CA SiteMinder Federation Standalone

Federation Standalone Release Notes

r12.52

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.

Chapter 3: New Features in CA SiteMinder® Federation Standalone r12.52

This section contains the following topics:

Administrative UI New Look and Feel

The CA SiteMinder® Federation Standalone Administrative UI is now refreshed to meet the CA standard for fonts, colors, icons, and images. The menu navigation for the Administrative UI has new styles but uses the familiar tab interface. The steps in the configuration wizards have a new, more colorful look. The new look improves the navigation and makes configuration tasks easier.

Social Sign-on

CA SiteMinder® Federation Standalone now lets users get access to a federated resource using their social networking credentials instead of the federation system credentials.

Social sign-on consists of the following features:

- Authentication of users using an OAuth authorization server.
- Configuration of a credential selector page that provides users with various identity providers as authentication choices.

The features are independent of each other. You can configure the federation system to implement one or both of them.

SAML 2.0 POST Binding

r12.52 supports SAML 2.0 HTTP POST binding as a method for exchanging requests and responses during authentication and single log-out requests.

Claims Transformation of Assertion Attributes

Claims transformation manipulates claims during a federated single sign-on transaction. Claims, also known as attributes, help customize the attributes and improve the user experience at a partner.

The software can perform three different modifications to assertion attributes:

- **Transformation:** Changing the value of an assertion attribute to a different value.
- **Addition:** Adding an assertion attribute if it does not exist already.
- **Deletion:** Deleting an assertion attribute on a conditional basis.

Session Store Attributes Available for Assertions

Session attributes can be persisted in the session store after a user is authenticated. From the session store, the system can add the attributes to an assertion to customize the requested application.

WS-Federation 1.2 Support

CA SiteMinder® now supports the WS-Federation 1.2 profile for partnership federation. You can configure single sign-on and sign-out using the WS-Federation profile.

WS-Federation Metadata Exchange

The Policy Server supports the Web Services Metadata Exchange profile for WS-Federation partnerships. This web service enables the CA SiteMinder® local partner to respond to requests from a remote partner for metadata. The exchange occurs as an HTTP request and response.

SAML 2.0 Attribute Query Support

A CA SiteMinder® IdP supports the SAML 2.0 Assertion Query/Request profile and can respond to attribute queries. The IdP also extends the profile functionality by accepting queries for attributes not in the assertion or in the metadata. When the IdP receives an attribute query, the IdP first checks its user directory to find the attributes. If the attributes are not found, the Policy Server checks the session store.

Note: Only the CA SiteMinder® IdP supports the query profile. A CA SiteMinder® SP as the requesting partner only supports the proxied attribute query feature.

SAML 2.0 User Attribute Retrieval from a Third-Party Identity Provider

In a SAML 2.0 federated environment, CA SiteMinder® supports a feature referred to as a proxied attribute query. The proxied attribute query is based on the SAML 2.0 Assertion Query/Request profile.

A proxied query enables the Policy Server to contact a third-party Identity Provider and request values for attributes that are not in its session store. The Policy Server can then pass the attributes back to the application at the Service Provider.

SAML 2.0 Attribute Authority Metadata

When you export metadata from a local SAML 2.0 IdP entity or an IdP-to-SP partnership, the attribute service URL is in the exported metadata. This information is relevant for local IdPs acting as an Attribute Authority, one of the roles necessary for the Attribute Query/Response profile.

Federation System Administration

Several administrators in your company can be responsible for different aspects of federation management. You can assign the administration of CA SiteMinder® Federation Standalone to multiple people in your organization to establish accountability and separation of responsibilities.

Log Enhancements to Aid Troubleshooting

The federation log files FWSTrace.log and the smtracedefault.log now contain checkpoint log messages that indicate what is happening during a transaction. You can search on these checkpoint messages to follow some of the processes occurring during a transaction.

In addition to the checkpoint messages, there are transaction IDs in the log to follow a transaction. If a transaction fails, the checkpoint messages and transaction IDs can help you determine the specific problem.

Certificate List Cross References Partnerships

In the Administrative UI, the Certificate and Private Key List for X509 certificate management now includes a Partnerships column. This column displays the federated partnerships that use each private key/certificate. The partnerships are displayed as a link. If there is only one partnership in the column, the link takes you to a filtered partnership list. The list shows only the one partnership. If there are multiple partnerships in the column, the link takes you to an unfiltered federation partnership list.

Chapter 4: Known Issues

This section contains the following topics:

Installation, Upgrade, and Performance Issues

The following topics describe issues that you can occur when installing or upgrading CA SiteMinder® Federation Standalone. Other issues are related to system performance.

Configure the Session Store Timeout for Heavy Load Conditions

Under heavy load conditions, long-running queries necessary for session store maintenance tasks, such as removing idled–out or expired sessions, can timeout. Adjust the timeout for session store maintenance tasks (60 seconds by default), by increasing the value of the MaintenanceQueryTimeout registry setting. Increase the value so that the maintenance thread can complete its tasks successfully.

The MaintenanceQueryTimeout registry setting can be found at the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\
SessionServer
```

Apache access_log is Unavailable

Symptom:

By default, CA SiteMinder® Federation Standalone does not generate access_log in the httpd.conf file.

Solution:

To generate access_log, uncomment the following line in the httpd.conf file:

```
CustomLog logs/access_log common|CustomLog logs/access_log combined
```

Console Mode Required for UNIX Systems with IPv6 Addresses (159528)

If the UNIX system where you plan to install and configure CA SiteMinder® Federation Standalone uses an IPv6 address, run the installation and configuration in only console mode. If you try to install or configure in GUI mode, the installation program defaults to console mode due to a third-party limitation.

Microsoft SQL Express is Not Supported as a Database

Do not install Microsoft SQL Express as a database for CA SiteMinder® Federation Standalone. It is not supported.

Uninstalling SiteMinder Before Installing CA SiteMinder® Federation Standalone

Symptom:

If you are installing CA SiteMinder® Federation Standalone on a system where CA SiteMinder® or SPS was installed previously and is now removed, you might get an error message when installing CA SiteMinder® Federation Standalone.

Solution:

In this case you can follow this procedure:

1. Navigate to one of the following locations for your platform:

   Windows

   C:\Program Files\Zero G Registry

   UNIX

   /var or *federation_install_dir*/
2. Back up the .com.zerog.registry.xml file, saving it under a new name.
3. Remove any information related to SiteMinder or SPS in the registry file.
4. Save the changes to the registry file.

Rename Localized Connector Library After Upgrade

A localized version of the connector library is available for this release.

If you have upgraded from version 12.5 or older to CA SiteMinder® Federation Standalone r12.52, rename the localized connector library before using it.

Follow these steps:

1. Locate the following library:

   `smauthsmconnectorI18n`

2. Change the name of the library to the following name:

   `smauthsmconnector`

3. Restart CA SiteMinder® Federation Standalone r12.52.

CA SiteMinder® Federation Standalone UI Issues

The following topics describe issues you may encounter when using the CA SiteMinder® Federation Standalone UI.

SSL UI Connection Allows Non-SSL Access to the UI (87262)

Symptom:

If you enable SSL for the connection to the CA SiteMinder® Federation Standalone UI, the UI is still accessible over a non-SSL (HTTP) connection, potentially exposing an administrator's credentials.

Solution:

Enable the UI SSL port then disable the UI HTTP port.

To enable SSL for the UI

1. Run the Configuration Wizard, supplying values or accepting the defaults for the Admin UI HTTP Port and the Admin UI SSL Port settings.

   Note: You can skip this step if these ports were already defined when you first installed and configured CA SiteMinder® Federation Standalone.

2. Log in to the CA SiteMinder® Federation Standalone UI.

3. Select Infrastructure, SSL Configuration.

   The SSL Configuration dialog displays.

4. Click Activate in the Administrative UI SSL Configuration box.

   By clicking this button, SSL is enabled to protect the UI.

5. Exit the UI.

To disable the HTTP UI Port

1. Navigate to *federation_install_dir*\secure-proxy\proxy-engine\conf.
2. Open the server.conf file.
3. Comment out the setting **local.http.port=***port_number* by adding a pound sign (#) in front of the setting.
4. Save the server.conf file.
5. Restart the federation services according to your operating environment.

   - **Windows**

     Use the stop and start shortcuts as follows. If you logged in as a network user and not a local administrator, right-click the shortcut and select Run as administrator.

     a. Start, All Programs, CA, Federation Standalone, Stop services

     b. Start, All Programs, CA, Federation Standalone, Start services

   - **UNIX**

     a. Open a command window.

     b. Run the following scripts:

     *federation_install_dir/*fedmanager.sh stop

     federation_install_dir/fedmanager.sh start

     Note: Do not stop and start the services as the root user.

CA SiteMinder® Federation Standalone UI Permits only ASCII Characters (97031, 97033, 97034, 96471, 96473, 98181)

The CA SiteMinder® Federation Standalone Installation Wizard, Configuration Wizard, and User Interface support only ASCII characters for entries. Do not use UTF-8 characters.

Custom Post Form Help Description

For HTTP-POST single sign-on, the description for the Custom Post Form field is incorrect. The correct description is:

Custom Post Form

Names the custom auto-POST HTML form for HTTP-POST single sign-on. Enter only the name of the form, not the path to the form. The product provides a form named defaultpostform.html.

The physical page must reside in the directory *federation_install_dir*\customization, where *federation_install_dir* is the installed location of CA SiteMinder® Federation Standalone.

Partnership and Entity Issues

The following topics describe issues you may encounter when configuring federation partnerships and entities.

UTF-8 Characters in Federation Objects Causing Failures (179000)

Symptom:

In an i18n environment, federation transactions fail when a federation object contains any UTF-8 characters, which are not part of the Latin-1 (ISO-8859-1) character set.

Solution:

For an i18n environment, confirm that the HTTP connectors for the servlet containers in use by CA SiteMinder® Federation Standalone are configured for UTF-8. For instructions on setting the connectors to accept UTF-8 characters, see the appropriate documentation for your servlet container.

Federation Transaction Fails with Forms Authentication (179120)

Symptom:

Federation transaction fails with forms authentication when objects or entities are defined in French or Japanese characters with users either in French or Japanese.

Solution:

Update the standalone.xml file of Jboss 6.1 to include the system properties for URL Encoding.

Follow these steps:

1. Open the standalone.xml file available at the following location, in a text editor:

   ```
   Jboss_install_dir/standalone/configuration
   ```

2. Add the following lines after the <extensions> tag and before the <management> tag:

   ```
   <system-properties>
   <property name="org.apache.catalina.connector.URI_ENCODING" value="UTF-8"/>
   <property
   name="org.apache.catalina.connector.USE_BODY_ENCODING_FOR_QUERY_STRING"
   value="true"/>
   </system-properties>
   ```

3. Save and close the text editor.

Deployment of Federation Web Services Fails on JBoss 6.1 (174757)

Symptom:

Deploying the Federation Web Services (affwebservices.war) on JBoss 6.1 fails with the following exception:

```
Caused by: org.jboss.as.server.deployment.DeploymentUnitProcessingException:
JBAS011232: Only one JAX-RS Application Class allowed
```

This error is caused by an open issue in JBoss.

Solution:

Edit the affwebservices deployment descriptor to add a number of <context-param> entries.

Follow these steps:

1. Open the affwebservices deployment descriptor file (*webagent_option_pack*/affwebservices/WEB-INF/web.xml) in a text editor.
2. Add the following lines after the <web-app> tag and before the <servlet> tag:

```
<context-param>
<param-name>resteasy.scan</param-name>
<param-value>false</param-value>
</context-param>
<context-param>
<param-name>resteasy.scan.resources</param-name>
<param-value>false</param-value>
</context-param>
<context-param>
<param-name>resteasy.scan.providers</param-name>
<param-value>false</param-value>
</context-param>
```

3. Save and exit the text editor.

Federation Does Not Support the Cookie Provider (172511)

CA SiteMinder® Federation and CA SiteMinder® Federation Standalone, which use the Web Agent Option Pack, do not support the use of the Cookie Provider for federated configurations.

Encryption of an Assertion and the NameID fails with Java 1.7 (160057)

Symptom:

Encryption of an assertion and of the NameID fails with Java 1.7 installed.

Solution:

For Java 1.7, remove the following security provider entry from the java.security file:
`security.provider.1=com.oracle.security.ucrypto.UcryptoProvider ${java.home}/lib/security/ucrypto-solaris.cfg`

HTTP-Artifact Requires Encrypted Assertion with Non-ASCII Characters (98479)

If an assertion contains non-ASCII characters and it is sent using the HTTP-Artifact profile, encrypt the assertion or check that the artifact back channel is an SSL connection. This issue is only relevant for SAML 2.0.

Spaces Not Allowed in Partnership Names (74945)

Do not use embedded spaces in names for federation partnerships.

Federation Agent for Windows Authentication Issues

The following topics describe issues you may encounter when configuring the Federation Agent for Windows Authentication.

Federation Agent for Windows Authentication Supports Only ASCII Characters (175820)

The Federation Agent for Windows Authentication only supports ASCII characters in user names. The Federation Agent does not support multibyte Unicode characters. If your Windows user name contains multibyte characters, the federation request fails.

Chapter 5: Defects Fixed in 12.5

This section contains the following topics:

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

This section contains the following topics:

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 configuration file the logger.properties 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: Documentation

This section contains the following topics:

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 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.

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.

Chapter 9: 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