CA SiteMinder® Secure Proxy Server

Release Notes

Release 12.5

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 in r12.5—This chapter describes the features of the administrative user interface, group configuration, multiple instances of SPS, custom error pages, enhanced proxy rules, updated logger configuration for server.log, SessionLinker, Integrated Windows Authentication, SSL client certificate authentication, integration with CA Wily Introscope and support for WebDAV, SHA-2, Web Agent features, 2048-bit and 4096-bit keys, ASA, agent discovery, Policy Server, upgraded components, OneView monitor, Web agent features, and enhanced load balancing and limit incoming connections.
- The following Known Issue was removed as it is either fixed or no longer apply in this update:
  - Value for requestblocksize or responseblocksize Parameters

Contents

Chapter 1: General Release Information

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 SPS must have Java JDK 1.6.0_30 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

This section contains the following topics:

Administrative User Interface

The SPS provides a user interface for administering the various features of the SPS. The Online Help for the Administrative UI is provided as scenarios.

You can use the Administrative user interface to perform the following tasks:

- Manage proxy rules
- Manage session schemes settings
- Manage user agents settings
- Manage virtual hosts settings
- Manage session store settings
- Manage federation settings
- Manage proxy service settings
- Manage Tomcat settings
- Manage Apache settings
- Manage log settings
- Manage SSL settings
- Manage custom error pages settings
- Manage group configuration settings

For information about using the administrative user interface, see the *Online Help*.

Group Configuration

Group configuration lets you perform a central configuration of multiple SPS hosts configured to a Policy Server at a time. If you group the hosts configured to a Policy Server, you can manage the configuration of the hosts servers using any host in the group.

For information about group configuration, see the *Online Help*.

Important! The group configuration feature is not supported on CA SiteMinder Release 6.0 and Release 12.0. The support for the group configuration feature will be available only from the cumulative releases (CRs) starting from CA SiteMinder Release 12.5 CR 1 Policy Server.

Support for Multiple Instances

You can install multiple SPS instances on the same computer. Each SPS instance uses a unique instance name and ports for communication, and creates a separate directory structure.

For information about installing multiple instances of SPS, see the *SPS Administration Guide*.

Custom Error Pages

The SPS supports the custom error pages feature, which lets you customize the error pages that the Web Server displays when a client request fails.

For information about using custom error pages, see the *SPS Administration Guide* and *Online Help*.

Support for the Web Distributed Authoring and Versioning Protocol

The SPS supports Web Distributed Authoring and Versioning (WebDAV) protocol.

SHA-2 Support

The SPS provides support for the SHA-2 family of one-way hash functions in SAML 2.0 assertions.

Support for SessionLinker

The SPS supports SessionLinker functionality that is similar to the functionality of an ERP SessionLinker.

For information about using SessionLinker, see the *SPS Administration Guide.*

Support for Web Agent Features

SPS supports all features of a Web agent.

For information about Web agent, see the CA SiteMinder r12.5 bookshelf.

Support for 2048 Key Support

The SPS supports the 2048-bit and 4096-bit asymmetric keys in encryption.

Support for Application Server Agent

You can use Application Server Agents with the SPS instead of a web agent.

Limit Incoming Connections

You can configure Apache to limit the number of incoming connections to SPS.

Agent Discovery

The SPS lets you discover a SPS agent and display the SPS agent details.

Support for OneView Monitor

The SPS supports integration with OneView Monitor that lets you monitor the data performance of the SPS web agent.

Support for SSL Client Certificate Authentication

You can configure SPS to support SSL client certificate authentication between SPS and backend web server.

For information about SSL client certificate authentication, see the *SPS Administration Guide* and *Online Help*.

Support for Wily Introscope

The SPS supports integration with CA Wily Introscope that lets you monitor the data performance of the SPS and SPS web agent.

For information about data monitoring using CA Wily Introscope, see the *SPS Administration Guide*.

Policy Server support

The SPS supports the following versions of the Policy Server:

- CA SiteMinder Release 12.5
- CA SiteMinder Release 12.0 SP3 CR10
- CA SiteMinder Release 6 SP6 CR08
- CA SiteMinder Release 6 SP5 CR35

Upgraded Components

The SPS supports the following updated components:

- Tomcat 7.0.27
- Apache 2.2.22
- HttpClient 4.1
- OpenSSL 0.9.8x
- log4j 1.2.8
- JDK 1.7

Support for Integrated Windows Authentication

The SPS supports the Integrated Windows Authentication (IWA) to access SiteMinder protected resources.

For information about supporting IWA, see the *SPS Administration Guide.*

Chapter 3: Changed Features

This section contains the following topics:

Enhanced Load Balancing

The SPS supports load balancers that improve resource utilization and decrease request computing time.

Enhanced Proxy Rules

The proxy rules are enhanced to support new conditions that are based on cookie existence, cookie value, and header existence.

For information about configuring proxy rules, see the *SPS Administration Guide* and *Online Help.*

Updated Logger Configuration for server.log

SPS uses the logger.properties file to manage the log settings. the server.conf file no longer contains log settings.

For information about log settings, see *SPS Administration Guide* and *Online Help*.

Chapter 4: Known Issues

This section contains the following topics:

Starting SPS on Solaris 10 Systems

There is a known problem with Apache that can prevent SPS from starting on Solaris 10 systems when an SSL connection is being used.

After registering SPS with the Configuration Wizard, the Apache Virtual Host directive $NETE_SPS_ROOT/httpd/conf/httpd-ssl.conf is set shown following:

```
##
## SSL Virtual Host Context
##
<VirtualHost _default_:443>
```

For Solaris 10 systems we recommend using the IP address of the machine instead of _default_.

Startup Error in SSL Mode on Windows

When enabling SPS for SSL mode on Windows you can possibly see the following error:

```
C:\Program Files (x86)\CA\secure-proxy\httpd\bin>configssl.bat -enable
Reconfiguring the SiteMinder Secure Proxy service
The SiteMinder Secure Proxy service is successfully installed.
Testing httpd.conf....
Errors reported here must be corrected before the service can be started.
Syntax error on line 62 of C:/Program Files (x86)/CA/secure-proxy/httpd/conf/ext
ra/httpd-ssl.conf:
SSLSessionCache: Invalid argument: size has to be >= 8192 bytes
```

This error occurs because on 64-bit Windows environments, the 32-bit applications are installed under the Program Files (x86) folder by default. The parentheses are not allowed on Windows in folder names. Apache is aware of this issue; Apache does not have an official release for Windows 64-bit operating environments.

On 64-bit Windows environments, install the SPS at some other location, for example, the C:\CA folder.

JVM Installation Error on Solaris and Linux

When you specify the JDK path during the console mode installation of the SPS on a Solaris or Linux computer, the following error is displayed:

```
Unable to install the JVM included with this installer
```

This is a bug with InstallAnywhere 2009. The error does not affect the installation.

SSL-ID Authentication Fails with Mozilla Firefox

When you configure the SSL-ID session scheme, the SessionCreateException occurs during authentication with Mozilla Firefox. To resolve the issue, perform the following steps:

1. Open Mozilla Firefox.
2. Type about:configure in the address bar.
3. In the advanced settings, set the value of security.enable_tls_session_tickets to false.

No Support for SafeWord Server Authentication Scheme

The SPS does not support the SafeWord Server authentication scheme.

Uninstallation Error on Solaris 11

When you try to uninstall the SPS within the same user session in which you installed the SPS, the following error occurs:

```
Invocation of this Java Application has caused an InvocationTargetException. This application will now exit.
```

This issuue occurs if you have used JDK 1.7.0.1 to install the SPS on the Solaris 11 computer. To resolve the issue, open a new user session and uninstall the SPS.

No Support for Spaces in Request URLs

If a resource request contains a space in the request URL, the request fails. As a workaround, perform the following steps:

1. Open the ACO you created for SPS in the WAMUI.
2. Delete the %25 value from the BadUrlChars parameter of the ACO.
3. Save the change.

Performance Effect of FIPS ONLY Mode

When you enable the FIPS ONLY mode on SPS, the performance of SPS is affected.

The Certificate Generation Failed Exception Occurs During Upgrade

When you upgrade from SPS r6.0 or 12.0 to 12.5, the following exception occurs:

```
Certificate generation failed: Certificate contains invalid public key
```

To resolve the issue, you must perform the following steps:

1. Log on to the SPS Admin UI.
2. Navigate to Administration, SSL Config.
3. Delete the certificates with the following details:

   ```
   Serial number=00
   ```

   ```
   Issuer, Subject= Thawte Universal CA Root, Thawte Universal CA Root, Thawte
   ```
4. Save the changes.

Chapter 5: Defects Fixed

This section contains the following topics:

Fixed Defects List

The following defects are fixed in this release:

STAR Number	Issue Description
20940480-1, 20858596-1	When the proxy-rules.xml file is parsed, the javax.servlet.ServletException: Error parsing Proxy Rules file expection occurs.
20191517-1	The closing double quote (") is missing at the end of a content-type header request.
20765951-1	The communication socket of a request is closed before SPS responds to the request.
20957502-1	When the MiniCookie session scheme is used, the SMDATA cookie is not set in the web browser.
20972773-1	The connection pool messages contain unwanted messages.

Chapter 6: Product Limitations

This section contains the following topics:

Support for Japanese Characters

The Secure Proxy Server does not support Japanese characters included in URLs, host names, and proxy rules.

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.

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.

Appendix A: Acknowledgements

This appendix lists the third-party software used in SPS for which licensing agreement information has been provided. The following third-party software are used in SPS:

Note: To view the licensing agreement information for a third-party software in HTML format, click Third Party Software Acknowledgements. To view the licensing agreement information for a third-party software in text format, see the third_party_software_acknowledgements file in the \\Secure Proxy Server v12.5\Bookshelf_Files\TPSA folder.

- Apache HTTP Web Server 2.2.22
- Apache SOAP 2.3.1
- Commons beanutils 1.7
- Commons Collections 3.1
- Commons Logging Package 1.1.1
- curl 7.25.0
- EXPAT 2.0.1
- Google Protocol Buffers 2.4.1
- httpclient 4.1.2

- ICU4C 3.4
- jboss 4.0.1 SP1
- JSTL (The JSP Standard Tag Library) 1.0.6
- JWSDP 1.4
- Log4cplus 1.0.2
- Log4j 1.2.8
- MIT Kerberos V5 Release 1.5
- mod_jk 1.2.30
- myfaces 1.1.4
- openidselector 1.2
- OpenSSL 0.9.8x
- PCRE 8.1
- Tomcat 7.0.27
- Xalan-J 2.7.0
- Xerces-C 2.5.0
- Xerces-C 2.7.0
- Zlib 1.2.5

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