CA SiteMinder® Secure Proxy Server

Release Notes

12.52 SP1

ca technologies

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Documentation Changes

The following documentation updates have been made since the last release of this documentation:

- New and Changed Features—This chapter describes the support for the authentication and authorization web services and new language settings, and changes to configuration of SSL.
- The following Known Issue was removed as it is either fixed or no longer apply in this update:
  - Performance Effect of FIPS ONLY Mode

Contents

Chapter 1: Secure Proxy Server Release Notes

This section contains the following topics:

Operating System Support

The prerequisites for running the SPS differ based on the server platform. Prerequisites pertain to the system on which you will run the SPS, not the destination servers to which the SPS will route incoming requests.

For detailed information about platform support, you can refer to the SPS Platform Support Matrix at http://ca.com/support.

System Requirements

To run the SPS your system must have at least 256 MB of RAM and 400 MB of free hard disk space.

Installation and Upgrade Notes

Installation and upgrade procedures for this release of CA SiteMinder® Secure Proxy Server are in the *Secure Proxy Server Administration Guide.*

Note: If you interrupt an uninstallation of the SPS, some of the files previously installed may not be removed. After uninstalling the SPS, navigate to the installation directory and manually remove any remaining files.

Java JDK Installation Requirement

The operating environment where you intend to install the CA SiteMinder® SPS must have Java JDK 1.6.0_32 or later already installed.

Documentation

Updated documentation for this product is available at http://ca.com/support.

The documentation, in bookshelf format, includes:

- CA SiteMinder ® Secure Proxy Server Administration Guide
- CA SiteMinder ® Secure Proxy Server Release Notes

Note: This documentation refers to CA SiteMinder Secure Proxy Server as SPS.

Technical Support

For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Technical Support at http://ca.com/support.

Chapter 2: New Features

New Feature for r12.52 SP1

CA SiteMinder® SPS now supports the Citrix NetScaler SDX appliance. CA SiteMinder® SPS is delivered as an appliance which contains the CA SiteMinder® SPS software and the operating system files that are required to work on NetScaler SDX. You can provision an instance of CA SiteMinder® SPS using the NetScaler SDX UI.

Note: For more information, see the Implementing section in the CA SiteMinder® documentation platform.

Chapter 3: Changed Features

Upgrade of OpenSSL

CA SiteMinder® SPS uses OpenSSL 0.9.8za to fix the following vulnerabilities:

- CVE-2014-0224: An SSL/TLS MITM vulnerability exists in OpenSSL 0.9.8y and earlier. An attacker using a carefully crafted handshake can force the use of weak keying material in OpenSSL SSL/TLS clients and servers. This can be exploited by a Man-in-the-middle (MITM) attack where the attacker can decrypt and modify traffic from the attacked client and server.
- CVE-2014-0221: DTLS recursion flaw exists in OpenSSL 0.9.8y and earlier. By sending an invalid DTLS handshake to an OpenSSL DTLS client, the code can be made to recurse, eventually crashing in a DoS attack.
- CVE-2014-3470: Anonymous ECDH denial of service flaw exists in OpenSSL 0.9.8y and earlier. OpenSSL TLS clients enabling anonymous ECDH ciphersuites are subject to a denial of service attack.
- CVE-2014-0076: Fix for the attack described in the paper "Recovering OpenSSL ECDSA Nonces Using the FLUSH+RELOAD Cache Side-channel Attack".

For more information about the vulnerabilities, see the OpenSSL documentation set.

Chapter 4: Defects Fixed in 12.52 SP1

STS Failure (183516)

Symptom:

The r12.52 SPS STS deployment xsd files, like soap12.xsd, have imported xml.xsd, which requires outbound internet access. The request filas with a 500 error displayed in the browser.

Solution:

This problem has been corrected.

Star issue 21735111-01

Resolution of RFI: MBCS URL Support (181151)

Symptom:

In RFI #179239, customer asks whether SPS 12.51 and later supports serving requests to MBCS url in the backend server.

Solution:

The answer is yes, and the SPS Guide has been updated to provide this information.

Star issue 21614120-1

User Was Unable to Configure Or Remove CAAdvancedAuthDSN (181778)

Symptom:

The user was unable to configure or remove CAAdvancedAuthDSN that was created after running the SPS 12.52 configuration wizard.

Solution:

This problem has been corrected.

Star issue 21663206-1

The http_connection_timeout Parameter Was Not Working (181742)

Symptom:

In r12.5 and above, the is not honoring the value passed into the http_conenction_timeout parameter.

Solution:

This problem has been corrected.

Star issue 21695829

SPS 12.51 Exhibited Different Behavior in Different Browsers (178748)

Symptom:

The customer was unable to get application to work properly on all browsers.

Solution:

This problem has been corrected.

Star issue 21577929-1

SPS Returned Wrong HTTP Response Value (177085)

Symptom:

When the WebAppClientResponse parameter of the SPS ACO was set to return code as 403, or any other value, SPS was setting return code of http response as 200 instead of the value specified.

Solution:

This problem has been corrected.

Star issue 21467829;1

The Support of STS Web Service is Unclear (70462)

Symptom:

The STS web service content is not clear that it is supported only with Office 365.

Solution:

The CA SiteMinder® SPS documentation is updated to clarify the support.

STAR issue: 21813719-01

Unable to Install CA SiteMinder® SPS as a Non-root User (63021, 55654)

Symptom:

I am unable to install CA SiteMinder® SPS as a non-root user on Linux.

Solution:

The CA SiteMinder® SPS is updated to mention that users must have write permission on the /opt/etc/CA directory on Linux.

STAR issue: 21718443-01, 21698958-01

The Example Value of xmlns:nete is Incorrect (55916)

Symptom:

The example that is documented in xmlns:nete does not match the value that is provided in proxyrules.xml.

Solution:

The CA SiteMinder® SPS documentation is updated to mention the value as provided in proxyrules.xml.

STAR issue: 21754567-02

The Logout Request URI of Authentication Rest Interface is Incorrect (55904)

Symptom:

The documented URI for the logout request in the Authentication Rest Interface is incorrect.

Solution:

The CA SiteMinder® SPS documentation is updated to mention the correct URI.

STAR issue: 21755360-01

The Supported OpenSSL Version is Vulnerable (55897)

Symptom:

The OpenSSL version that is supported is vulnerable to attacks.

Solution:

CA SiteMinder® SPS is upgraded to use OpenSSL 0.9.8za.

STAR issue: 21771635-1

http_connection_timeout Fails to Work (55594, 55865)

Symptom:

The http_connection_timeout parameter is not working in CA SiteMinder® SPS Release 12.5 and later.

Solution:

The documentation is updated to inform that if you configure the -Dhttp_connection_timeout parameter in the SmSpsProxyEngine.properties file during initiation, the value of -Dhttp_connection_timeout precedes the value of http_connection_timeout.

STAR issue: 21695829-01

The SPSTrace Log File Does Not Contain Detailed Logs (55857)

Symptom:

The log message in the SPSTrace file does not contain detailed debugging information though the debug logging on proxy rules is enabled.

Solution:

This issue is resolved.

STAR issue: 21752386-01

The Path to the Lib Directory is Incorrect (55780)

Symptom:

The path to lib directory in Tomcat is documented incorrect.

Solution:

The CA SiteMinder® SPS documentation is updated to mention the correct path to the lib directory.

STAR issue: 21730064-01

Unable to Mask Host Headers in Filters (55713)

Symptom:

Unable to mask the host header of a group of filters.

Solution:

This issue is fixed.

STAR issue: 21690324-01

The Default Values of server.conf File Must be Updated (55630)

Symptom:

The default value of the following parameters in server.conf must be updated to suit most commonly used production values:

- enablecachepostdata
- ajp13.max_threads
- http_connection_pool_max_size
- http_connection_timeout
- http_connection_stalecheck
- http_connection_pool_min_size
- http_connection_pool_incremental_factor
- httpd.conf access_log

Solution:

The default values are updated in server.conf.

STAR issue: 21652689-01

Unable to Upload File to an Application (54141)

Symptom:

While trying to upload a file through CA SiteMinder® SPS to an application, an internal server error message is displayed.

Solution:

This is no longer an issue.

STAR issue: 21474835

WebAppClientResponse Parameter Value Changes Automatically (54375)

Symptom:

When the WebAppClientResponse parameter is set to return code as 403 or any other value, CA SiteMinder® SPS sets the return code of http response as 200 instead of the value specified.

Solution:

This is no longer an issue.

STAR issue: 21467829-01

Chapter 5: Defects Fixed in 12.52

Server 500 Error while Accessing the SPS User Interface (178615)

Symptom:

The SPS was formerly protected using a form-based authentication scheme. This method worked with r12.5. However, with r12.51 using this method caused a server 500 error.

Solution:

This issue is no longer valid in12.52 because the installer protects the UI by default. The existing protection topic is updated with the new procedure.

Star issue 21482778-1.

Updates to SPS Documentation (178610)

Symptom:

The SPS documentation required be corrected for the configuration of SPS AdminUI (r12.51).

Solution:

The documentation has been fixed indirectly ecause the Ui has been updated in r12.52.

Star issue 21595300-1.

The Secure Proxy Server Failed to Mask the Destination URL (177119)

Symptom:

The Secure Proxy Server was failing to mask the destination application URL even after using the the following Forward rule.
proxy_rules.xml :
<nete:case value="/ucmepp/">
<nete:forward filter="UCM">
" target=_blankhttp://xt99s.na.ko.com:16183/ucmepp/$1</nete:forward>
</nete:case>

Solution:

This problem is fixed.

Star issue 21468512-1.

SAMLDataPlugin Was Missing in SPS Install (174197)

Symptom:

SAMLDataPlugin was not included in the SPS Installation. This plug-in is required for HTTP Header Redirect Mode to work.

Solution:

The plug-in is now included in the SPS installation.

Administrrative User Inferface URL Not Clear

Symptom:

The URL to launch the Administrative User Interface did not specify that the Tomcat port has to be specified with the fully qualified host name.

Solution:

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

STAR Issue: 21482552-1

Protect the Administrative User Interface Documentation (173062)

Symptom:

The procedure to protect the Administrative User Interface (UI) has an error.

Solution:

This is no longer an issue. In this release, the Administrative UI is protected as part of the installation.

STAR Issue: 21482512-1

Extra Space in Closing TAG (172764)

Symptom:

The CA SiteMinder Web Services Scenarios Guide, Authentication REST Interface section for the authentication web service logout request" had a space in the closing TAG.

Solution:

The space has been removed.

Star Issue 21467829;1

Extra Space in TAG Name (172760)

Symptom:

The CA SiteMinder Web Services Scenarios Guide,, Authentication REST Interface section on page 15 had a space shown in the value for the LoginResponse.authenticationResponses.response.name TAG.

Solution:

The extra space was removed.

Star issue 21467829;1.

Mismatched TAGS in Web Services Document (172758)

Symptom:

The CA SiteMinder Web Services Scenarios Guide, Authentication REST Interface, Login Response section had mismatched TAGS for an HTTP return code 200.

Solution:

The documentation has been corrected.

Star issue 21467829;1.

SPS Displays Destination Application URL (172522)

Symptom:

SPS r12.5 does not mask the destination application URL even when the forward proxy rules are used.

Solution:

This is no longer an issue. The filteroverridepreservehost parameter has been added to the server.conf file.

Note: For more information, see the *Administration Guide*.

STAR Issue: 21468512-1

HTTP Headers Redirect Mode Was Not Working for SPS (172422)

Solution:

HTTP Headers Redirect were not working.

Symptom:

This problem has been corrected. The attribute data appears in the headers as appropriate.

SPS Start-up Problem

Symptom:

The customer was seeing the following error:

```
*** glibc detected *** /apps/java/jdk1.6.0_43/bin/java: double free or corruption
(!prev): 0x09107de8 ***
======= Backtrace: =========
/lib/libc.so.6[0x2b99a1]
/lib/libc.so.6[0x2bc0e1]
/usr/lib/libstdc++.so.6(_ZdlPv+0x22)[0xa0394df2]
/usr/lib/libstdc++.so.6(_ZdaPv+0x1e)[0xa0394e4e]
/apps/secure-proxy/agentframework/bin/libSPS60Agent.so(_ZN13CSmNamedMutex20GetDef
aultServerPathEv+0xf7)[0xa1aa2e43]
```

Solution:

This is no longer an issue:

Star issue: 21374490-1

Chapter 6: Product Limitations

SAML 2.0 Features that Cannot Be Used with the Simple URL Session Scheme

The following features do not work when the simple_url session scheme is configured for the SPS:

- Allow/Create Feature

  As part of a single sign-on request, a Service Provider may request a particular user attribute to be included the assertion; however, the value of the required attribute may not be available in the user record at the Identity Provider.

  If the Service Provider's request includes the Allow/Create attribute and the Identity Provider is configured to create a new identifier, the Policy Server at the Identity Provider will generate a unique value as part of the NameID. This value is then included in the assertion that is sent back to the Service Provider.

  When using the SPS, the SAML 2.0 Allow/Create functionality fails with the simple_url session scheme on Service Provider side. However, the Allow/Create feature does work with the default session scheme.

- Single Logout

  The SAML 2.0 single logout feature is not supported when the SPS is configured to use simple_url session scheme. However, single logout does work with the default session scheme.

- Use of the SiteMinder sample_application.jsp file for IdP-initiated SSO

  SiteMinder supports the use of a custom web application to supply user attributes to the SiteMinder Single Sign-on service. The SiteMinder-provided sample web application, sample_application.jsp, cannot be used if a simple_url session scheme is configured for the SPS at the Identity Provider.

For more information about these SAML 2.0 features, see the *CA SiteMinder Federation Security Services Guide*.

POST Preservation Issue with Transfer-Encoding Header

The SPS has a limitation for post preservation support with Transfer-Encoding chunked header.

For chunked data to be sent from the SPS to a protected resource, the user should be authenticated and have an established session. The SPS does not challenge a user for credentials in response to a request where chunked data is sent via a POST.

When using proxy filters for accessing the request or response data, the request or response is no longer sent in a chunked format. The entire request or response body is buffered within SPS and sent in a non-chunked or content-length based format.

Large File Handling Limitation

The SPS handling of large files is limited by system resources, memory, and JVM.

If pre-filters or post-filters access a request or response body, the SPS does not use large file-handling block size. The SPS buffers the entire request or response body.

Filter and Group Filter Name Restrictions

The following limitations affect group filters or filters definitions:

- Group filters should be defined using valid and existing filter names, otherwise the SPS may not process the request.
- The groupfilter name should be unique. If one or more groupfilters share the same name, the last groupfilter will overwrite the other groupfilters.

The groupfilter names and filter names should be different. You cannot use the same names for group filter names and filter names. If the filter names and groupfilter names are the same, the results may be unpredictable.

SPS Federation and Security Zones

A Secure Proxy Server that is deployed as a federation gateway cannot support SSO security zones when using multiple virtual hosts.

Chapter 7: Limitation for SAML 1.1 Transactions

SAML 1.1 transactions work with an authentication scheme that uses Active Directory configured with an LDAP namespace as the user directory.

Chapter 8: Documentation

This section contains the following topics:

Known Issues

The known issues of the following CA SiteMinder® components are confidential and are no longer included in Release Notes:

- Policy Server
- Web Agent
- SDK
- Federation
- Web Services Security
- CA SiteMinder® SPS

To view the known issues, perform the following steps:

1. Click Release Notes in the bookshelf main page.
2. Click Confidential Content against Known Issues and log in to CA Support Online.

Changes to the Administration Guide

The following changes are made to the documentation set:

- The Administration Guide content is structured based on tasks such as Installing, Configuring.
- To facilitate better user experience on our new platform, the Online Help content of administrating CA SiteMinder® SPS using Administrative UI is merged with the Administration Guide content of administrating CA SiteMinder® SPS using backend files. The new content is available in Administration Guide, Configuration Methods of CA SiteMinder® SPS. The following changes are done as a result of this task:
  - The Online Help content that is embedded in Administrative UI is not updated with the new content and is still accessible through the Help option in Administrative UI. It contains content that describes how to administer CA SiteMinder® SPS using Administrative UI. However, the Online Help content is no longer delivered through the bookshelf.
  - The Configure the Proxy Rules and Create Virtual Hosts scenarios are now delivered as task based content. You can find the content in Configuration Methods of CA SiteMinder® SPS.

Chapter 9: Acknowledgements

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

Appendix A: 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