CA SiteMinder® Web Services Security

Release Notes

12.52 SP1

CA Technologies Product References

This document references the following CA Technologies products:

- 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 1: Welcome

This document contains information on CA SiteMinder® Web Services Security features, operating system support, installation considerations, known issues, and fixes.

Chapter 2: Web Services Security System Requirements

The following requirements must be met or exceeded to install and run correctly.

Operating System Support

Before you install any CA SiteMinder® Web Services Security components, verify that you are using a supported operating system and third-party software.

More information:

Locate the Platform Support Matrix (see page 27)

Platform Support

For a complete list of supported web servers, application servers, databases, directories, web browsers, and CA interoperability requirements, see the CA SiteMinder® Web Services Security 12.52 SP1 Platform Support Matrix.

Note: CA SiteMinder® Web Services Security extensions that were formerly only available in the CA SOA Security Manager Policy Server are now integrated into the CA SiteMinder® Policy Server. Therefore, refer to the CA SiteMinder® 12.52 SP1 Platform Support Matrix for platform support information relating to the Policy Server.

More information

Locate the Platform Support Matrix (see page 27)

SiteMinder WSS Agent Requirements

The following minimum system requirements must be met for SiteMinder WSS Agents to install and run correctly.

- **Memory**—2 GB system RAM.
- **Available disk space**:
  - SiteMinder WSS Agent for Web Servers—200 MB free disk space in the install location.
  - SiteMinder WSS Agent for Oracle WebLogic—50 MB free disk space in the install location
  - SiteMinder WSS Agent for IBM WebSphere—50 MB free disk space in the install location
  - All SiteMinder WSS Agents—200 MB of free space in the system temporary file location.

Note: For additional non–system requirements, see the corresponding SiteMinder WSS Agent Guide.

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)

Chapter 3: Web Services Security Installation and Upgrade Considerations

Compatibility with Other Products

To ensure interoperability if you use multiple products, such as SiteMinder, Identity Manager, and Federation Manager check the Platform Support Matrices for the required releases of each product.

More information:

Locate the Platform Support Matrix (see page 27)

System Locale Must Match the Language of Installation and Configuration Directories

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.

Host registration Fails When Policy Server Has a Link-Scoped IPv6 Address When Configuring SOA Agent on Linux (136734)

Linux does not support connections to link-scoped IPv6 addresses without additional information: The name of the interface on which to do the networking. This means that when registering a Linux system as a trusted host during SiteMinder WSS Agent configuration, it fails with the following error when the IP address of the Policy Server is link-scoped:

```
Registration failed (bad ipAddress[:port] or unable to connect to Authentication server (-1)).
```

Workaround

Use global or site-scoped IPv6 addresses.

r12.1 SOA Agents and 12.52 SP1 SiteMinder WSS Agents Cannot Consume SAML Session Tickets Produced by the Other Agent Version (147478)

r12.0 SOA Agents encrypt and decrypt SAML Session Tickets using the RC2 algorithm. However, 12.52 SP1 SiteMinder WSS Agents encrypt and decrypt SAML Session Ticket using the Advanced Encryption Standard (AES) algorithm by default. As a result, r12.1 SOA Agents and 12.52 SP1 SiteMinder WSS Agents cannot consume SAML Session Tickets produced by the other agent version.

To configure a 12.52 SP1 SiteMinder WSS Agent to use the RC2 encryption algorithm to exchange SAML Session Tickets with r12.0 SOA Agents, set the BackwardEncryption parameter in the XmlToolkit.properties file for that agent.

Follow these steps:

1. Navigate to one of the following locations:
   - *agent_home*\java (SiteMinder WSS Agents for Web Servers)
   - *WSS_Home**wlsagent*\config (SiteMinder WSS Agent for WebLogic)
   - *WAS_Home*\properties (SiteMinder WSS Agent for WebSphere)

   Note: The addresses that are provided are for Windows platforms. Substitute forward slashes (/) on UNIX platforms.
2. Open XmlToolkit.properties in a text editor.
3. Uncomment and modify the backwardencryption parameter line as follows:

   ```
   backwardencryption=yes
   ```

4. Save and close the XmlToolkit.properties file.
5. Restart the SiteMinder WSS Agent.

Windows Considerations

The following considerations apply to supported Windows operating environments:

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.

Required Operating System Patches on Solaris (24317, 28691)

The following table lists required and recommended patches by version:

Version	Required	Recommended
Solaris 9	■ 111722-04 or any superseding patch ■ 111711-15 or any superseding patch	none

You can find patches and their respective installation instructions at SunSolve (http://sunsolve.sun.com).

Red Hat Enterprise Linux AS and ES Considerations

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

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
   ```

Chapter 4: New Features and Changes to Existing Features

Upgrade of CAPKI

CA SiteMinder® is upgraded to use CAPKI 4.3.4 to fix the following OpenSSL 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.

Chapter 5: Defects Fixed in SOA Security Manager Releases

Web Services Security Defects Fixed in r12.52 SP1

There were no defects fixed for Web Services Security for r12.52 SP1.

Chapter 6: Web Services Security Defects Fixed in r12.1 SP3

The r12.1 SP3 release contains the following fixes.

Authentication of Encrypyted Requests Intermittently Failing with Red Hat Policy Server (77348)

Attempts by all SOA Agent types to connect to a RedHat Policy server to authenticate an encrypted request fail intermittently.

Responses Configured to Generate Signed SAML Session Tickets Using Public Key Obtained from XML Digital Signature Authentication Produce Unsigned SAML Session Tickets (98865)

Generation of *signed* SAML Session Tickets using the public key obtained from a digital signature by the XML Digital Signature authentication scheme results in the generation of an *unsigned* rather than signed SAML Session Ticket.

That is, if a web service is protected by the XML Digital Signature authentication scheme and a SAML Session Ticket response is configured to extract the client's public key from the certificate and use it to sign the SAML assertion, the generated SAML Session Ticket is *not* signed as expected.

Workaround

Configure the policy to obtain the public key from a source other than the document with the digital certificate. For example, configure the response to obtain the public key from a client certificate sent over an SSL connection or from the user store.

WS-Security SAML 1.1 Holder of Key Assertion Not Accepted More Than Once (97266)

SOA Security Manager does not accept a WS-Security SAML 1.1 holder of key assertion token more than once; SAML 1.1 holder of key tokens cannot therefore be used in use cases where replay is required.

Workaround

SAML 2.0 holder of key tokens work as expected and can be used in to implement use cases in which replay is required.

Responses Defined When Creating an Application Within Secure Web Services from WSDL Operation Are Not Immediately Usable (70468)

If you choose to create the application object that will define your security policy from within the Secure Web Services from WSDL wizard any Responses created from the Responses tab of the Create Application nested task are not displayed or available for assignment in the Define web service protection policy table.

Workaround

If you need to bind responses to web service ports and operations on the Define Policies page of the Secure Web Services from WSDL wizard, you must create the application and the required responses prior to running the wizard.

SOA Agent for IBM WebSphere Fails Under Load on Windows

Because of a memory leak in com/ibm/ws/security/auth/AuthCache, the SOA Agent for IBM WebSphere fails under load.

An IBM support ticket (PMR 30393,756,000) is open for this issue.

Error Logged During Administrative UI Install on WebLogic (74188)

When you install the CA SiteMinder® Web Services Security Administrative UI in console mode on a Weblogic Application server, a non-fatal error “ERROR - Command failed: Installing Workflow Store Data “ is written to the install log. You can ignore this error.

Chapter 7: Web Services Security Defects Fixed in r12.1 as of CR1

This r12.1 release contains the following fixes.

Variables Created in Admin UI Containing Expression Keywords as Variable Name Substrings Being Resolved Incorrectly (71976)

Symptom:

Variables created in the CA SiteMinder® Web Services Security Administrative UI which contain expression keywords (or, and, and so on) as substrings of the variable name are resolved incorrectly by the expression editor. For example a variable named "RandomVariableName" will be incorrectly converted to the name "R&omVariableName" causing the expression to be evaluated incorrectly.

Solution:

This is no longer an issue.

SOA Agent Configuration Wizard Fails to Make Necessary Configuration File Changes for SOA Agent for Apache Web Server (78481)

Symptom:

The SOA Agent configuration wizard is not making required configuration changes in the httpd.conf file or creating the required webagent.conf file, preventing the SOA Agent from starting.

Solution:

This is no longer an issue.

Installer Properties File Used for Unattended Install Contains Bad Entries for SOA Admin UI on Windows (73363)

Symptom:

In the SOA installer property file created during install (*SOA_HOME*\install_config_info\ca-soasmr12-installer.properties), required double backslashes in pathnames in entries related to the SOA Admin UI are not present. For example, rather than the following expected entry:

```
DEFAULT_NETE_JAVA_HOME = E:\\ProgramFiles\\Java\\jdk1.5.0_01
```

The following incorrect entry is written in the file:

```
DEFAULT_NETE_JAVA_HOME has value E:ProgramFilesJavajdk1.5.0_01
```

Solution:

This is no longer an issue.

Uninstalling SOA Agent for IBM WebSphere Breaks the Application Server (72302)

Symptom:

When uninstalling the SOA Agent for IBM WebSphere, the CA SiteMinder® Web Services Security uninstaller incorrectly deletes the *WS_HOME*/java/jre/lib/ext and *WS_HOME*/lib/ext directories, preventing the IBM WebSphere Application Server from running.

Solution:

This is no longer an issue.

Uninstall Does Not Remove the ETPKI Folder (72027)

Symptom:

The SOA Security Manager r12.1 uninstaller does not removing the *soa_home*\siteminder\ETPKI folder.

Solution:

This is no longer an issue.

Uninstall Does Not Remove SDK (68885)

Symptom:

The CA SiteMinder® Web Services Security does not uninstall files associated with the CA SiteMinder® Web Services Security SDK.

Solution

This is no longer an issue.

Failover to Second Policy Server in Cluster Fails for SOA Agent for Web Servers (73808)

Symptom:

The SOA Agent for Web Servers does not failover to a secondary Policy Server in a clustered environment when the primary Policy Server fails.

Solution:

This is no longer an issue.

Documentation Install Does Not Remove Older Documentation in Upgrade Scenario (74629)

Symptom:

The CA SiteMinder® Web Services Security r12.1 documentation install leaves all existing r12.0 documentation files in place when upgrading to r12.1.

Solution:

This is no longer an issue.

Chapter 8: International Support

An *internationalized* product is an English product that runs correctly on local language versions of the required operating system and required third-party products, and supports local language data for input and output. Internationalized products also support the ability to specify local language conventions for date, time, currency and number formats. CA SiteMinder® Web Services Security is an internationalized product.

A *translated* product (sometimes referred to as a *localized* product) is an internationalized product that includes local language support for the product user interface, online help and other documentation, and local language default settings for date, time, currency, and number formats. CA SiteMinder® Web Services Security is *not* a translated product.

Chapter 9: Platform Support and Installation Media

This section contains the following topics:

Locate the Platform Support Matrix

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

Follow these steps:

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

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

Technology Partners and CA Validated Products

The latest list of partners and their validated products.

Locate the Bookshelf

The 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 Web Services Security Installation Media

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

Follow these steps:

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

Chapter 10: Third-Party Software Acknowledgements

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

Chapter 11: 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.

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.

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.

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