CA SiteMinder®

Federation Security Services Release Notes

r12.0 SP2

Contact CA

Contact Technical Support

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

- 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

Provide Feedback

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

If you would like to provide feedback about CA product documentation, complete our short customer survey, which is also available on the CA Support website, found at http://ca.com/docs.

Contents

Chapter 1: Welcome

This document contains information on SiteMinder Federation Security Services features, operating system support, known issues and fixes.

Federation Security Services is installed by the Policy Server on one system and the Web Agent Option Pack on another system. For information about those products, see the documentation for those products.

Chapter 2: New Features

There are no new features in this release.

Chapter 3: Changes to Existing Features

This section contains the following topics:

Policy Server Option Pack Integrated with Policy Server

The Policy Server Option Pack is no longer a separately installable SiteMinder component. The features installed by the Policy Server Option Pack (Federation Security Services, eTelligent Rules, Web Services variables) are now incorporated into the SiteMinder Policy Server and are installed by the Policy Server installation.

Licensing for Federation Security Services is still separate from licenses for SiteMinder.

Note: For Federation Security Services, the Web Agent Option Pack is still a separately installable component and is required to install Federation Web Services, one of the components of the Federation Security Services set of features.

SAML Affiliate Agent Availability

The SAML Affiliate Agent is not part of the SiteMinder r12 SP1 product set; however the 6.x SAML Affiliate Agent can communicate with the R12 SP1 Policy Server.

We recommend using the FSS Administrative UI for configuration operation with the 6.x SAML Affiliate Agent.

To download software and documentation for the 6.x SAML Affiliate Agent, go to the Technical Support site.

Note: The SAML Affiliate Agent only supports SAML 1.0 and it is not FIPS-compatible.

Chapter 4: Operating System Support

Federation Security Services is installed by the Policy Server, which installs the FSS Administrative UI and Web Agent Option Pack. Before you install these components, ensure you are using a supported operating system and third-party software.

For a list of supported operating systems, Web Servers, databases, Web browsers, LDAP directory servers, and servlet:

1. Log into the Technical Support site.
2. Search for the SiteMinder platform matrix for r12.0, which includes r12.0 SP2.

Chapter 5: Known Issues

This section contains the following topics:

Account Linking Does Not Work with CGI Password Services (67556)

In a federated environment, account linking does not work with CGI-based Password Services because of an issue with POST preservation. Use FCC-based Password Services if you want to configure account linking in a federated environment.

Note: CGI-based Password Services is a deprecated feature.

Web Agent Protecting FWS Application Must Trust Default Security Zone (56704)

If you are using Federation Security Services in an environment that includes SiteMinder security zones, you must configure the Web Agent that is protecting the Federation Web Services (FWS) application to trust the default security zone, which is called SM. To do this, include the default security zone (SM) for the SSOTrustedZone parameter, which is one of the configuration parameters for the Web Agent.

For more information about this parameter, see the *Web Agent Configuration Guide*.

Chapter 6: Fixes in r12 SP1 and SP2

This section contains the following topics:

SAML 2.0 Autopost Forms No Longer Require JavaScript (73858, 83123)

Symptom:

The autopost forms used for SAML 2.0 use to require JavaScript to be enabled in the user's browser.

Solution:

The autopost forms no longer require JavaScript.

SAML 2.0 Error Message For SSO Service Too Detailed (74355, 83122)

Symptom:

Calls to the SAML 2.0 Single Sign-on service that contain incorrect parameters for the Service Provider ID and/or the protocol binding display too much detail in the error message.

STAR Issue: 17444140-01

Solution:

A more generic error message is now displayed in the browser to eliminate any possibility of an attacker gaining information on the correct values of the Service Provider IDs and protocol bindings. The more detailed error message is still logged.

Authentication URL Open to Malicious Attacks (74278, 76976, 83114,83117)

Symptom:

The SMPORTAL query parameter in the Authentication URL is subject to malicious modification when a user is redirected to be authenticated and establish a SiteMinder session.

STAR Issue: 17429022-01

Solution:

The SMPORTAL query parameter can now be encrypted to prevent malicious attacks by using the new Use Secure URL feature. For details about this feature, see the *Federation Security Services Guide.*

Session Cookie is not Marked as Secure by the Assertion Cosumer Service (74449, 83124)

Symptom:

When an SMSESSION cookie is being set in the browser for a SAML 2.0 federation, it is marked as Secure if the UseSecureCookies parameter is set in the AgentConfigObject corresponding to Federation Web Services.

Solution:

The SMSESSION cookie is now marked as secure.

Web Agent Option Pack Fails when TRANSIENTIP Checking is Enabled (75240, 83125)

Symptom:

The Web Agent Option Pack fails when the TransientIPCheck setting is enabled in the AgentConfigObject and the Web Agent and the Web Agent Option Pack are operating on different machines.

STAR Issue: 17181546-01

Solution:

When TransientIPCheck is enabled in the AgentConfigObject, it now works properly in scenarios where the Web Agent and the Web Agent Option Pack are operating on different machines.

Wrong Private Key is Used to Sign Assertions (76161, 83118)

Symptom:

The wrong key in the smkeydatabase is being used to sign assertions.

STAR Issue: 17507633+17527146;01

Solution:

To sign SAML 1.1 assertions, ensure that the correct certificate for each partnership is used when multiple affiliate domains are defined. If signed assertions are specified but no signing alias is selected, use the certificate corresponding to the defaultenterpriseprivatekey alias.

NameID in Assertion Had the Wrong Format (76311, 83119)

Symptom:

When the NameID in an assertion was set to X509SubjectName and the NameID was configured as an LDAP DN, the Policy Server at the Identity Provider was escaping all the commas in the NameID. This format is wrong because only commas (and other special characters) within attribute values should be escaped. The commas that separate the different parts of the DN should not be escaped.

STAR Issue: 17509310;01

Solution:

When the NameID is set to X509SubjectName and the contents of the NameID is an LDAP DN, do not escape the commas separating the relative DNs. For example, the following DN is valid:

Uid = user1, dc=systemtest, dc=com

Session Server Error When Assertion Attribute Value is Blank or NULL (76985, 83120, 83703)

Symptom:

If you select PersistAttributes for the Redirect Mode of a SAML or WS-Federation authentication scheme, a session server error occurs when an attribute value in an assertion is blank or set to Null.

Solution:

If you choose PersistAttributes and the assertion contains attributes that are left blank, a value of NULL is written to the session store. This value acts as a placeholder for the empty attribute and it is passed to any application using the attribute.

For more information about the Redirect Mode, see the *Federation Security Services Guide*.

SLO Logout Response Has Incorrect Destination Value (77359, 83121)

Symptom:

The SLO Logout Response has a destination value that is unexpected.

When you configure single logout (SLO) at the Identity Provider or Service Provider, the value should be the destination entered for SLO Response Location URL setting, but instead the value is that of the SLO Location URL setting.

STAR Issue: 17498047;01

Solution:

The destination for the SLO Logout Response is now correctly set.

SiteMinder Cannot Process Multi-valued Attributes from an Assertion (77883, 80490, 83115)

Symptom:

A SiteMinder Policy Server acting as a Service Provider is not capable of processing or retrieving multi-valued attributes from a SAML 2.0 assertion.

STAR Issue: 17589511-01

Solution:

Multi-valued attributes are now appropriately handled by a SiteMinder Service Provider.

Error Occurs If User is Not in the First Listed User Directory (78618, 83531)

Symptom:

If a user does not exist in the first listed user directory configured for the SiteMinder Service Provider, an error is written to the smps.log that reads: [ERROR] Failed to find 'id' in affiliate user directory. This error message should not be written to this log file.

STAR Issue: 17532267

Solution:

The error message has been removed from Policy Server logs. Now an error message is only reported in the SM trace logs.

Chapter 7: 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.

In addition to the English release of this product, SiteMinder supports *only* those languages listed in the following table.

Language	Internationalized	Translated
Brazilian-Portuguese	Yes	No
Chinese (Simplified)	Yes	No
Chinese (Traditional)	Yes	No
Czech	Yes	No
Danish	Yes	No
Dutch	Yes	No
Finnish	Yes	No
French	Yes	No
German	Yes	No
Greek	Yes	No
Hungarian	Yes	No
Italian	Yes	No
Japanese	Yes	No
Korean	Yes	No
Norwegian	Yes	No
Polish	Yes	No
Russian	Yes	No
Spanish	Yes	No

Language	Internationalized	Translated
Swedish	Yes	No
Turkish	Yes	No

Note: If you run the product in a language environment *not* listed in the table, you may experience problems.

Chapter 8: Documentation

This section contains the following topics:

Guide Names

The names of the SiteMinder guides are as follows:

Guide
Policy Server Release Notes
Web Agent Release Notes
SDK Release Notes
API Reference Guide for Java
Programming Guide for Java
API Reference Guide for C
Programming Guide for Perl
SDK Overview Guide
Policy Server Installation Guide
Upgrade Guide
Policy Server Configuration Guide
Policy Server Administration Guide
Web Agent Installation Guide
Web Agent Configuration Guide
Web Agent Option Pack Guide
Federation Security Services Guide
Federation Security Services Release Notes
Directory Configuration Guide

To view PDF files, you must download and install Adobe Reader from the Adobe web site if it is not already installed on your computer.

SiteMinder Bookshelf

You can find complete information about SiteMinder by installing the SiteMinder bookshelf. The SiteMinder bookshelf lets you:

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

SiteMinder product documentation is installed separately. We recommend that you install the documentation before beginning the installation process.

Documentation installation programs are available for download from the CA Technical Support site.

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.