CA SiteMinder Federation Standalone

Federation Standalone Release Notes

r12.52 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.

Contents

Chapter 1: Welcome

Welcome to CA SiteMinder® Federation Standalone. These release notes contain product installation considerations, operating system support, known issues, and information about contacting CA Technical Support.

Chapter 2: Operating System Support

For a list of supported operating systems for CA SiteMinder® Federation Standalone, refer to the Platform Support Matrix for the product.

To locate the platform matrix:

1. Log into the Technical Support site.
2. Search for the CA SiteMinder® Federation Standalone Platform Support Matrix for r12.52 SP1.

Chapter 3: New Features

New Features for r12.52 SP1

There are no new features in this release.

Chapter 4: Changed Features

Upgrade of OpenSSL

CA SiteMinder® Federation Standalone 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 5: Defects Fixed in 12.5

Protection Against XML Signature Wrapping Attacks (168095)

A malicious user can commit an XML signature wrapping attack by changing the content of a document without invalidating the signature. By default, software controls for the Policy Server and Web Agent Option Pack are set to defend against signature wrapping attacks. However, a third-party product can issue an XML document in a way that does not conform to XML specifications. As a result, the default signature checks can result in a signature verification failure.

Signature verification failures occur for the following reasons:

- A duplicate ID element is in the XML document and the signature references this duplicate ID. Duplicate ID attributes are not permitted.
- The XML signature does not reference the expected parent element, and a signature wrapping vulnerability is logged.

If a federation transaction fails, examine the smtracedefault.log file and the fwstrace.log file for a signature verification failure. These errors can indicate that the received XML document is not conforming to XML standards. As a workaround, you can disable the default Policy Server and Web Agent protection against signature wrapping attacks.

Important! If you disable the protection against signature vulnerabilities, determine another way to protect against these attacks.

To disable the XML signature wrapping checks:

1. Navigate to the xsw.properties file. The file exists in different locations for the Policy Server and the Web Agent.
   - For error messages in the Policy Server smtracedefault.log file, go to *siteminder_home*/config/properties
   - For error messages in the Web Agent fwstrace.log, go to

     *web_agent_option_pack_ home/*affwebservices/web-INF/classes.

     Note: If the web agent option pack is installed on the same system as the web agent, the file resides in the *web_agent_home* directory.

2. Change the following xsw.properties settings to true:
   - DisableXSWCheck=true (Policy Server setting only)
   - DisableUniqueIDCheck=true (Policy Server and Web Agent Option Pack setting)

     Note: The value of the DisableUniqueIDCheck setting must be the same for the Policy Server and the Web Agent Option Pack.
3. Save the file.

STAR issue: 21321479;1

Chapter 6: Defects Fixed in 12.52

Unable to retrieve the HTTP Headers (173924)

Symptom:

When using remote provisioning at the SP side with the delivery mode set as HTTP headers, the HTTP headers cannot be retrieved.

Solution:

This is no longer an issue.

STAR Issue: 21493785-1

Values for Idle and Max Cookie Timeouts Changed (173107)

Symptom:

The FEDSESSION cookie timeout settings default values changed.

Solution:

The values in the documentation have been updated.

STAR issue: 21455676-01

Asserting Party Not Accepting ACS URL in an Authentication Request (170971)

Symptom:

CA SiteMinder® Federation Standalone was not accepting and processing the Assertion Consumer Service URL in the incoming authentication request. The system did not verify whether the authentication request had an Assertion Consumer Service URL defined.

Solution:

For an IdP-to-SP partnership, the Administrative UI has a new check box labeled **Accept ACS URL in the Authnrequest**. This check box is in the SSO section of the SSO and SLO step of the partnership configuration. To confirm that the URL is present and valid in the authentication request, and it is in the metadata, select this option.

STAR issue: 21361990

Incorrect XPSExport Command Syntax for Backing Up a Configuration (173659)

Symptom:

The XPSExport command syntax specified in the following line of "Back up an Existing Configuration" is incorrect:

`XPSExport export_file_name -xa -passphrase passphrase`

Solution:

This issue has been fixed. The command syntax is now correctly stated as follows:

`XPSExport export_file_name -xe -xp -passphrase passphrase`

STAR issue: 21480783-2

User Database Configuration Failure (173170)

Symptom:

When you configured the ODBC User Directory settings after configuring an LDAP User Directory, the Connection Credentials fields are disabled.

Solution:

This is no longer an issue. The binding parameter in the UI TAG was used for the ODBC and LDAP connections. The LDAP and ODBC User Directory configuration pages now have two different bindings.

STAR issue: 21485109-1

CSR Request for Apache Web Server Wrong Size

Symptom:

Generating a CSR Request for 2048 bits for the embedded Apache web server was generating a certificate with 1024 bits.

Solution:

This is no longer an issue.

STAR issue: 21376361

Contry Drop-down List Does Not Display Values (171912)

Symptom:

The Country drop-down list in the Request Certificate page of the Administrative UI displays question mark symbols.

Solution:

This is no longer an issue.

STAR Issue: 21454397-1

SAML Authentication Scheme Fails to Authenticate (170507/173913)

Symptom:

The SAML authentication scheme does not authenticate the second user after the first user is authenticated in a different branch of the same user directory.

Solution:

This is no longer an issue.

STAR Issue: 21283896/21497645

fedmanager.sh Script Using $(logname) Instead of ${LOGNAME} (170497)

Symptom:

The fedmanager.sh script was using $(logname) instead of ${LOGNAME}. This substitution caused the script to fail when root was using 'su - fmuser' to launch the script as fmuser.

Solution:

This is no longer an issue.

STAR issue: 21399266-1

Upgrade from 12.1 SP3 to 12.5 Was Failing (169579)

Symptom:

The upgrade from 12.1 SP3 to 12.5 upgrade was failing. The following message is an excerpt from the installation log file:

```
Unable to initialize crypto subsystem Failed to open the encryption key file.
```

Solution:

This is no longer an issue.

STAR issue: 21362417-1

Flags Required in Open Format Cookie (168080)

Symptom:

The Open Format Cookie that the IWA sets do not have the following flags set:

- Secure
- HttpOnly

As a result, JavaScript can extract this cookie.

Solution:

This is no longer an issue.

STAR Issue: 21308386-2

Logging Configuration File was not Updated (171956)

Symptom:

The federation standalone product uses log4j for logging messages to the server.log file. The logger.properties file is one of the files that determines what is recorded in the server.log file. The guide did not reflect this change.

Solution:

The name and location of the logger.properties file has been updated in the documentation.

STAR issue: 21454409-1

Log4j.properties File Omitted and Incorrect SSL Command Syntax (165412)

Symptom:

The log4j.properties file is not documented. This file controls additional logging for Administrative UI operation.

The command to start the federation services with SSL was incorrectly documented.

Solution:

The log4j.properties file is now described in the information about logs that monitor federation activities.

The command to start the federation services is now correct. The command is now documented as ./fedmanager.sh startssl.

STAR issue: 21257428-1

Failover and Load Balancing Process Needs Clarifying (145146)

Symptom:

The diagrams for failover and load balancing need modifications. Also, the explanation of each function is unclear.

Solution:

Updates to the failover and load balancing pictures have been made. Also, the steps and explanations have been clarified.

STAR issue: 20533073;1

Chapter 7: Defects Fixed in r12.52 SP1

Incorrect Filename for Log File (53337)

Symptom:

The name of the nohup.out.log file had a random number instead of a proper format.

Solution:

This is no longer an issue. The file now has the following format:

`nohup.outYYYYMMDD_hhmmss.`

STAR Issue: 21454410-01

The Name of the nohup.out Log Was Set Incorrectly (172212)

Symptom:

The naming convention of nohup.out log was nohup.outxxxxxxxxxx.log(xxx is random number). The expected format was nohup.outYYYMMDD_hhmmss.

This issue was found only on Windows platforms.

Solution:

This problem has been corrected.

Star issue 21454410-01

The ñ character Made SiteMinder Searches Fail (168418)

Symptom:

Including the ñ character caused SiteMinder searches to fail. Other UTF 8 characters did not have the same effect.

Solution:

This problem has been corrected.

Star issue 21159919;1

Chapter 8: Documentation

CA SiteMinder® Federation Standalone Bookshelf

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

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

View the 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 any documentation, we recommend that you download it before beginning the installation process.

Chapter 9: 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.

A *translated* product (sometimes referred to as a *localized* product) is an internationalized product that includes local language support for the product's user interface, online help and other documentation, as well as local language default settings for date, time, currency, and number formats.

CA SiteMinder® Federation Standalone has been internationalized and localized to the extent indicated in the platform support matrix for CA SiteMinder® Federation Standalone r12.52 SP1.

Chapter 10: Third-Party Software Acknowledgements

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

Product Enhancements

CA SiteMinder® Federation Standalone 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® Federation Standalone supports:

Keyboard	Description
Ctrl+X	Cut
Ctrl+C	Copy

Keyboard	Description
Ctrl+V	Paste
Ctrl+Right	Next Word
Ctrl+Down	Scroll Line Down
End	Line End