enhanced Session Assurance with DeviceDNA™ helps prevent unauthorized users from hijacking legitimate sessions with stolen cookies. The session clients are validated using the unique DeviceDNA™ that the product collects from the system of the user. This validation assures that the client who initiated the session is the same client that is requesting access. Users lacking valid DeviceDNA™ are denied access to protected resources.

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

Enhanced User Disambiguation Using Windows and Kerberos Authentication

This release includes the following enhancements to support user disambiguation for Windows and Kerberos authentication:

- A Kerberos authentication scheme template is available from the Policy Server. You can select this scheme in the Administrative UI for resources that CA SiteMinder® protects. The addition of this scheme allows the user to configure Kerberos Authentication from the Administrative UI. See the updated chapter on Kerberos authentication in the Policy Server Configuration Guide.
- The User DN Lookup field has been modified in the Windows Authentication template, and also included in the new Kerberos Authentication template. This addition is so that these configuration schemes can honor the lookup start and end attributes in a search filter. Previously, the two input formats were:

  AD/LDAP Lookup Format:

  CN=%{UID},CN=Users,DC=%{DOMAIN},DC=com

  AD/LDAP Search Format:

  (sAMAccountName=%{UID})

  The new format is any combination of variables UID and DOMAIN without any supporting attribute names:

  %{UID}

  %{UID}@{DOMAIN}
- The User Directory object has been enhanced to include the User Object and User Class fields for the LDAP search. This addition is to support cross-repository identity mapping.

CA Directory Password Policy Control

You can configure the Policy Server to honor the CA Directory password policies. The Policy Server, together with a properly configured Web Agent, can send configured warnings and notifications that are based on the directory password policies to end-users.

Chapter 3: Changes to Existing Features

This section contains the following topics:

Enhanced Application Policy User Interface

The Application Policy user interface is enhanced with the following features:

- You can scroll in the tables that display the resources and roles, and resources and responses information.
- You can filter search results based on roles, resources, or responses.

MS Passport Authentication Scheme Not Supported

This release of CA SiteMinder® no longer supports the MS Passport Authentication Scheme.

SMPS Log Data Enhanced

When an LDAP call fails, SMPS log lists search query for the search calls.

Configuration Wizard No Longer Requires Microsoft SQL Server Administrator Account with Create Permission to Create if Schema is Present

When you install the Policy Server, you can automatically configure Microsoft SQL Server as a policy store. Previously, if you wanted to configure Microsoft SQL Server during installation you required the credentials of a database administrator with **create** permission.

In 12.52, if the CA SiteMinder® schema is already present in the database, the wizard does not require the credentials of a database administrator with **create** permission.

Features Frozen Since the Previous Japanese Version 12.0.3

Some features from older versions were frozen in CA SiteMinder® 12.5. These frozen features are no longer being updated or maintained. The documentation for these frozen features is no longer translated. The following table lists the features from previous releases that were frozen in CA SiteMinder® 12.5 and which feature to use instead for CA SiteMinder® 12.52:

If you used this feature in 12.0.3:	Use this feature instead for 12.52:
CGI Password Services	FCC Password Services
JSPPassword Services	FCC Password Services
An smpolicy.smdif file for default policy store objects	An smpolicy.xml file for default policy store objects
smobjexport utility	XPSExport utility
Multiple smkeydatabases	One centralized smkeydatabase
FWS application deployment instructions	FWS application deployment instructions now in Web Agent Option Pack Guide
Microsoft Passport	Feature dropped by Microsoft. No replacement available.

New Location of the Authentication and Authorization Web Services Scenario

As the Authentication and Authorization Web Services feature is configured and implemented on CA SiteMinder® SPS, the Authentication and Authorization Web Services scenario is moved from the CA SiteMinder® bookshelf to the CA SiteMinder® SPS bookshelf.

Chapter 4: Revised Guidance for the XPS Sweeper Utility

We now recommend scheduling the XPS Sweeper utility to run automatically every 24 hours. Scheduling this utility removes the tombstones of deleted policy store objects regularly.

Chapter 5: 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 140)

Chapter 6: Enhanced Domain Policies User Interface

The Rule and Rule Groups tables of the Domain Policy user interface are enhanced with the following features:

- You can sort the columns of the tables.
- You can filter rules by using the Name filter. When you enter a string, the rules matching the string are displayed. The Name filter accepts only strings but not regular expressions.

Chapter 7: System Requirements

Policy Server Requirements

The following minimum system requirements must be met for the CA 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.
  - 3 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.
  - 3 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**—3 GB.

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**—3 GB.

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**—3 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**—3 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 8: Installation and Upgrade Considerations

This section contains the following topics:

Upgrade Information Page

In addition to the *CA SiteMinder® Upgrade Guide*, CA Support Online includes valuable upgrade information. For more information, see the CA 12.52 Upgrade Information page.

System Locale Must Match the Language of Installation and Configuration Directories (169863)

To install and configure a CA SiteMinder® component to a non-English directory, set the system to the same locale as the directory. Also, make sure that you installed the required language packages so the system can display and users can type localized characters in the installer screens.

For the details on how to set locale and required language packages, refer to respective operating system documents.

Local Fonts and Packages Required to Support International Language Versions of CA SiteMinder® Installers

To type local characters in international language versions of CA SiteMinder® installation and configuration programs in GUI mode, install fonts for that language on your operating environment.

For the RedHat Linux operating environment, download the packages shown in this document.

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

Symptom:

You are doing a console mode installation of a CA 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 CA SiteMinder® components:

- Documentation
- Policy Server
- Administrative UI
- Report Server

Note: Information appears by platform. For more information about supported operating systems, see the 12.52 CA SiteMinder® Platform Support Matrix on the Technical Support site.

Documentation

The CA SiteMinder® bookshelf is available on the Support site. The bookshelf does not require an installer. For more information, see Locate the Bookshelf (see page 140).

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 12.52 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 CA 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 12.52 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 CA 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 12.52 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 CA SiteMinder® component.

More information:

Locate the Platform Support Matrix (see page 140)

Password Policy Message and Active Directory

If you are upgrading to 12.52, 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 CA 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 CA SiteMinder® authentication reason codes, we recommend that you verify that your implementation handles all password message values (PasswordMsg) that the CA 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 CA SiteMinder® authentication reason code.

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

Certificate Revocation List Issuer

If you are upgrading to 12.52 and a CRL is stored in an LDAP directory service, consider the following items:

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

Deprecated CA 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 12.52 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 CA 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 *CA SiteMinder® Upgrade Guide*.

Policy Server Upgrade Requirement for 12.5 GA and 12.5 CR1

The format of certificates that are stored in the 12.52 policy store is different from certificates that are stored in Policy Server r12.5 GA and Policy Server r12.5 CR.

Therefore, export certificates that were imported into the Policy Store before CA SiteMinder® r12.5 CR2 before you upgrade and then reimport them.

Follow these steps:

1. Before you upgrade the Policy Server to 12.52, export the certificates using the Administrative UI or smkeytool.
2. After you successfully export the certificates, delete the certificates from the Policy Store using Administrative UI or smkeytool.
3. Complete the upgrade procedure to Policy Server 12.52.
4. Import the certificates (that were exported in Step 1) using the Administrative UI or smkeytool.

Considerations for Upgrading r6.x to r12.x

If your Policy Server and policy store are operating in mixed-mode during an upgrade to 12.52, 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 CA 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 CA 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 CA 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 CA SiteMinder® utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

To 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

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

- 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.

Policy Server Upgrade Creates New Files

During a Policy Server upgrade, the installer creates new versions of certain files for 12.52. The installer creates the following files in the *policy_server_home*/config directory:

- conapi.conf
- JVMOptions.txt
- profiler_templates
- siteminder.conf
- SMocsp.sample.conf
- SmSWEC.cfg
- smtracedefault.txt
- snmp.conf
- snmptrap.conf
- trace.conf

The installer creates the following files in the *policy_server_home*/properties directory:

- AMAssertionGenerator.properties
- AssertionGeneratorFramework.properties
- cdslog4j.properties
- EntitlementGenerator.properties
- FederationAttributeConfig.properties
- InfoCard.properties
- JSAMLAssertionStrings.properties
- JSAMLProtocolStrings.properties
- log4j.properties
- LoggerConfig.properties
- logging.properties
- openformatexpression.conf
- scriptActiveExpConfig.properties
- smkeydatabase.properties
- WebServiceConfig.properties
- xsw.properties

These 12.52 files use the .new extension: For example, the JVMOptions.txt file from the previous version remains untouched. The installer creates an 12.52 version of the JVMOptions.txt file that is named JVMOPtions.new.

If the original file included customized settings, be sure to modify the .new file with your customized settings. Rename the .new file with the extension from the original file.

For example, if you had custom settings in your JVMOptions.txt file, copy those changes to JVMOptions.txt.new. Rename the JVMOptions.txt.new to JVMOptions.txt.

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 12.52:

- 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*.

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 CA 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 CA 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 CA SiteMinder® component:

- Installation
- Configuration
- Administration
- Upgrade

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

To run CA 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 CA 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 CA 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 CA SiteMinder® command.

More information:

Contact CA Technologies (see page 3)

Deploying CA SiteMinder® Components

If you are deploying CA 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 CA 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 CA SiteMinder® does not support. For supported operating systems, see the CA SiteMinder® 12.52 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 CA SiteMinder® does not support. For supported operating systems, see the CA SiteMinder® 12.52 Platform Support Matrix. For system requirements, see the *Policy Server Installation Guide*.

Chapter 9: General Considerations

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 12.52 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

CA 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
- CA 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
- CA 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 12.52 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 12.52 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 CA SiteMinder® Agent in a Japanese operating system environment may have no more than 175 characters.

Chapter 10: Known Issues

This section contains the following topics:

Administrative UI Contents Not Displaying Properly (176842)

Symptom:

After you change the language in the browser, the contents of the Administrative UI still appear in the previously selected language.

Solution:

Whenever you change the language, clear the browser cache and restart the browser for the current language environment to take effect.

Post Processing Chain Value Causing OpenID Authentication Failure (174220)

Symptom:

OpenID authentication can fail after you upgrade from a version 12.5 Policy Server with the OpenID authentication scheme configured to a version 12.52 Policy Server. The problem occurs when the value of the Post Processing Chain field for the OpenID authentication scheme is set to com.ca.sm.openid.command.StoreClaimsToContext.

Solution:

Modify the class name in the Post Processing Chain field to com.ca.sm.openid.command.StoreClaimsToContextasClaims so that the OpenID authentication scheme functions properly.

Internet Explorer 9 Requires Compatibility View

Symptom:

The OK and CANCEL buttons do not work when configuring XPath expressions for a DCC web service authentication scheme. This behavior exists only when using Internet Explorer version 9.

Solution:

Run Internet Explorer in Compatibility View as follows:

1. See if the Compatibility View button appears in the Address bar. (If you don't see the button, there is no need to turn on Compatibility View.)
2. Tap or click the Compatibility View button to display the site in Compatibility View.

Once you turn on Compatibility View, Internet Explorer will automatically show that site in Compatibility View each time you visit. You can turn it off by tapping or clicking the button again. Or, you can clear the entire list of sites using Compatibility View by deleting your browsing history.

Policy Server Configuration Fails if the Supplied Database Name Contains Japanese Characters (165423)

The Policy Server Configuration Wizard fails if the supplied Database Name value contains Japanese characters.

Policy Server Management Console Cannot Connect to an Audit Store with a Multi-Byte Character Database Name (UNIX) (167772)

On UNIX and Linux platforms, the Policy Server Management Console fails to make a connection to an audit store if the database name contains multi-byte characters, returning Error Code-1063.

OpenID Authentication Scheme Usability Issue (151046)

Configuring the OpenID authentication scheme, requires manual editing of an XML file and copying it to all Policy Servers.

STAR issue: 20777171;1

Administrative UI Behavior Confusing After Inactivity Timeout (171765)

After a period of inactivity, the Administrative UI displays a dialog that states "Session expires in 5 mins; Click 'Ok' to extend the session."

This dialog persists even after the Administrative UI session expire after 5 minutes of further inactivity. Clicking OK after this time dismisses the dialog and appears to return you to the Administrative UI. However, clicking any link or task in the Administrative UI actually results in being logged out.

Cannot View Reports if Report Server Connection is Established Using an IP Address (167987)

Symptom:

The View SiteMinder Reports operation is unable to communicate with the Report Server If the Policy Server connection to the Report Server was configured using the server IP address.

Solution:

Configure the connection to the Report Server using the Report Server hostname, not its IP address.

ASA Agents Can Enable TCP/IP Keep-Alives

Symptom:

ASA Agents now can enable TCP/IP Keep-Alives to prevent network outages from impacting ASA operations.

Solution:

Do one of the following:

- (Windows) Create the following system environment variable with a value of 1:

  SM_ENABLE_TCP_KEEPALIVE

- (UNIX)

  1. Create the following system environment variable:

     SM_ENABLE_TCP_KEEPALIVE=1

  2. Export the environment variable.

Note: The value must be 0 (disabled) or 1 (enabled). If a value other than 0 or 1 is configured, the environment variable is disabled. If the environment variable is disabled, the Policy Server does not send KeepAlive packets to idle Web Agent connections.

Policy Server Can Terminate When Using Novell eDirectory as the Policy Store (175150)

When using Novell eDirectory 8.8 as the policy store, the Policy Server can abnormally terminate. CA Technologies and Novell are investigating the issue.

Star issue 21526251-1.

Novell ticket number 10864464047.

Error Message When Installing the Reports Server on Red Hat Linux 6 32-bit System (169884)

Symptom:

The cabi-linux-3_3_0_2 installer for a Red Hat Linux 6 32-bit machine is expecting a 64-bit library. The following error message displays during the installation of the Report Server:

```
******************************
Linux: Your system is missing required components (STU00120):
******************************
Missing patch: libXext-1.1-3.el6.x86_64
Missing patch: libXext-devel-1.1-3.el6.x86_64

If you continue your installation may not work correctly. (STU00109)
Please press Enter to continue...
```

Solution:

Ignore the error message and proceed with the installation. The Reports Server successfully installs despite this error message.

SAML1.1 Partnership Artifact Transaction Fails With Delegated Authentication

The SAML1.1 partnership artifact transaction fails with delegated authentication when "NAME" is used as the query parameter.

For the artifact transaction to be successful, perform *one* of the following two workarounds:

- When using the TestDA application, do not enter the Service Provider ID. If the NAME query parameter was used to initiate the SAML 1 request, the TestDA application returns both NAME and CONSUMERID resulting in the failure of the artifact transaction.
- When dealing with a specific partnership, do not mix the usage of NAME and CONSUMERID. If you want to switch, restart the servlet container.

RSA SecureID Auth Scheme Not Supported in FIPS Mode

The Policy Server in FIPS mode on Solaris 11 is not supported for the RSA SecureID HTML form authentication scheme.

DSN Names with Non-ASCII Characters Not Supported

Only English characters can be used in Data Source Names (DSN) for ODBC databases that are used as a CA SiteMinder® user, policy, or session store.

AttributeType Not Registered Error in the Administrative UI Log

On installing the Administrative UI, the Administrative UI log shows an error message that the AttributeType has not been registered. The Administrative UI uses ApacheDS which causes this error. You can ignore this error message.

Cannot Specify Non-English Path to Install Administrative UI

You cannot specify local (non-English) characters in the installation path of the Administrative UI.

Local Characters in 4.x Agent Names Not Supported in the FSS Administrative UI

Symptom:

I cannot log in to the FSS Administrative UI.

Solution:

The FSS Administrative UI could possibly have a 4.x agent name with local (non-English) characters. The FSS Administrative UI does *not* support the use of local (non-English) characters in 4.x Agent names.

Objects that Support Only English-Language Characters

Although CA SiteMinder® 12.52 is internationalized, the following objects support English-language (US-ASCII) characters only:

- All cookie names.
- All persistent cookie names.
- The value of the SSOZoneName Agent configuration parameter.
- 4.x Agent names in the FSS Administrative UI.
- Agent names in the FSS Administrative UI.
- Agent configuration objects (ACOs) in the FSS Administrative UI.
- Host configuration objects in the FSS Administrative UI.
- Agent group names in the FSS Administrative UI.
- Administrator names in the FSS Administrative UI.
- AuthValidate Directory Mappings in the FSS Administrative UI.
- Named expressions

The smldapsetup Utility Fails

The smldapsetup utility fails in the following cases:

- The locale of the Policy Server machine differs from the locale of the LDAP machine.
- The LDAP administrator username contains non-English characters.

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, CA SiteMinder® generates the SmStartupEvents.audit file. However, no SNMP events are generated. CA SiteMinder® records the start–up events in the reference log file.

Report Server Configuration (150327,119313)

With CA SiteMinder® 12.52, 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 CA SiteMinder® component:

- Installation
- Configuration
- Administration
- Upgrade

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

To run CA 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 CA 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 CA 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 CA SiteMinder® command.

More information:

Contact CA Technologies (see page 3)

Oracle RAC Propagation Window Results in CA SiteMinder® Errors

Symptom:

The Oracle RAC nodes propagate changes within 7 seconds. CA 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 CA SiteMinder® errors. These CA 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 CA 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 CA 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 CA 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 Support

The Policy Server and the Windows LDAP directory drivers for policy stores and user stores have a configuration limitation that is related to FIPS 140.

When a Windows Policy Server is configured for FIPS-only operation, it does not restrict SSL to FIPS–only algorithms. This behavior occurs when the following conditions are met:

- The Policy Server is using LDAP–over SSL for a policy.
- The Policy Server is using LDAP–over SSL for a user store.

The Policy Server is using LDAP–over SSL for a policy store and a user store.

Customers that must observe all FIPS-140 algorithm restrictions can modify the SSL configuration files and can deploy FIPS-compliant certificates.

Reports and CA SiteMinder® Performance

Under certain circumstances, running analysis and audit-based reports may slow CA 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 CA 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)

CA 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*.

Application Resources Dialog Topic in Administrative UI Help Has Incorrect Statement Regarding Wildcard Characters (179031)

The Application Resources Dialog topic in the Administrative UI Online Help includes the following incorrect statement about wildcard characters in the Resource field:

> **Note**: Asterisk (*) and question mark (?) characters are treated as literal characters in resource filters (not wildcards).

Asterisk (*) characters are in fact treated as wildcards so the statement should actually read as follows:

> **Note:** The question mark (?) character is treated as a literal character in resource filters (not as a wildcard).

STAR issue: 21576159-1

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 12.52, 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 CA 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 CA 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.

OAuth and OpenID Authentication Scheme Problems on Solaris (167716)

Symptom:

- The OpenID authentication scheme discovery fails due to a connection error: The Policy Server cannot perform discovery on the provided OpenID identifier.
- The OAuth authentication scheme cannot verify the OAuth token that the OAuth provider issued after a successful authentication.

Solution:

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

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

Advanced Password Services (APS) Issues

The following APS issues exist:

APS Uses Unsafe Functions on Windows Server 2008

Symptom:

On Windows Server 2008, Advanced Password Services uses functions deemed unsafe by Microsoft Security Development Lifecycle (SDL).

Solution:

This is no longer an issue. The unsafe functions have been replaced.

APS Client Components Must Be Configured as 4.x Agents Which Do Not Support IPv6 Addressing (167337)

Symptom:

When configuring APS, you create 4.x Agent objects to represent for the Help Desk (APSAdmin), Forgotten Password (FPS), and Change Password interface client components. However, agents that are configured to act as 4.x Agents do not support IPv6 addresses.

Solution:

In a pure IPv6 environment, install and configure the APS client components on the same system as the Policy Server and use a loopback IP address (for example, 127.0.0.1) in the agent configuration.

Otherwise, use an IPv4 and IPv6 mixed environment.

Chapter 11: Defects Fixed in 12.5

This section contains the following topics:

WebLogic Agent Failed to get DMS Group Membership Details (CQ155207)

Symptom:

During any group membership searches, the agent returned the following error:

```
SmUserDirectory Failure
```

Solution:

This issue is fixed.

STAR Issue # 20747701:01

The Web Service Variable not Encoding Ampersands in Nested Variables (CQ151736)

Symptom:

The web service variable did not properly encode ampersands (&) in nested variables.

Solution:

This issue is fixed.

STAR Issue # 20726860:01

Web Service Variable resolution HTTP Thread not Closing Sockets (CQ154111)

Symptom:

The web service variable resolution HTTP thread is not closing sockets on the Policy Server in a timely manner. The sockets remain in a CLOSE_WAIT state. Under heavy loads, this situation exhausted the supply of file descriptors.

Solution:

This issue is fixed.

ServerHeartbeat Thread Crash (CQ156277)

Valid on RedHat

Symptom:

The ServerHeartbeat thread crashed.

Solution:

This issue is fixed.

STAR Issue # 20872776:01

Policy Server Hung When Connection Limits Exceeded (CQ157598)

Symptom:

The Policy Server hung when its connection limits were exceeded.

Solution:

The issue is fixed.

STAR Issue # 20904378:01

FSS Administrative UI not Authenticating External Administrators Whose Passwords Contain Ampersands (CQ157596)

Symptom:

The FSS Administrative UI was not authenticating external administrators whose passwords contain ampersands (&).

Solution:

The issue is fixed.

STAR Issue # 20933409:01

MaxThreadCount Does not Accept Values Above 10 (CQ153043)

Valid on RedHat

Symptom:

The MaxThreadCount setting did not accept values greater than 10.

Solution:

The issue is fixed.

STAR Issue # 20818420:01

UseSecureCookies Parameter and Advanced Password Services (CQ153055)

Symptom:

Setting the UseSecureCookies parameter-value to yes did not always set secure flags in the following cookies:

- NPSFPSDN
- NPSFPSMacros
- NPSFPSSpecial
- NPSFPSData

Solution:

The issue is fixed.

STAR Issue # 20716855:01

Administrative UI and FSS Administrative UI inconsistencies in 12.0.3.9 Regarding Host Configuration Object - Clusters (CQ160633)

Symptom:

The following conditions were observed:

- Administrative UI does not display the "Failover Threshold Percentage" or "Failover Threshold" for a Host Configuration Object created in the FSS Administrative UI on the Clusters Tab.
- Modification of the "Failover Threshold Percentage" in the Administrative UI for the host configuration object incorrectly creates a parameter on the General Tab in the FSS Administrative UI with an incorrect name of "FailOverThreshold".
- Modifying the "Failover Threshold Percentage" value on the Cluster Tab of the FSS Administrative UI does not appear in the "FailOverThreshold" parameter on the General Tab. The FailOver Threshold value does not appear in the Administrative UI.
- Modification of the "FailOverThreshold" parameter on the General Tab of the FSS Administrative UI does not modify the "Failover Threshold Percentage" on the Clusters Tab.
- "FailOverThreshold" parameter from General Tab of the host configuration object in the FSS Administrative UI is not appearing in the "General" section.

Solution:

These issues are fixed.

STAR Issue # 20736264:01

Running Policy Server 12SP3CR09 on Policy Store 6.0SP5CR09, Policy Server crash randomly (CQ158841)

Valid on Solaris

Symptom:

Policy Server version 12.0.3.9 crashed randomly when using a 6.0.5.9 policy store.

Solution:

This issue is fixed.

STAR Issue # 21052167:02

OneView is showing inconsistent values for HItRate (CQ155300)

Symptom:

The OneView monitor showed inconsistent values for HItRate.

Solution:

This issue is fixed.

STAR Issue # 20863232:01

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 *CA 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 *CA 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.

Administrative UI Deletes Users from Policy Objects When Modifying Realms or Policies After Importing r6.x Policy Store (157701)

Symptom:

Administrative UI deletes users from policy objects when modifying realms or policies after Importing an r6.x policy store.

Solution:

This is no longer a problem.

STAR issue: 20993077-1

Boolean User Directory Attribute Mappings in Application Object Roles Fail (154130)

Symptom:

User directory attribute mappings defined in Application object roles that include boolean expressions fail to resolve.

Solution:

This is no longer a problem.

STAR issue: 20881853-1

CA SSO (smauthetsso) Custom Authentication Scheme Fails in FIPS Mode on Windows (150671/164657)

Symptom:

Authentication using the CA SSO (smauthetsso) custom authentication scheme fails in FIPS mode on Windows.

Solution:

This is no longer a problem.

STAR issue: 20736967

Dead Lock Condition in the LDAP Authentication Layer (162301)

Symptom:

An error in the LDAP authentication layer results in a dead lock condition.

Solution:

This is no longer a problem.

STAR issue: 21181025;1

Host Registration Fails Using smreghost Fails When Pointing to an r6.x Extended Policy Store (164607)

Symptom:

The Policy Server does not allow host registration using smreghost when pointing to an r6.x extended policy store.

Solution:

This is no longer a problem.

Kerberos Authentication Fails for Users With a Large Number of Group Memberships in Active Directory (154373/164659)

Symptom:

Kerberos authentication fails for users who have a large number of group memberships in a Microsoft Windows Active Directory.

Solution:

This is no longer a problem.

STAR issue: 20906310-1

OpenID Authentication Fails When Multiple User Directories are Configured in a Domain (162951)

Symptom:

OpenID authentication fails with the following error when multiple user directories are configured in a domain: "nonce verification failed."

Solution:

This is no longer a problem.

STAR issue: 21175148;1

Policy Server Cannot Authenticate Users from User Directories with Password Policies Using an r6.x Policy Store (160138)

Symptom:

Policy Server cannot authenticate users from a user directory with password policies using an r6.x policy store.

Solution:

This is no longer a problem.

STAR issue: 21112688;1

Policy Server Configuration Wizard Fails When Using Drives Other Than C: on Windows (153459)

Symptom:

The Policy Server configuration wizard fails when using Disk drives other than C: in the Windows platform.

Solution:

This is no longer an issue.

STAR issue: 20885033;1

Policy Server Configuration Wizard Shows the Incorrect Minimum Required JDK/JRE Version (157948)

Symptom:

The Policy Server configuration wizard incorrectly shows the minimum required JDK/JRE version as 1.6.0.30.

Solution:

This is no longer a problem.

STAR issue: 20991445

Policy Server Does Not Properly Protect Resources When Using an r6.x Extended Policy Store

Symptom:

The Policy Server incorrectly marks resources as not protected when using an r6.x extended policy store.

Solution:

This is no longer a problem.

STAR issue: 21173076-1

Policy Server Exits Abnormally on Linux When Identity Manager Integration is Enabled (151725/150968)

Symptom:

When attempting to configure an Identity Manager directory on a Linux Policy Server, the directory creation operation fails and the Policy Server exits abnormally.

Solution:

This is no longer an issue.

STAR issue: 20679358

Policy Server Installer Fails to Configure IPlanet Web Server/ASF Apache for FSS UI During Installation (155738)

Symptom:

The Policy Server installer fails to configure IPlanet web server/ASF Apache 32-bit for FSS UI when the "Web Server" option is selected during an installation.

Solution:

This is no longer a problem.

STAR issue: 20982339;1

Policy Server Installer Hangs When Encryption Key Contains Dollar Sign ($) Characters (160825)

Symptom:

The Policy Server installer hangs if the encryption key contains the dollar sign($) character.

Solution:

This is no longer a problem.

STAR issue: 21136554-1

Policy Server Race Condition Prevents Updates to Agent Configuration Objects Using the Java Policy Management API (154521/164660)

Symptom:

A Policy Server race condition can prevent updates to Agent Configuration Objects using the Java Policy Management API.

Solution:

This is no longer a problem.

STAR issue: 20932855

XPSDDInstall Abnormally Terminates When Upgrading from r12 SP3 to r12.5x Policy Server (158655)

Symptom:

The XPSDDInstall utility abnormally terminates when upgrading from the Policy Server from r12 SP3 to r12.5x.

Solution:

This is no longer a problem.

STAR issue: 21077994-01

FSS Applet UI Did Not Launch in RH5 [157387]

Symptom:

The FSS Applet UI did not launch in RH5. The FSS UI was not launched if it did not have the Policy Server environment variables.

Solution:

This problem has been fixed.

Star issue 20982339;1

FSS UI Does Not Allow More Than 10 IP Addresses in a Policy Definition (158631/163943)

Symptom:

The FSS UI does not allow more than 10 IP addresses in a policy definition.

Solution:

This is no longer a problem.

STAR issue: 20318453

Authorization Fails for Users in ODBC Directories Configured With UNION-based Query Schemes (159354)

Symptom:

Authorization fails for users in ODBC directories configured with UNION-based query schemes.

Solution:

The Policy Server logic has been optimized to execute as follows when authenticating users in an ODBC database:

1. Validate the distinguished name (DN) with the SQL query configured in "InitUser". This steps checks whether the DN is a user or not.
2. If the above does not produce result, execute the SQL query configured in "GetGroupProp". This steps checks whether the DN is a user or not.

This optimization prevents the Policy Server from executing a UNION-based SQL query that is configured in "Get User/Group" for every "user" authentication.

STAR issue: 21097422-1

Policy Server Cannot communicate over SSL with LDAP Directory Servers That Specify an AKI (Authority Key Identifier) Attribute in the Certificate (160293/164029)

Symptom:

The Policy Server cannot communicate over SSL with LDAP directory servers that specify an AKI (Authority Key Identifier) attribute in the certificate.

Solution:

This is no longer a problem.

STAR issue: 21125449-1

Administrative UI and smkeytool Fail to Properly Import and Store Certificates Over 1024 Characters to Active Directory Policy Store (160848)

Symptom:

Administrative UI and smkeytool fail to properly import and store certificates over 1024 characters to an Active Directory policy store.

Solution:

The Administrative UI and the SiteMinder key tool (smkeytool) are now able to import and store the certificates whose key length is greater than 1024 characters in the policy store.

STAR issue: 21131704;1

Policy Server Configuration Wizard Breaks the FSS UI on Windows on Windows 2008/Windows 2008 R2 (157938)

Symptom:

The Policy Server configuration wizard does not check for the CGI IIS role as a prerequisite for configuring the IIS web server and breaks the FSS UI.

Solution:

This is no longer a problem. The Policy Server installer now checks for the CGI IIS role in the Windows.

STAR issue: 20991445

Policy Server Abnormally Terminates Processing OnAuthAttempt Rules Bound to an Application Object (161793)

Symptom:

If a user provides invalid credentials, the Policy Server abnormally terminates when processing an OnAuthAttempt rule that is bound to an Application object.

Solution:

This is no longer a problem,

STAR issue: 21161067-1

Policy Server Fails to Authorize Users in Active Directory if Load Balancing is Configured in the Administrative UI (160607)

Symptom:

If load balancing is configured in the Administrative UI, the Policy Server does not authorize users in Active Directory.

Solution:

This is no longer a problem.

STAR issue: 21135327-2

Chapter 12: Defects Fixed in 12.51

This section contains the following topics:

Administrative UI Localization Strings Missing [148680]

Symptom:

A few strings were missing from the Administrative UI localization bundles.

Symptom:

This problem was fixed indirectly with the FW upgrade to version 2.2.

Star issue 20680999;1

More Than One Way Is Available to Locate a Web Page within a Set of Web Pages [149533]

Symptom:

VPAT standard states: “More than one way is available to locate a Web page within a set of Web pages except where the Web page is the result of, or a step in, a process."

Solution:

The Administrative UI now includes site map link in the footer, which launches a page that displays all the available. Clicking the link launches the task.

Hostname Missing in CA SiteMinder® Trace Logs [151003]

Symptom:

In the CA SiteMinder® trace log, the Hostname did not appear in the Data column for the Received Agent Request line.

Solution:

This problem has been corrected.

Star issue 20720366-1

HTTPSClient.java Truncates One Byte in Response [151370]

Symptom:

HTTPSClient.java truncated one byte in a response in an SSL communication.

Solution:

This problem has been fixed.

Star issue 20709184

The Administrative UI Was Not Displaying the Failover Threshold Value [152997]

Symptom:

The Administrative UI did not display the Failover Threshold for a Host Configuraiton Object created in the FSS UI.

Solution:

This issue has been corrected.

Star issue 20736264;1

The Session Portion in the Anonymous Authentication Scheme Was Not Disabled in Firefox or Safari Browsers [154723]

Symptom:

When modifying an authentication scheme for a realm to Anonymous, the Session portion was not disabled for the Firefox and Safari browsers.This flaw allowed a user to modify the maximum and idle timeout.

Solution:

This problem been corrected.

Star issue 20917601-1

Date in Activity-By-User Report Incorrect [153070]

Symptom:

After the administrator generated the activity-by-user report, the date in the detail section (the date below the name of the web agent) was incorrect.

Solution:

The date has been corrected.

Star issue 20601274-2

The saml.namespace.prefix Did Not Change [153074]

Symptom:

The saml.namespace.prefix did not change from saml to ns1 after a couple of attempts.

Solution:

The root cause was to reset the value of namespace prefix explicitly for WSFED protocol to ns1. After further analysis we found that setting this namespace is to print the value of the assertion with the prefix ns1 in the WSFED protocol.

This issue has been fixed.

Star issues 20572229;1+20666241;1+20700082;01

The VEXIST Function Was Not Working [153135]

Symptom:

The VEXIST function was not working as expected. The documentation states that the VEXIST function accepts a named expression, a context variable, or user attribute. The function determines whether the input parameter is defined.

Solution:

This issue has been fixed.

Start issue 20468703;01

Policy Server Was Unable to Reestablish Connection with Database [153300]

Symptom:

After a database is refreshed and restarted, the Policy Server cannot connect to the database. The workaround was to modify the User Directory definition, or to stop and start Policy Server.

Solution:

By default, the Policy Server does not retry a database connection in case of invalid credentials. You can enable the retrial of connection by enabling a key EnableRetryForInvalidCredentialsError in the registry. To disable EnableRetryForInvalidCredentialsError, set its value to zero (the default).

Star issue 20775937

Error Message When Saving SAML Authentication Schemes Following Upgrade (CQ153307)

Symptom:

After upgrading the product from 6.0.4 to 12.0.3, I received the following error message when trying to save or update my SAML authentication schemes:

```
Issuer value must be unique for all SAML 1.1 POST Auth Schemes
```

Solution:

This issue is fixed.

Time Stamp Anomaly in Audit Logs [153382]

Symptom:

A customer was trying to import audit logs into ODBC database using the smauditimport utility. The customer noted that the smauditimport uses local time and the GMT offset is stripped off during insertion of records into database.

Solution:

This issue has been addressed using the gmtime instead of the localtime.

Star issues 20779428-1,20808318-1

Policy Server R12 Sp3 Build 258 Solaris 10 Set-up Failure [153536]

Symptom:

Core dump file showed that the failure happened during LDAP result processing.

Solution:

This issue has been fixed.

Star issue 20763726-2

Named Expressions Using Non-ASCII Characters Failed [153544]

Symptom:

An exception occurred when the named expression used a non-ASCII character. The customer was unable to create another expression afterwards.

Solution:

This problem has been corrected. Named expressions now allow non_ASCII characters.

Star issue 20830571

Admin Applet Only Allows 10 IP Addresses in Policy [153776]

Symptom:

On a Policy Server version 6.0 SP5 CR15 the IP Addresses tab of Policy accepts no more than ten IP addresses. After the administrator adds the tenth IP address, the ADD button is grayed out.

Support tested with R12 and saw the same limitation with FSS UI. There is no such limitation when using the Administrative UI.

Solution:

This issue has been corrected.

Star issue 20318453

SAML Target with Query Parameter at Realm Failed [153791]

Symptom:

Because unique SAML authentication schemes are set at the realm level, they specify the complete target including the query string. When the query string is specified, the Service Provider sees the resource as not protected by the FWS and results in a 500 error.

Solution:

The code that determines whether the URL is protected now adds any query parameter that is on the request.

Event Viewer Error Occurred When SM r6sp6cr2 Policy Server Started Up [153912]

Symptom:

This error occurred when a user accessed a protected resource using the certorform authscheme.

Solution:

This error has been fixed.

Star issue 20571107;1

XPSCounter Was Not Working When a Connection to SSL Enabled UD (ODBC) [153920]

Symptom:

Customer was getting segmentation fault when using the XPSCounter program with SSL enabled UD (ODBC). XPSCounter worked fine with a non-SSL port.

Solution:

This problem has been corrected.

Star issue 20809282-1

Accessing Agent Configuration Objects from the FSS UI Caused a Policy Server Failure [154104]

Symptom:

While accessing ACO from the FSS UI, the Policy Server reads property section. If the property section contains an invalid entry, the Policy Server fails..

Solution:

Validate the property section before accessing the properties.

Star issue 20797838

Policy Server Profiler Did Not Add Headers at the Start of a New Log [154520]

Symptom:

Unlike the Web Agent Trace, which puts in headers at the start of each new log file, the Policy Server profiler does not. This inhibits the ability to appropriately follow and correct problems within log files.

Solution:

This problem has been addressed.

Star issue 20890141;01

Missing TransactionID in Authentication Message in Policy Server Profiler Trace Logs [155208]

Symptom:

In The Policy Server Profiler Trace logs, the TransactionID was not logged in the line where Authentication Status message is logged.

Solution:

This issue has been fixed.

Star issue 20955265-1

SMSAVEDSESSION Deleted After Access Resource Not Allow Impersonation [155736]

Symptom:

With an impersonation session, the user gets a SAVEDSESSION cookie and an impersonated SMSESSION cookie. The SAVEDESSION Cookie is sometimes deleted on a challenge. Because the SAVEDESSION cookie is deleted, the user fails to log out impersonation using @smpopsession=true.

Solution:

The problem has been corrected.

Star issue 20881788-1

Auto-sweep Setting Would not Change to False (CQ157057)

Symptom:

The auto-sweep setting for the XPS-tools would not change to false.

Solution:

This issue is fixed.

STAR Issue # 21044876:01

Password Policy can Prevent RSA Ace/SecureID Password Change (157216)

Symptom:

If a password policy is configured to force a lower case character and a new user is required to change the PIN, the change fails.

Solution:

This issue is fixed.

STAR issue: 20958896

Issue with Switching the LOG LOCAL TIME Registry [158101]

Symptom:

When the LogLocalTime parameter was set 0x1, the SMPS events appear in Local Time. When the LogLocalTime parameter was set 0x0, the SMPS logged events with GMT time. If the Policy Server failed to read the LogLocalTime parameter during an update, the LocalTime was changing from LocalTime to GMT.

Solution:

An explicit condition is set to check for the local time. If this operation is successful, then Logger Timezone is adjusted accordingly. If the Policy Server fails, the existing TimeZone value is preserved.

Star issue 20683202-1

Policy Server in Mixed Environment Fails (158841)

Symptom:

A 12.0.3 cr09 Policy Server failed randomly when communicating with a 6.0.5 cr09 policy store.

Solution:

The issue is fixed. The Policy Server does not randomly fail in the mixed-—mode environment.

STAR issue: 21052167–2

One View Monitor Shows Null Pointer Exception [158990]

Symptom:

A client created a custom table in the One View Monitor. The client added a field in the table. The monitor displayed null pointer exception. In other words, NULL checks are missing for variables, which results in NULL-pointer exceptions.

Solution:

The problem has been addressed. Null pointer exceptions occur.

Star issue 21010205-1

Bulk Loading Audit Records Fails on Oracle (161705)

Symptom:

The bulk loading functionality of the smauditimport utility does not work for an Oracle audit store.

Solution:

The issue is fixed. The utility can be used to bulk load records in to an Oracle audit store.

STAR issue: 21045785–1

PS Configuration Wizard Does Not Allow For Retry for LDAP Configuration [157947]

Symptom:

The Policy Server configuration wizard did not give the retry option to change any LDAP-related information. The wizard only showed abort and exited. When the configuration was rerun, the configuration was stuck at the step of importing the objects.

Solution:

The wizard now supports the retry option for the LDAP configuration.

Start issue 20991445

Kerberos Ticket in HTTP Header causes Authentication Failure (159208)

Symptom:

If the Kerberos token in the HTTP authorization header is more than 4096 bytes, Kerberos authentication fails.

Solution:

This issue is fixed.

STAR issue: 20906310–1

Cannot Create a Federation Partnership in the Administrative UI on Windows Server 2008 R2 with French Language Pack (159616)

Symptom:

On Windows Server 2008 R2 with the French language pack, federation partnership creation fails with the following error message in the Policy Server log:

```
09:37:45,021 DEBUG [NamesExceptionHandler] Exception while reading
5328e4c6_sqljdbc.jar
java.util.zip.ZipException: error in opening zip file
```

Solution:

This is no longer an issue.

STAR issue: 21081194-1

Administrative UI and FSS UI Inconsistencies in Host Configuration Object - Clusters Configuration [159938]

Symptom:

In the HostConfig object, the cluster configuration failover threshold percentage was not reflected in Administrative UI. The FSS UI was working correctly.

Solution:

This issue has been corrected.

Star issue 20736264-1

SharePoint PeoplePicker Timeouts (CQ160259)

Symptom:

My SharePoint people picker times out when I search a large database. I do not want to disable the loopback feature.

Solution:

This issue is fixed with the following registry setting:

`EnableSorting`

For more information, see the Agent for SharePoint Guide.

STAR Issue # 20956438:01

Policy Server Reports ODBC Error with Audit Store (161511)

Symptom:

If the following conditions are met, the Policy Server reports an ODBC error with the audit store when stopped:

- The environment contains multiple 12.0.x Policy Servers.
- The administrative Policy Server is configured for an ODBC audit store.
- The remaining Policy Servers are configured for text-based auditing.

Solution:

The issue is fixed.

Java Stack Trace Provided Sensitive Information [161676]

Symptom:

A Java stack trace report provided detailed information that can possibly be valuable to an attacker.

Solution:

This problem was resolved in FW 2.2. The Java stack trace is no longer shown in the Administrative UI.

Star issue 21164212

Enabling Secure Cookies

Symptom:

Information about how to enable secure cookies after registering the Administrative UI with HTTPS was unavailable.

Solution:

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

STAR Issue: 21164228

Cookie Issue: HttpOnly Flag Not Set [161680]

Symptom:

If an attacker finds a flaw in the application such as cross-site scripting, then the attacker system can appropriate the cookie. Setting the HttpOnly attribute means that client side Javascript cannot read the cookie.

Solution:

Set httpOnly flag for cookies.

Star issue 21164232

SAML Token Claim Did Not Include All Active Directory Groups [161738]

Symptom:

A SAML token claim that was sent from SiteMinder to SharePoint did not include all Active Directory Groups for some users.

Solution:

The problem has been resolved.

Star issue 21159815-1

IBM Directory Server Referrals and SiteMinder

Symptom:

Information about whether the IBM Directory Server referrals are compatible with CA SiteMinder® was unavailable.

Solution:

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

STAR Issue: 21278328-1

Policy Server Memory Consumption Increases during Policy Store Import (167569)

Symptom:

Importing a policy store in parallel with cache updates can result in a gradual increase of Policy Server memory consumption.

Solution:

This issue is fixed.

STAR issue: 21072845–2

Administrative UI Allows Browser to Store and Autocomplete Password Field Contents (161675)

Symptom:

The Administrative UI allows a user browser to remember credentials entered into the password field for later autocompletion of that field. This is a security risk as the stored credentials can be captured by an attacker who gains access to the system on which the credentials are saved.

Solution:

This is no longer an issue. The Administrative UI does not allow the browser to store the contents of the password field.

STAR issue: 21164211

Administrative UI Susceptible to Clickjacking Attacks

Symptom:

The Administrative UI is susceptible to clickjacking (also known as "UI redress attacks"), in which an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link or typing login information on another page when they intend to click or type on the Administrative UI login page.

Solution:

This is no longer an issue. The Administrative UI does not open inside an invisible frame and instead displays an error message.

STAR Issue: 21164191

Problem with AKI Attributes on Certificates (CQ164030)

Valid on Windows

Symptom:

I have problems configuring my SSL connections when the certificates for my directory servers use the AKI attribute.

Solution:

This issue is fixed. 12.52 uses an upgraded LDAP SDK that does not have this issue.

STAR Issue # 21125449:01

Unable to Create a Search Query in the Administrative UI (165003)

Symptom:

The Administrative UI expression editor does not support queries that include multiple parenthesis.

Example:

```
(&(c3sBillableStatus=0)(|(c3sAuthorizedProductId=SciFinder)(c3sAuthorizedProductId=SCIFINDER-ACADEMIC)))
```

Solution:

The issue is fixed. The expression editor supports queries that include multiple parenthesis.

STAR issue: 20993066–1

Global Authorization Events and Anonymous Authentication (165663)

Symptom:

If a realm is protected with the Anonymous authentication scheme, global authorization events are not processed.

Solution:

The issue is fixed.

STAR issue: 21203859–1

Cannot Create User Name with Special Characters

Symptom:

A user name that contains the following special characters causes an error during authentication:

% + " & [\ ] ^ ' { | } < > #, / \r \n * =.

Solution:

Use regular alphanumeric characters in user names.

Policy Server Failed under Load of DoManagement Calls [168102/168994]

Symptom:

The Policy Server was failing on Red Hat 5. The customer did not identify any particular activities that seemed to be causing the problem.

Solution:

The Policy Server no longer fails under this condition. The Process ID of the Policy Server through the duration of the DoManagement call remains the same.

Chapter 13: Defects Fixed in 12.52

This section contains the following topics:

Additional Information About Bulk Loading Audit Data ODBC Database Required in Policy Server Administration Guide (159529) (see page 137)
Addition of the OpenID Authentication Plug-in (see page 137)

Event Library File Documentation (178452)

Symptom:

Information about adding an Event Library file (eventsnmp.dll) while using a monitoring service to monitor the Policy Server, was not available.

Solution:

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

STAR Issue: 21567951;1

Apache Process Aborts on Accessing login.fcc File (177053)

Symptom:

The Apache process aborts on accessing the login.fcc file using an incorrect path.

Solution:

This is no longer an issue.

STAR Issue: 21565391-1

Create Partnership Drop-down Not Displaying Properly (176737)

Symptom:

The Create Partnership drop-down menu is not displayed properly in the Administrative UI.

Solution:

This is no longer an issue.

STAR Issue: 21556418;1

Information to Upgrade r12 Policy Server is Unclear (176533)

Symptom:

The *Upgrade Guide* does not have clear instructions about how to upgrade an r12.x Policy Server to 12.52 when smkeydatabase is in use.

Solution:

This is no longer an issue. The Migration Considerations section of the *Upgrade Guide* has been updated.

STAR Issue: 21535336-1

Administrative UI Not Working After Upgrade (176504)

Symptom:

On upgrading the Administrative UI to 12.51, the Administrative UI is not working properly.

Solution:

This is no longer an issue.

STAR Issue: 21275704-3

The Administrative UI Failed while Manipulating Federation Partnerships (175622)

Symptom:

The Administrative UI slowed down and failed with an AGENTAPI_FAILURE while manipulating Federation partnerships.

Solution:

This problem is fixed.

Star issue 21493650-1.

Authorization Fails with EPM Application (175148)

Symptom:

If the role uses BELOW and if the user directories are configured in the load balancing mode, authorization fails with the EPM application,

Solution:

This is no longer an issue.

STAR Issue: 21517922-1

Administrative UI Added an Extra Pair of Parenthesis on the LDAP Notation (174905)

Symptom:

When a user tried to add users to a Domain Policy, the Administrative UI was adding an extra pair of parenthesis on the LDAP Notation.

Solution:

The JavaScript code now only adds parenthesis in a complex LDAP expression.

Star issue 21506542-1.

The smkeytool Was Not Importing Two Files in R12.51 cr01 (174693)

Symptom:

Smkeytool was generating an error while running the following command:

```
smkeytool.sh -addprivkey -alias testcert -keyfile SampleAppPrivKey.key -certfile SampleAppCert.crt
```

This command worked in previous versions.

Solution:

This issue has been corrected.

Star issue 21514671.

Latin ISO Users in AD/AD LDS User Store Were not Able to Authenticate (174354/172053)

Symptom:

The Policy Server authenticated English users without any issues. Non English users, however, in AD with AD namespace were not authenticated

Solution:

This is no longer a problem.

Star issue 21430448;1.

VLV Indexing on Some LDAP User Directories Causes SiteMinder Agent Group Lookups to Fail (174279)

Symptom:

Flaws in the Virtual List View (VLV) implementation on some LDAP user directories can cause SiteMinder Agent group lookups to fail, returning zero entries and raising a “directory unwilling to perform" error.

Solution:

If you experience SiteMinder Agent group lookup failures as described, disable VLV lookups on the Policy Server.

Create the registry key EnableVLV of type DWORD at the following location:

`HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\Siteminder\CurrentVersion\DS\LDAPProvider`

EnableVLV

Disables or enables VLV for LDAP directory lookups. To disable VLV, set EnableVLV to 0. To enable VLV, set EnableVLV to 1.

Values: 0 (disabled) or 1 (enabled).

Default: 1 (enabled).

STAR issue: 20397633-1

Upgrade Results in Suddden Spike in CPU Usage (174236)

Symptom:

Upgrading from r6 to 12.51 results in the smpolicysrv process using 100 percentage of CPU usage.

Solution:

This is no longer an issue.

STAR Issue: 21507336;1

CA SiteMinder® Web Services Documentation (173173)

Symptom:

The URLs to load the WSDL and WADL files and the REST URI were incorrect.

Solution:

This is no longer an issue. The Web Services Scenarios *Guide* has been updated.

STAR Issue: 21483616-1

The Administrative UI Was Not Properly Localized (173072)

Symptom:

When installing the Administrative UI on a French OS and accessing with a browser with locale in English, some part of the login page was in French. Everything is required to bein English.

Solution:

This is no longer a problem.

Star issue: 21480703-01

The Policy Server Was Randomly Failing (172992)

Symptom:

Th Policy Server was randomly failing in a customer environment. The core dump analysis verified that the failure was due to inappropriate data casting while printing the error logs.

Solution:

This issue is not longer a problem.

Star issue 21467303;1.

Wrong Location for jar files in shfedimport.sh (172882)

Symptom:

When we ran the smfedimport.sh, we got a java.lang.NoClassDefFoundError. We noticed the java script calls for certain jar files in the /opt/software/ca/siteminder/bin/thirdparty/ location but they are actually located in /opt/software/ca/siteminder/bin/endorsed.

Solution:

The location of the jar files is now correct.in the script.

Star issue 21476994-1.

Using Custom Authentication Scheme Results in Memory Leak (172871)

Symptom:

Using a custom authentication scheme results in a memory leak in the Policy Server.

Solution:

This is no longer an issue.

STAR Issue: 21411442;2

Error in Authentication REST Interface Tag (172762)

Symptom:

The end tag of the login responses for the Authentication REST Interface had a blank space.

Solution:

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

STAR Issue: 21467829;1

Slow PS Response When Modifying ACO Objects (172272)

Symptom:

When users modified an ACO, they experiences a 7-10 minutes lag before the Administrative UI displayed the final “task completed” message.

Solution:

This issue has been corrected.

Star issue 21437423-1.

Identity Mapping Not Working (172128)

Symptom:

The identity mappings between LDAP or ODBC directories and the custom directories are not working.

Solution:

This is no longer an issue.

STAR Issue: 21452663-1

Web Agent or Web Agent Option Pack Failed to Start (172124)

Symptom:

When first policy server listed in HCO is down, the web agent or web agent option pack did not start or initialize. When there are multiple policy servers defined in HCO, with Failover option NO, and the first policy server in the list is down, then WA or WAOP is not connecting to any other PS and not initialized.

Solution:

This is no longer a problem.

Star issue 21450634-1

Test Tool Basic Playback Mode does not work if Policy Server is running in FIPS only Mode (154109)

Symptom:

If the Policy Server is running in FIPS only mode, then the Basic Play Back Mode of the CA SiteMinder® Test Tool does not work correctly.

Solution:

This is no longer an issue. The Test Tool has been fixed. A new topic added to the SiteMinder Test Tool chapter in the *Policy Server Configuration Guide*: "How to Use the Test Tool in a FIPS-only Environment."

STAR issue: 20890864-1

Error in Processing Active Expression

Symptom:

CA SiteMinder® was throwing an error when retrieving a web services variable. The error in smtracedefault.log was: "Failed with error 'SmJavaAPI: Expression evaluation returned a null."

Solution:

This problem has been corrected.

Star issue: 21392046

Exception When Editing Users in SAML SP Object

Symptom:

When attempting to edit an existing user entry within a SAML Service Provider Object, the Administrative UI encounteredd an exception. This exception was seen after importing a policy store from V6.

Solution:

This is no longer an issue.

Star issue: 21399289-1

Administrative UI Console Was Missing Entire Section

Symptom:

The Administrative UI console was missing an entire section of "user attribute" for custom directory setup.

Solution:

This is no longer an issue.

Star issue: 21406240-1

Entity Type Changes from Remote IDP to Remote SP During Import (170262)

Symptom:

When trying to import metadata having multiple entities, the first entity in the list is imported rather than the one that is selected.

Solution:

This is no longer an issue.

STAR Issue: 21386774-1

Missing Authentication Authorization Web Service Default Settings Template in Administrative UI

Symptom:

The documentation for this web service referenced the AuthAzServiceDefaultSettings template ito create a new ACO, but it did not yet exist.

Solution:

A template is now available. The documentation has been corrected to correspond with the template.

Star issue: 21388970-1

Policy Server not Rolling Logs (170020)

Symptom:

The customer was unable to get their logs to roll automatically, which was causing the policy server to become non-operational.
The process never crashed. It only failed to operate properly when the log file got to 2 GB in size.

Solution:

This is no longer an issue.

Star issue: 21349366-1

Bad Search Filter Error (169127)

Symptom:

When you import a policy server using XPSimport, a bad search filter error is displayed.

Solution:

This is no longer an issue.

STAR Issue: 21329382-1

Unable to Edit SQL Entry within a Policy

Symptom:

The Policy User tab lists the user policy objects for the SQL ODBC users. When the user clicked on the edit icon in modify mode, the user was unable to edit.

Solution:

This is no longer an issue..

Star issue: 21148478;3

Default Values of ACO Parameters in Web Agent Configuration Guide Unclear (155294)

Symptom:

The defaults values for the BadFormChars, BadCssChars, and BadUrlChars ACO parameters in the *Web Agent Configuration Guide* are not clear.

Solution:

This is no longer an issue. The *Web Agent Configuration Guide* has been updated.

STAR Issue: 20933042-1

CA SiteMinder® Agent for JBoss Guide Provides Incorrect Directions for UNIX Environment Settings (165866)

Symptom:

The "Set the JBoss Environment on UNIX" topic in the CA SiteMinder® Agent for JBoss Guide incorrectly states that JBOSS_CLASSPATH entries should be separated using a semicolon (;).

Solution:

This is no longer an issue. The guide has been updated to show the use of a colon (:) to separate JBOSS_CLASSPATH entries.

STAR issue: 21264939-01

List of Required Linux Libraries in Policy Server Installation Guide is Incomplete (169240, 169427)

Symptom:

The topic "Required Linux Libraries" in the Policy Server Installation Guide does not contain all the libraries that are necessary.

Solution:

This is no longer an issue. The documentation has been updated.

STAR issue: 21343328-04

The Policy Server Configuration Guide Contains Incorrect Information About Impersonation Scheme Prerequisites (PROD00172378)

Symptom:

The topic "Impersonation Scheme Prerequisites" in Chapter 9 of the Policy Server Configuration Guide incorrectly states that smauthimpersonate.dll (Windows) and smauthimpersonate (UNIX) are installed with the Web Agent. These files are actually installed on the Policy Server.

Solution:

This is no longer an issue. The documentation has been updated.

STAR issue: 21467135;1

Administrative UI Linux Prerequisite Information in Policy Server Installation Guide Needs Consolidation (171403)

Symptom:

Different Administrative UI Linux requirements are included in two chapters in the *Policy Server Configuration Guide.*

Solution:

This is no longer an issue. The Linux requirements have now been consolidated.

STAR issue: 21436925-1

Additional Information About Bulk Loading Audit Data ODBC Database Required in Policy Server Administration Guide (159529)

Symptom:

The *Policy Server Administration Guide* should state that the Enable bulk load option in the ODBC Oracle Wire Protocol Driver Setup dialog must not be set when importing audit data into an Oracle database using the -b option.

Solution:

This is no longer an issue. The documentation has been updated.

STAR issue: 21045785-

Addition of the OpenID Authentication Plug-in

Symptom:

The OpenID Authentication scheme requires a new plug-in for web servers that are doing authentication.

Solution:

The plug-in has been incorporated into CA SiteMinder®.

Star issue:20777360;1

Chapter 14: Documentation

This section contains the following topics:

CA SiteMinder® Bookshelf

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

- Use a single console to view all documents published for CA 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 CA 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 15: Platform Support and Installation Media

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. Log in to the CA Support site.
2. Locate the Technical Support section.
3. Enter CA SiteMinder® in the Product Finder field.

   The CA SiteMinder® product page appears.
4. Click Product Status, CA SiteMinder® Family of Products Platform Support Matrices.

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

Locate the Bookshelf

The CA 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 CA SiteMinder® in the Select a Product Page field and press Enter.

   The CA SiteMinder® product page appears.

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

   The CA SiteMinder® bookshelf main page appears.

Locate the Installation Media

You can find the installation media on the Technical Support site.

Follow these steps:

1. Log in to the CA Support site.
2. Locate the Technical Support section.
3. Click Download Center.
4. Locate the Support by Product section.
5. Type **CA SiteMinder®** in the Select a Product Page field, and then press Enter.
6. Click Downloads.

   The Download Center screen appears.
7. Enter **CA SiteMinder®** in the Select a Product field.
8. Select a release from the Select a Release drop-down list.
9. Select a Service Pack from the Select a Gen Level drop-down list.
10. Click Go.

    The Product Downloads screen appears. All CA SiteMinder® installation executables are listed.

Appendix A: Third–Party Software Acknowledgments

CA SiteMinder® incorporates software from third–party companies. For more information about the third–party software acknowledgments, see the CA 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 CA SiteMinder®.

Product Enhancements

CA 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

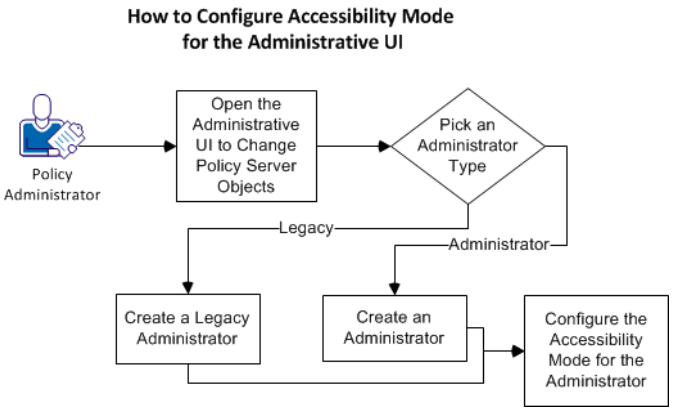
The following table lists the keyboard shortcuts that CA SiteMinder supports:

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

How to Configure the Accessibility Mode for the Administrative UI

CA SiteMinder® is a web-based product. The product can be configured to be accessible.

The following graphic describes how to configure the accessibility mode for the Administrative UI:



Follow these steps:

1. Open the Administrative UI to change the Policy Server objects (see page 149).
2. Pick an administrator type (see page 149) (from the following list):
   - Create an administrator (see page 150).
   - Create a legacy administrator (see page 151).
3. Configure the accessibility mode for the administrator (see page 152).

Open the Administrative UI to Change Policy Server Objects

Change the objects on your Policy Server by opening the Administrative UI.

Follow these steps:

1. Open the following URL in a browser.

   `https://host_name:8443/iam/siteminder/adminui`

   host_name

   Specifies the fully qualified Administrative UI host system name.

2. Enter your CA SiteMinder® superuser name in the User Name field.
3. Enter the CA SiteMinder® superuser account password in the Password field.

   Note: If your superuser account password contains dollar-sign ($) characters, replace each instance of the dollar-sign character with $DOLLAR$. For example, if the CA SiteMinder® superuser account password is $password, enter $DOLLAR$password in the Password field.
4. Verify that the proper server name or IP address appears in the Server drop-down list.
5. Select Log In.

Pick an Administrator Type

The following types of administrators are available:

- The administrators who have their accounts and credentials that are stored in an external third-party database outside of the product.
- The legacy administrators who have their accounts and credentials that are stored inside the policy store.

Any type of administrators can be configured to use the accessibility mode. However, to create administrators, an external database must be configured first.

Pick *one* of the following administrator types for which you want to configure the accessibility mode:

- Administrator (see page 150)
- Legacy Administrator (see page 151)

Create an Administrator

You create a legacy administrator in the Administrative UI. This legacy administrator uses the accessibility mode of CA SiteMinder®.

Follow these steps:

1. Select Administration, Administrator.
2. Select Administrators.

   The Administrators page appears.
3. Select Create Administrator.

   The Create Administrator page appears.
4. Select Lookup under General.

   The Select a User page appears.
5. Specify search criteria and Select Search.

   Users matching the specified criteria appear.
6. Select the administrator that you want and pick Select.

   The full name of the user appears in the Name field. The URL to the user in the external store appears in the User Path field.
7. Select Submit.

   The administrator is created and a confirmation message appears.
8. Configure the accessibility mode for this administrator (see page 152).

Create a Legacy Administrator

You create a legacy administrator in the Administrative UI. This legacy administrator uses the accessibility mode of CA SiteMinder®.

Follow these steps:

1. From the Administrative UI, select Administration, Administrator, Legacy Administrators.
2. Select Create Legacy Administrator.
3. Verify that the following option button is selected:

   `Create a new object of type Legacy Administrator`
4. Select OK.

   The Create Legacy Administrator screen appears.
5. Select the Name field, and then enter a user name of the Legacy Administrator.
6. Verify that the following option button is selected:

   `SiteMinder database`
7. Select the Password field and type a password for the Legacy Administrator.
8. Select the Confirm Password and type the same password that you used in Step 7.
9. Select the following option button:

   `System`
10. Select Submit.

    The administrator is created and a confirmation message appears.
11. Configure the accessibility mode for this administrator (see page 152).

Configure the Accessibility Mode for the Administrator

Configure the accessibility mode for the administrator after creating it.

Follow these steps:

1. From the Administrative UI, select Administration, Administrator, Administrators.
2. Select the edit icon to the right of the legacy administrator to which you want to configure the accessibility mode.

   The Modify Administrator screen appears.
3. Select the following check box:

   `GUI Allowed`
4. Select Add.

   The Create Permission screen appears.
5. Configure the accessibility mode by doing the following steps:

   a. On the Create Permission screen, select the check boxes of the items that are shown in the Security Category column of the following table:

Security Category	V	M	X	B	R	P
Admin Administration	X	X				
Agent Administration	X	X				
Agent Type Administration	X	X				
Application Administration	X	X				
Application Role Administration	X	X				
Authentication Administration	X	X				
Directory Administration	X	X				
Domain Administration	X	X				
Expression Administration	X	X				
Global Policy Administration	X	X				
Host Administration	X	X				
Legacy Domain Administration	X	X				
Mapping Administration	X	X				
Password Policy Administration	X	X				
Policy Administration	X	X				
Report: Activity by User			X			

Security Category	V	M	X	B	R	P
Report: Admin Operations			X			
Report: Applications			X			
Report: Applications by User			X			
Report: Denied Authorizations			X			
Report: Denied Resources			X			
Report: Policy by Role			X			
Report: Protected Resources			X			
Report: Resource Activity			X			
Report: Resources by User			X			
Report: Roles by Application			X			
Report: Roles by Resource			X			
Report: Users by Resource			X			
Report: Users by Role			X			
User Administration	X	X				
Variable Administration	X	X				

b. After all of the check boxes corresponding to the Security Category column are selected, select OK.

   The Create Permission closes and the permissions that you selected appear on the Modify Administrator page.

c. Select the check boxes for the permissions columns (V, M, and X) as shown in the previous table.

6. Select Submit.

   The accessibility mode is configured and a confirmation message appears. Any administrators who require the accessibility mode can use this administrator account to access the Administrative UI.