CA SiteMinder®

Federation Security Services Release Notes

r12.0 SP3

Third Edition

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by CA at any time.

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and proprietary information of CA and may not be disclosed by you or used for any purpose other than as may be permitted in (i) a separate agreement between you and CA governing your use of the CA software to which the Documentation relates; or (ii) a separate confidentiality agreement between you and CA.

Notwithstanding the foregoing, if you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all CA copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, CA PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL CA BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF CA IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is CA.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Copyright © 2012 CA. All rights reserved. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

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 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

This section contains the following topics:

Signing and Verification using SHA-2 Algorithms

SiteMinder can use a private key/certificate pair to perform various digital signing tasks for federated communication.

SiteMinder now supports signing of certificates with the more secure SHA256 signature algorithm.

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

Enforcing One Time Use of Assertions

In compliance with the SAML 1.x and 2.0 specifications, SiteMinder can now enforce the one-time use of an assertion. By generating an assertion intended for one-time use, it tells the relying party not to retain the assertion for future transactions.

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

SiteMinder JSP Pages that Check for Cross-site Scripting

SiteMinder provides several JSP pages for use with SiteMinder federation functionality. These JSP pages check characters in a request to be sure that unsafe information in the output stream is not displayed in the browser. This check prevents against cross-site scripting attacks.

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

New Setting to Secure the IdP Discovery Target

When the SiteMinder Identity Provider Discovery Service receives a request for the common domain cookie, the request includes a query parameter named IPDTarget. An unauthorized user can place any URL in this query parameter and cause a redirection to a malicious site.

To protect the IPDTarget query parameter against attacks, there is a new configuration parameter named ValidFedTargetDomain, which lists all valid domains for your federated environment. When the IPD Service examines the IPDTarget query parameter, it obtains the domain of the URL specified by the query parameter. The IPD Service compares this domain to the list of domains specified for the ValidFedTargetDomain parameter to confirm it is a legitimate domain.

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

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 SPx product set; however the 6.x SAML Affiliate Agent can communicate with the R12 SPx 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.

Two New Ciphers for SHA256 Support Across the Back Channel

Federation uses an SSL client when processing back channel requests. You can now configure the Identity Provider to use SSL versions TLSV1_1 and TSLV1_2 with the following ciphers:

- RSA_With_AES_128_CBC_SHA256
- RSA_With_AES_256_CBC_SHA256

These ciphers are supported in FIPS and non-FIPS mode.

The determination whether to use SHA256 is made at the Identity Provider. The Service Provider broadcasts the SSL versions and ciphers that it supports. The Identity Provider is configured to accept a certain set of SSL versions and ciphers. Part of the SSL handshake includes communicating using the first configured match of versions and ciphers.

SiteMinder does not have a configuration setting for selecting the required algorithm. Administrators must verify that the Identity Provider is configured appropriately.

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 SP3.

Chapter 5: Installation and Upgrade Considerations

This section contains the following topics:

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 SiteMinder component:

- Installation
- Configuration
- Administration
- Upgrade

Note: For more information about which SiteMinder components support Windows Server 2008, see the SiteMinder Platform Support matrix.

To run 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 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 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 SiteMinder command.

More information:

Contact CA Technologies (see page 3)

Chapter 6: Known Issues for Federation Security Services

This section contains the following topics:

Attributes Appear Truncated at the Relying Party (157913)

Symptom:

The following issues occur:

- The directory attributes appear truncated at the relying party.
- The following message appears in the smtracedefault.log file:

  `[WARNING: Response attribute will be trimmed. [attr = SMUSERGRP:memberOf] [actual attr len = number] [ response attr len = number]]`

  Note: In the Warning message, SMUSERGRP represents the variable name and memberOf represents the attribute value. The error message is specific to your configuration.

Solution:

The maximum length for the user assertion attributes is configurable by modifying settings in the EntitlementGenerator.properties file. To modify the length, go to the *CA SiteMinder Federation Security Services Guide* and follow the procedure in the section "Specify the Maximum Length of Assertion Attributes."

SiteMinder Federation does not Support Directory Mapping (136609)

The SiteMinder federation security services feature does not support directory mapping. The user is tied to the directory they are initially authenticated against. If that directory is not present in the affiliate domain, the authorization fails.

CPU Spikes When Accessing a Federation Object (136694)

While trying to access a Federation object in the FSS UI, CPU usage was spiking to 98 or 99 percent. You can work around this issue by adjusting the buffer size value (Max AdmComm Buffer Size) to be larger than the default (256 KB). Care should be observed when setting this value, because too large a value can decrease overall performance. A value of 10MB can be too much, while 1MB can work well.

JDK Memory Leak with SAML 1.1 Artifact Transactions

If your federated environment is running on the following configuration, JDK 1.6.x may leak up to 4 KB of memory at the Identity Provider for each SAML 1.1 Artifact transaction:

- An r12.0 SP3 Policy Server is installed on Solaris 9.
- Java 1.6.x is installed on the Policy Server host system.
- Oracle databases are deployed as a SiteMinder session store, a user store, or both.

A case has been opened with Oracle to investigate the Sun Java 1.6 leak when running on Solaris 9.

If you have the previous configuration, contact Support for instructions on how to resolve this issue.

This leak is specific to the previous configuration. The leak does not occur if:

- A database other than Oracle is deployed as a SiteMinder session store, a user store, or both.
- The Policy Server is installed on Solaris 10.

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 7: Fixes in r12 SP3

This section contains the following topics:

LDAP Search Filter Handles Multiple %s Strings (142592, 150648)

Symptom:

Specifying an LDAP search filter in a SAML 2.0 authentication scheme at the Service Provider had a limitation. The Policy Server could not process an LDAP filter string with multiple %s characters.The Policy Server was not replacing all %s variable with the login ID.

This problem occurred for Federation Security Services.

Solution:

You can now specify an LDAP search filter containing multiple %s variables. The following are example strings now supported:

```
|(uid=%s)(uid=%s)
|(abcAliasName=%s)(cn=%s)
```

If user1 is the LoginID, the Policy Server resolves these strings as follows

```
|(uid=user1) (uid=user1)
|(abcAliasName-user1) (cn-user1)
```

Specify LDAP searches in the User Lookup field of the SAML 2.0 authentication scheme in the Administrative UI. The dialog can be found at the location Infrastructure, Authentication Schemes, General.

STAR Issue: 20375682

Truncation of Assertion Attributes (151642, 151887)

Symptom:

The assertion attributes are truncated after 1000 characters.

Solution:

This is no longer an issue. The *Federation Security Services Guide* has been updated.

STAR Issue: 20546848-1, 20608564-1, 20873093-1

Web Agent Option Pack Environment Script has Invalid Jars (144569, 147392)

Symptom:

The Web Agent Option Pack environment script and missing LD_LIBRARY_PATH has incorrect jar locations and does not have the LD_LIBRARY_PATH defined in the WAOP/bin location.

Solution:

This is no longer an issue. The Web Agent Option Pack Guide has been updated.

STAR Issue: 20513877

Smreghost Not Working on Linux (140319)

Symptom:

The Smreghost utility is not working correctly on Linux.

Solution:

This is no longer an issue.

STAR Issue: 20253544-1

IP Restriction for 1.x Artifact and POST (137275)

Symptom:

The IP restriction for 1.x Artifact and POST are not working.

Solution:

This is no longer an issue.

STAR Issue: 20098491-1

Configuring Persistent Attributes Works Correctly for SAML 2.0 (137052)

Symptom:

When getting the SamlValidator, the following error appeared:
errorjava.lang.ClassCastException: [Ljava.lang.String; cannot be cast to java.lang.String.

Solution:

The primitive type was changed from String to String[] to store the values returned from the Hashmap iterator.

Star issue: 20140602;1

Protection Against XML Signature Wrapping Attacks (168098)

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

SM--Information Missing for the smfedexport Command Options (155515)

Symptom:

There is no detailed information about the usage of the smfedexport utility options, such as –pubkey,-sign and –signingcertalias.

Solution:

The *Federation Security Services Guide* has clearer explanations of the smfedexport command options.

STAR issue: 20969179-01

Updated Session Index Causes Single Logout to Fail (123496)

Symptom:

A user authenticates at the IdP and is redirected back to the SP with an assertion. If the user clicks the browser back button upon returning to the SP, the session index is updated and stored in the SP session store.

When the user logs out, SiteMinder uses the session index from the original assertion, resulting in a session index mismatch. Single logout, if configured, fails.

Solution:

A new setting named Reuse Session Index has been added to the Single Logout tab of the SAML 2.0 Service Provider Properties. Enable this option so single log out works with third-party partners that do not honor the session index passed in newer assertions.

STAR Issue: 19613507-1

SessionNotOnOrAfter Parameter Could Not Be Modified (128759,109961)

Symptom:

When the SiteMinder IdP generates an assertion, it included a parameter named SessionNotOnOrAfter in the Authentication statement of the assertion. This parameter was set to the assertion validity duration by default and it could not be customized or omitted from the assertion.

Solution:

The SessionNotOnOrAfter parameter can now be customized or left out of the assertion by configuring the SP Session Validity Duration setting in the FSS Administrative UI. The *Federation Security Services Guide* has detailed instructions.

STAR Issue: 19635319

Problem with Forced Authentication When User Identity Changes (125553)

Symptom:

A user must reauthenticate at an IdP even though they have a session because the SP authentication request includes the query parameter ForceAuthn = True. The user reauthenticates with different credentials than the credentials he used to establish the original session. The IdP returns a SAML assertion, but it contains the user identity information from the original session, not the current session.

Solution:

Federation Security Services has been modified so that the IdP compares the userDN and the user directory OID for the current and existing sessions. If the sessions are not for the same user, the IdP returns a SAML 2.0 response indicating that the authentication has failed.

STAR Issue: 19742014

Federation Web Services Cannot Decode SMSESSION Cookie on Tomcat (129196)

Symptom:

If Federation Web Services is deployed on a Tomcat server, the Web Agent protecting the target resource at the Service Provider cannot decode the session cookie.

Note: Federation Web Services is installed by the Web Agent Option Pack.

Solution:

When Tomcat 5.5 and higher is used as application container for Federation Web Services, add the following system property to the Tomcat start-up shell or batch file and set it to true:

-Dorg.apache.catalina.STRICT_SERVLET_COMPLIANCE=true

STAR Issue: 19884857

Mutli-value Assertion Attributes Not Handled Properly (124560)

Symptom:

Sending LDAP attributes with more than one value was not properly handled by SiteMinder for SAML 2.0 and WS-Federation protocols. The attributes were separated by a caret ('^') in the assertion instead of being treated as separate elements.

Solution:

When you configure assertion attributes in the UI, place the prefix **FMATTR:** in front of the attribute name, each attribute value becomes a separate <AttributeValue> element in the assertion.

The *Federation Security Services Guide* contains specific configuration instructions.

STAR Issue: 19685750-1

Trace Message for Redirect Mode Displays Incorrect Text (100214)

Symptom:

The name of the "Profile Cookie" Redirect Mode option has changed to Legacy Cookie in the UI, but FEDProfileCookie is still displayed in the logs.

Solution:

The trace messages now indicate Legacy Cookie instead of FEDPROFILE cookie.

Full Logoff Failure (119281)

Symptom:

The full logoff feature only logged users off of two of my domains, but not the third domain.

Solution:

This issue is fixed.

Star Issue: 19299081:01

Error After Metadata Import Using smfedimport Tool (116041)

Symptom:

I exported information from an R12 SP2 service provider with the smfedexport tool and then imported the same information into the Identity Provider. When I ran the listCerts command on the smkeydatabase, I got the following error:

Certificate cannot be read from SMKeyDatabase

Solution:

This issue is fixed.

Star Issue: 19252927:01

FSS Administrative UI Will Not Start (118424)

Symptom:

When I try to start the FSS Administrative UI I receive the following error message:

```
Error :
Custom Action:    com.netegrity.ps_ws_config.PSWebServerConfig
Status: ERROR
Additional Notes: ERROR -     class
com.netegrity.ps_ws_config.PSWebServerConfig.install() runtime exception:
```

Solution:

This issue is fixed.

Star Issue: 19412216:01

Upgrade Overwrote AMAssertionGenerator.properties File (121216)

Symptom:

Upgrading the Policy Server Option Pack from r6.x SP5 CR22 to r12.x SP2 overwrote the settings in the AMAssertionGenerator.properties file.

Solution:

This issue is fixed.

Star Issue: 19561274:01

SPS is Not Redirecting to the URL in the Password Policy (111147)

Symptom:

SPS does not correctly redirect to the URL in the password policy when the maximum password failure attempts is exceeded.

Solution:

SPS now correctly redirects to the URL.

Federation Security Services at the SP Fails Due to Malformed SAML 2.0 Response (111148)

Symptom:

If Federation Security Services at the Service Provider receives a malformed SAML 2.0 POST assertion response, Federation Security Services terminates unexpectedly.

Solution:

Federation Security Services no longer fails in this case.

NETE_JDK_ROOT Defined Twice in Properties File (117162)

Symptom:

NETE_JDK_ROOT was defined twice in the nete-wa-opack-installer.properties file.

Solution:

The duplicate entry has been removed.

Star issue: 19303020

WS-Federation Redirects Return 400 Error to Browser (117425)

Symptom:

WS-Federation redirects from SiteMinder returned error code 400 messages to web browsers.

Solution:

This issue is fixed.

Star Issue: 19381642:01

Chapter 8: 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 not Marked Secure by the Assertion Consumer 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 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 user interface of the product, online help and other documentation, as well as local language default settings for date, time, currency, and number formats.

SiteMinder has been internationalized and localized to the extent indicated in the platform support matrix for SiteMinder r12sp3 J

Chapter 10: Documentation

This section contains the following topics:

SiteMinder Bookshelf

Complete information about SiteMinder is available from 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.

View and download the 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.

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.