CA SiteMinder®

Federation Security Services Release Notes

r6.0 SP6

Fourth Edition

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA Technologies 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 Technologies product documentation, you can send a message to techpubs@ca.com.

If you would like 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, which are installed with the Policy Server and Web Agent Option Packs. It describes new federation features, known issues and fixes.

Chapter 2: New Features for Federation Security Services

Federation Security Services r6.0 SP6 has no new features.

Chapter 3: Operating System Support

Before you install the Option Packs for Federation Security Services, ensure you are using a supported operating system and third-party software.

To locate the support matrix on the Support site

1. Click Technical Support.
2. Click Support By Product.
3. Select CA SiteMinder from the Select a Product Page list.
4. Scroll to Product Status and click Platform Support Matrices.

Chapter 4: Installation and Upgrade Considerations

Federation Security Services features are installed by the Policy Server Option Pack and the Web Agent Option Pack.

For installation and upgrade information on the Option Packs, see the *Policy Server and Web Agent Option Pack Guide*.

Verify HP-UX Patch Level to Install a SiteMinder Component

The SiteMinder installers for r6.0 SP6 require Java 1.6. If you want to install a SiteMinder component on a system that uses the HP-UX operating environment, do the following:

1. Go to the HP Software Depot web site.
2. Search the Software Depot for the following item:

   `JDK, JRE, and Plug-In 6.0.x Downloads and Documentation`
3. Verify that your system contains the correct prerequisites.

Upgrades and Microsoft Visual Studio

Valid on Windows

SiteMinder r6.0 SP6 components are compiled using Microsoft Visual Studio® 2005 (VC 8). Consider the following:

- Previous versions of SiteMinder were compiled using Microsoft Visual Studio 2003 (VC 7). Although we expect that all custom code compiled with Microsoft Visual Studio 2003 (VC 7) to continue to work, we recommend testing all custom code with SiteMinder r6.0 SP6.
- If you are using layered products, we recommend referring to the respective Platform Support Matrix to determine if the product is certified with SiteMinder r6.0 SP6. Examples of layered products include the following:
  - Application server agents
  - ERP agents
  - Advanced Password Services
  - The Secure Proxy Server
  - Identity Manager

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 iii)

Chapter 5: Known Issues

This section contains the following topics:

Web Agent Protecting Federation Web Services Must Trust Default Security Zone (56704)

If you are using Federation Security Services in an environment with SiteMinder security zones, you must configure the Web Agent that is protecting the Federation Web Services application to trust the default security zone, called SM. Therefore, include the default security zone SM when configuring the SSOTrustedZone parameter for this Web Agent.

Policy Server on a Japanese OS Cannot Display Affiliate Domain Objects After Upgrade to 6.0 SP 4 or higher

The contents of any affiliate domain objects that were created on a version of the Policy Server running on a Japanese OS prior to 6.0 SP1 will not be displayed as a result of an upgrade to 6.0 SP 4.

Single Logout Services Log Errors if ODBC/SQLError Component Enabled (41324)

If the ODBC/SQLError component is enabled in the Policy Server trace log, Single Logout Services may cause the following errors to be written to the trace log:

```
[13:42:44.0][CSmDbODBC.cpp:189][CSmDbConnectionODBC::MapResult][][][-1][[Micr
osoft][ODBC SQL Server Driver][SQL
Server]Violation of PRIMARY KEY constraint 'PK__ss_sessionvar5__571DF1D5'.
Cannot insert duplicate key in object
'ss_sessionvar5'.][][][][]
[13:42:44.0][CSmDbODBC.cpp:277][CSmDbConnectionODBC::MapResult][][Mapped
Result: -1059 Error Message:
"[Microsoft][ODBC SQL Server Driver][SQL Server]Violation of PRIMARY KEY
constraint 'PK__ss_sessionvar5__571DF1D5'. Cannot
insert duplicate key in object 'ss_sessionvar5'." SQL State: 23000.][][][][][][]
[13:42:44.0][CSmDbODBC.cpp:189][CSmDbConnectionODBC::MapResult][][][-1][[Micr
osoft][ODBC SQL Server Driver][SQL Server]The
statement has been terminated.][][][][]
[13:42:44.0][CSmDbODBC.cpp:277][CSmDbConnectionODBC::MapResult][][Mapped
Result: -1059
Error Message: "[Microsoft][ODBC SQL Server Driver][SQL Server]The statement has
been terminated." SQL State:
01000.][][][][][][]
[13:42:44.0][CSmDbODBC.cpp:189][CSmDbConnectionODBC::MapResult][][][-1][][][][
[]
[13:42:44.0][CSmDbODBC.cpp:277][CSmDbConnectionODBC::MapResult][][Mapped
Result: -1059 Error Message: "" SQL State:
.][][][][][][]
```

This is normal and the data is ultimately written to the session server database.

Incompatible SiteMinder Releases for Federation Security Services (44790)

SiteMinder versions 6.0 SP 3/6.x QMR 3 configured as a SAML 1.X consumer and the SAML Affiliate Agent 6.x QMR 3 are incompatible with SiteMinder versions 6.0 SP 2/v6.x QMR 2 and earlier configured as a SAML 1.X producer. The incompatibility is due to changes made in SiteMinder 6.0 SP 3/6.x QMR 3 to ensure conformance to the SAML specification based on the PingID certification tests.

Small Memory Leak with Policy Server Option Pack (91765)

The Policy Server Option Pack leaks a small amount of memory when executing SAML 2.0 Service Provider POST transactions.

Chapter 6: Defects Fixed in the Policy Server 6.0 SP6 Option Pack

This section contains the following topics:

Fixes in the Policy Server 6.0 SP6 Option Pack

DSA Keys Not Supported on Solaris 10 (97620/98080)

Symptom:

DSA keys created by the JDK 1.1 javakey tool, and stored in the JDK 1.1 IdentityDatabase use a deprecated OID (1.3.14.3.2.12). These keys will not be granted full privileges on Solaris 10 if the default security provider configuration is in place.

A workaround is to list the Sun provider (sun.security.provider.Sun) ahead of the PKCS11 provider (sun.security.pkcs11.SunPKCS11) in the java.security security properties located in the lib/security directory of the JDK installation.

Solution:

This issue has been documented in a new topic that has been added to the Policy Server Installation section of the Policy Server and Web Agent Option Pack Guide for 6.0 SP 6.

STAR Issue: 18653642-1

No Mechanism to Override SAML 1.0/1.1 TARGET Query Parameter (99811)

Symptom:

For SAML 1.0 and 1.1, TARGET is a required query parameter for SSO. There is no way to specify a Target URL in the SP-side configuration that can override this parameter, or a way to validate that the target is a protected SiteMinder resource.

Solution:

For SAML 1.0 and 1.1, a new Target URL parameter at the SP-side configuration is now available. This new field can override the Target query parameter. This field has been documented in the help for the SP-side configuration.

SiteMinder FSS Unable to Decrypt Encyrpted Assertions Generated by Oracle IdP (112719)

Symptom:

SiteMinder Federation Security Services is unable to decrypt encrypted assertions generated by an Oracle Identity Provider.

Solution:

This issue has been fixed.

STAR Issue: 19118514

Restarting Policy Server to Immediately Register a New Certificate Not Documented (113000)

Symptom:

The *SiteMinder Federation Security Services Guide* does not include information stating that the Policy Server must be restarted after a certificate is added to the key database to implement the change immediately.

Solution:

This issue has been fixed in the r6.0 SP6 *SiteMinder Federation Security Services Guide*.

STAR Issue: 19090737-01

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 Policy Server User Interface. The *Federation Security Services Guide* has detailed instructions.

STAR Issue: 19635319

Chapter 7: Defects Fixed in the Web Agent 6.x QMR 6 Option Pack

This section contains the following topics:

Fixes in the Web Agent 6.0 SP6 Option Pack

Application Server on AIX Crashes when Malformed SAML 2.0 Assertion Received (101481)

Symptom:

A web application server on an AIX system crashes when federation security services receives a malformed SAML 2.0 assertion.

Solution:

This issue is fixed.

STAR Issue: 18864059:01

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

Chapter 8: Defects Fixed in the Policy Server 6.0 SP5 Option Pack

This section contains the following topics:

Fixes for Policy Server 6.0 SP5 Option Pack

The following are defects fixed for the Policy Server Option Pack.

Metadata Processor Shows Incorrect Warning Message When Using Smfedexport (89812)

Symptom:

When running the smfedexport utility, the metadata processor displays a WARN_NOTEXIST_SCHEME warning message instead of an error message.

Solution:

The proper error message is now displayed.

STAR Issue: 18168812

Special Characters in a SAML 1.x Assertion Consumer URL Query String Cause Error (89452)

Symptom:

A SAML 1.x response was causing an error because special characters in the Assertion Consumer Service URL query parameters were not handled correctly.

Solution:

If the Assertion Consumer URL query parameters use any special characters, an exception is no longer thrown while converting the response from a string to XML document type.

SAML Parser Error Occurs When Consuming a SAML 1.1 Assertion with Special Characters (85642)

Symptom:

If the Policy Server is serving as a SAML 1.1 consumer, an error with the SAML parser appears while consuming an assertion that contains special characters.

Solution:

The Policy Server no longer produces SAML parser errors while consuming assertions that contain special characters.

STAR Issue: 18068611

No Mechanism to Sign Attribute Query Requests and Responses (85124)

Symptom:

Federation Security Services does not provide any mechanism to sign Attribute Query requests and corresponding Attribute Query responses.

Solution:

Federation Security Service now provides an option to sign Attribute Query and the corresponding SAML response. A check box has been added to the Attributes tab of the SAML 2.0 Auth Scheme that enables singing of Attribute Query requests. Also, a Require Signed Attribute Query checkbox has been added to the Attribute Svc tab of the Service Provider to specify that the IdP can accept only signed Attribute Query requests.

STAR Issue: 17549677

SiteMinder Rejects Assertion if <NameIdentifier> Element is Embedded in the <SubjectConfirmation> Value (51696)

Symptom:

SiteMinder rejects a SAML assertion if the <NameIdentifier> element is put in the XML assertion within the <SubjectConfirmation> value.

Solution:

The search for the <NameIdentifier> has been restricted to only the immediate next child level so this is no longer a problem.

SAML 2.0 Transactions Fail When Assertion Consumer Service URL Contains Port Number (47252)

Symptom:

On Windows platforms, SAML 2.0 transactions are failing when a valid port is appended to the Assertion Consumer Service URL.

Solution:

You can now have a valid port appended to the Assertion Consumer Service.

AuthenticationInstant Attribute Value Set Incorrectly (48584)

Symptom:

The SAML assertion attribute AuthenticationInstant was not being set to the time the user authenticated at the Identity Provider.

Solution:

The AuthenticationInstant attribute is now set to the correct time.

Process on UNIX System Fails When Viewing FederationWSCustomUser Directory (48846)

Symptom:

On UNIX platforms, the smpolicysrv process is failing when a SiteMinder administrator tries to view users in the FederationWSCustomUser directory.

Solution:

This is no longer a problem.

SAML Authentication Scheme Needs Optional <dsig:KeyInfo> Attribute (44815)

Symptom:

The SAML authentication scheme requires that signed SAML 1.1 assertions contain the optional <dsig:KeyInfo> attribute when trying to consume the assertion.

Solution:

SiteMinder no longer requires the optional attribute.

Multiple User Stores Identified by IP Address are Not Searched Properly During Authentication (52772)

Symptom:

Multiple user stores identified by IP addresses are not searched properly during SAML authentication.

Solution:

This is no longer a problem.

SAML 2.0 Authentication with Single Use Policy Enabled Causes Policy Server Failure (53113)

Symptom:

The Policy Server on a Solaris system acting as a Service Provider is failing when a SAML 2.0 authentication scheme is configured with the Enforce Single Use Policy option enabled.

Solution:

One of the parameters being passed from the SAML authentication scheme to the logging mechanism was NULL causing the crash. The SAML authentication scheme has been modified to ensure that it does not pass the null argument.

Require Signed AuthnRequests Option Fails on Solaris-based Identity Provider (53693)

Symptom:

If you configure a SAML Service Provider and check the Require Signed AuthnRequests option, the requests are failing.

Solution:

The requests are no longer failing.

Signature Processing for SAML Post Profile Fails When TransactionMinder is Installed (54217)

Symptom:

When the Policy Server Option Pack and TransactionMinder are installed and configured together, signing functionality does not work.

Solution:

Signature processing is now successful regardless of whether or not TransactionMinder is installed with the Policy Server Option Pack or not.

Sample Class Missing from SDK Installation (54230)

Symptom:

The sample class directory, sdk/samples/authextensionsaml20 is missing from the 6.0 SDK installation.

Solution:

The directory is now part of the SDK kit.

Policy Server Fails When Several Failover Servers Exist for SAML 1.1 POST Authentication (54624)

Symptom:

The Policy Server was failing during a SAML 1.1 Post authentication process when a user directory had a large number of failover servers configured.

Solution:

The Policy Server no longer fails. The number of failover servers allowed has been increased.

Apply Button Deletes the XPATH query for XML Body Variable (54839)

Symptom:

Clicking the Apply button at the bottom of the XML Body Variable Editor in the Policy Server User Interface removes the XPATH query when the variable is configured using the Advanced Query option on the Advanced tab.

Solution:

This is no longer an issue.

SAML 2.0 Authentication Scheme with Server Redirect Mode Set Ignores Assertion Attributes with Certain Name Formats (54517)

Symptom:

When an assertion contains attributes with a Name Format of **unspecified** or **url**, the Service Provider at the consumer ignores the assertion attributes if the SAML 2.0 authentication scheme is configured with the Server Redirect mode.

Specifically, the following attributes are ignored:

- urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified
- urn:oasis:names:tc:SAML:2.0:attrname-format:uri

It only sets attributes with a name format of urn:oasis:names:tc:SAML:2.0:attrname-format:basic.

Solution:

The unspecified and url attributes are no longer ignored in Server Redirect mode.

SiteMinder Fails to Process a Third-party Assertion with Multi-valued Attributes (54562)

Symptom:

When a third-party generates a SAML assertion with an attribute that has multiple values from the user store, the Policy Server is not processing the assertion correctly.

Solution:

The Policy Server can now process assertions from third-parties with multiple values.

Unattended Upgrade of the Policy Server Option Pack on Windows 2003 Causes a System Reboot (55548)

Symptom:

When upgrading the Policy Server Option Pack in unattended mode, the Windows 2003 system was rebooting.

Solution:

This is no longer occurring.

Persistent Identifier for IdP-initiated SSO Not Being Generated (69108)

Symptom:

The Identity Provider does not dynamically create an opaque persistent identifier for IdP-initiated single sign-on requests even if the Service Provider sends an AuthnRequest with the Allow Creation of a New User Identifier flag set.

Solution:

FSS now correctly generates an opaque persistent identifier for IdP-initiated single sign-on requests if the Allow IDP to Create New User Identifier checkbox in the SSO tab of the SAML 2.0 Auth Scheme Properties dialog is set.

Unnecessary smdspropc.cpp Error in Policy Server Logs (78618)

Symptom:

When using a SAML Service Provider, if the user does not exist in the first listed directory it results in the following error printed to the smps log:

[ERROR] Failed to find 'id' in affiliate user directory

Solution:

When a SAML Service Provider is configured with multiple user directories, an error is no longer logged in the Policy Server log for each directory instance that does not contain the user prior to the directory instance in which the user is located. The messages are still be printed in the SMTRACE log.

User Attributes in Assertions Not Allowed to be Set to NULL (79547, 76985)

Symptom:

For SAML1.1, SAML 2.0 and WS-Federation, a session server error occurs when an assertion is generated with an attribute value that is blank or set to Null.

Solution:

Assertions can be contain user attributes that may be blank or set to Null without causing a session server error. In this case, the assertion attribute value will be sent as NULL.

SMPORTALURL Query Parameter Subject to Malicious Modification (74278)

Symptom:

When a user is redirected to the Authentication URL, the SMPORTALURL query parameter could be manipulated to redirect the user to a malicious site.

Solution:

To prevent possible malicious modification of URLs when a user is redirected to an authentication URL, the SMPORTALURL query parameter can now be encrypted. To encrypt this parameter, select the Use Secure URL option in the appropriate dialog at the producer/Identity Provider/Account Partner site, or set the SDK parameter USE_SECURE_AUTH_URL property to 1 in the SP or IDP object.

Note: If the Use Secure URL option is selected, the following servlet must be specified for the Authentication URL:
http(s)://*idp_server*:*port*/affwebservices/secure/secureredirect

Signature for SAML 1.1 Assertions Unclear With Multiple Affiliate Domains (76161)

Symptom:

When multiple affiliate domains use different signing keys, the Policy Server does not pick up the correct signing key when the respective SAML 1.1 assertion is being generated.

Solution:

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

Commas Cannot Separate Relative DNs in the NameID Defined as an X509SubjectName (76311)

Symptom:

When the NameID in an assertion is set to X509SubjectName and the contents of the NameID is an LDAP DN, the Policy Server is escaping the commas in the NameID. For example, **&ltns2:NameID.**

Solution:

Do not escape the commas separating the relative Distinguished Names in the NameID.

SLO Response Location URL Not Being Set Correctly (77359)

Symptom:

Single Logout Response has the incorrect destination value.

Solution:

The destination attribute in SLO response messages is now correctly set when the SLO response location URL has been configured.

Multi-valued Attributes Not Properly Handled at the Service Provider (77883)

Symptom:

The SiteMinder Policy Server is not capable of processing or retrieving multi-valued attributes from a SAML 2.0 assertion.

Solution:

When acting as a SAML 2.0 Service Provider, the Policy Server now properly handles multi-valued assertion attributes.

Proper Error Not Returned When Signing Alias is Invalid (64173)

Symptom:

SAML 2.0 Assertion Generator succeeds at signing the assertion or response when an invalid signing alias is configured.

Solution:

The proper error is returned when an invalid signing alias is configured.

Incorrect Option Displayed for the smfedexport Utility (72942)

Symptom:

If you display the command options for the smfedexport utility, it is showing the -encryptionkeyalias command, which is incorrect. The command option should be decryptionkeyalias.

Solution:

The correct command option is now being displayed.

Invalid Stream Header Error with 302 Cookie Data and Server Redirects (75270)

Symptom:

When the SAML 2.0 assertion consumer received an assertion with attributes not containing the optional NameFormat element, a 500 error was being returned when the redirect mode was set to 302 cookie redirect or server redirect.

Solution:

The NameFormat is correctly inferred to be Unspecified and an error is no longer returned.

Single Logout Request After SMSESSION Expires Causes 500 Server Error (60437)

Symptom:

A 500 error occurs if a single logout request (IDP- or SP-initiated) is sent after the user's SMSession has expired.

Solution:

This is no longer an issue. A single logout response is returned is returned.

Failed Assertion Decryption Results in Unclear ClassCastException (64645)

Symptom:

If SiteMinder fails to successfully decrypt an assertion a ClassCastException messages is sent.

Solution:

A meaningful error message and return an error code instead is sent if the assertion cannot be decrypted.

Error During Import of Metadata Because of Options Used to Create Export File (70391)

Symptom:

If you use the smfedexport tool with the -sign and -pubkey options to create an XML file that contains the public key of the issuer importing the file with the smfedimport utility causes an error.

Solution:

This is no longer an issue. The -sign and -pubkey options can be used and the import will be successful.

Mismatched Certificate/Key Pair Being Imported (71311)

Symptom:

The smkeytool utility allows you to import a mismatched private key and public certificate.

Solution:

The smkeytool utility now matches the private key and the public certificate being imported.

NameID Greater than 99 Characters Being Truncated (72361)

Symptom:

If a user's NameID in the directory contains more than 99 characters, it was truncated in the assertion.

Solution:

The limit for the NameID has now been increased to 1024 characters.

Resource Partner-initiated SSO Not Operating Properly for WS-Federation (73467)

Symptom:

Single sign-on transactions initiated by a WS-Federation Resource Partner are not working.

Solution:

This is no longer a problem.

Query String in Redirection URL to Password Services FCC is Truncated (69431)

Symptom:

The query string in the redirect URL to the Password Services FCC is truncated when a SAML 1.x authentication scheme is used and the user at the consumer is administratively disabled by SiteMinder.

Solution:

When a user is administratively disabled at a Service Provider site protected by the SAML 1.x authentication scheme, the query string in the redirect URL is no longer truncated.

Issues Retrieving Certain New Certificates when SAML 2.0 Authentication Configured (70821)

Symptom:

SAML 2.0 POST transactions fail at the Service Provider when trying to retrieve newly generated certificates.

Solution:

This is no longer an issue.

Assertions Sent with False PersistentID and Null NameID (71907)

Symptom:

An assertion is still sent when the Persistent Identifier is disabled and there is no Name ID in the assertion.

Solution:

The assertion is no longer sent if these conditions exist.

New Certificates Not Being Retrieved Due to Serial Number Issue (69936)

Symptom:

An incompatibility with the serial numbers of some newly generated certificates prevents the certificates from being retrieved from the smkeydatabase.

Solution:

The conversion of serial number strings now ensures the certificate can be fetched from smkeydatabase.

Signing Alias, Issuer DN, Serial Number Fields Not Properly Enabled (67253)

Symptom:

Signature fields in SAML 2.0 Service Provider Properties dialog are not enabled until the Require Signed AuthnRequests check box is selected on the SSO tab or the HTTP-redirect check box is selected in the SLO tab. This prevents the proper configuration of assertion and response signing in cases where signed Authnrequests cannot be required and single logout cannot be used.

Solution:

The Signing Alias, Issuer DN and Serial number fields in the General Tab of the Service Provider Properties dialog of the Policy Server User Interface are now properly enabled when needed.

Multiple CRLs Added to the smkeydatabase Causes Registration Error (61695)

Symptom:

SMKeytool does not support more than one LDAP -based CRL at a time. After adding a second LDAP CRL to the key store, any subsequent operations performed on the smkeydatabase are failing.

Solution:

A registration error no longer occurs when multiple CRL's are added to the smkeydatabase.

AuthnRequest and SLO Request Signing and Validation Should Not Allow Expired Certificates (61951)

Symptom:

Signing and verification for AuthnRequests and single logout requests is successful with the expired certificates.

Solution:

AuthnRequests and single logout requests now fail if the signing and validation certificates are expired.

Unavailable Certificate Authority for CRL Causing an Exception (64456)

Symptom:

After adding LDAP revocation list to the smkeydatabase, decryption of an encrypted SAML 2.0 POST assertion fails and logs an error in the smps.log.

Solution:

This error no longer occurs.

CRL Is Not Checked for Every Transaction as Configured (65541)

Symptom:

If the DBUpdateFreqencyMinutes value in the smkeydatabase.properties file is set to a non-zero value, such as 10, the Certificate Revocation List (CRL) is not read for every transaction.

Solution:

The CRL is now checked for every transaction.

Certificates with Escaped Characters Cause Error for Signed Assertions (65845)

Symptom:

The error "UTF-8 escape sequence: Two characters per hex byte required" occurs when producing a signed assertion using certificates that contain escaped characters.

Solution:

This error no longer occurs when escaped characters are used.

SAML 2.0 and WS-Federation Do Not Verify Timestamps Properly (66044)

Symptom:

SAML 2.0 and WS-Federation authentication schemes were not using the configured SkewTime value to correctly correctly verify timestamps in SAML assertions.

Solution:

The SAML 2.0 and WS-Federation authentication schemes now properly verify timestamps in SAML assertions.

IsPassive Processing at the IdP is Returning an HTTP Error (66333)

Symptom:

The Identity Provider is not sending back a response when an IsPassive directive is received that cannot be satisfied. Instead, an HTTP error is returned.

Solution:

A SAML response is now sent back when an IsPassive directive is received that cannot be honored.

Consumer as a SAML Requester Cannot Retrieve Multi-valued Attributes (80490)

Symptom:

When an Identity Provider acting as an Attribute Authority sends a multi-valued attribute, the Service Provide cannot retrieve the value in a local attribute so the transaction does not execute successfully, logging an error in the smtrace logs "Failed to resolve the variable 'variable-name."

Solution:

The Service Provider can now successfully retrieve multi-valued attributes from the SAML2.0 attribute authority.

Chapter 9: Defects Fixed in the Web Agent 6.x QMR 5 Option Pack

This section contains the following topics:

Fixes for Web Agent 6.x QMR 5 Option Pack

The following are defects fixed for the Web Agent Option Pack.

Custom Error Page Needed for Certain Error Conditions (81128)

Symptom:

Certain error conditions cause Java exceptions to display. There is no mechanism to redirect users to custom error pages instead.

Solution:

Federation Security Services now provides custom error pages. For certain error conditions, FSS redirects users to a defined set of URLs instead of returning HTTP errors.

For more information about custom error pages, see the *Federation Security Services Guide.*

STAR Issue: 17593510

Credential Collector Fails when Target Query Parameter is NULL (89557)

Symptom:

If the value for the Target query parameter in a SAML 1.x single sign-on request or POST is NULL in the string. the SAML credential collector cannot fufill the request.

Solution:

This is no longer an issue. If the Target is NULL, the appropriate error message displays.

STAR Issue: 18328228

Browser Caching SAML 2.0 Assertions (95960)

Symptom:

There is a problem trying to re-post a SAML 2.0 assertion if a user selects the back button in the browser. This is happening because the browser caches the SAML 2.0 assertion.

Solution:

SAML 2.0 assertions can no longer be cached in the browser.

STAR Issue: 18279463

WS-Federation Signature Verification Error for Accented Characters in an Assertion (95586)

Symptom:

In a deployment where ADFS is operating as the Account Partner and Federation Security Services is operating as the Resource Partner, a signed assertion that contains accented characters fails signature verification at the Resource Partner.

Solution:

This is no longer an issue. Accented characters in an assertion are now properly processed during signature verification.

STAR Issue: 18477282

Partially URL-encoded Target Query String Causes Problem for SAML 1.1 POST (97990)

Symptom:

If any part of the TARGET query parameter is URL-encoded, the entire URL becomes URL-encoded in the AUTO POST form. When the encoded URL arrives at the consumer, the request is not processed correctly.

Solution:

Partial URL-encoding of the TARGET query parameter no longer results in the entire URL being encoded.

STAR Issue: 18677920-1

SiteMinder Rejects Assertion if <NameIdentifier> Element is Embedded in the <SubjectConfirmation> Value (51696)

Symptom:

SiteMinder rejects a SAML assertion if the <NameIdentifier> element is put in the XML assertion within the <SubjectConfirmation> value.

Solution:

The search for the <NameIdentifier> has been restricted to only the immediate next child level so this is no longer a problem.

User Not Authorized Before Redirection to the Target Resource (46918)

Symptom:

If you configure a SAML authentication scheme and select Server Redirect as the mode by which the user is redirected to the target resource, the authentication scheme fails to check if the authenticated user is also authorized before redirecting the user to the target resource.

Solution:

To fix this problem, the administrator must define realms, rules, and policies to protect target resources. In Server Redirect mode, the target URL is defined with respect to the context of the FWS servlet that consumes the assertion and not the root of the hosting web or application server. Specifically, realm definitions must start with /affwebservices in the resource filter of the realm.

Assertions Did Not Support Multi-byte Characters (47360)

Symptom:

SiteMinder did not support multi-byte characters in assertions.

Solution:

A SiteMinder SAML producer can now create appropriate SAML assertions containing UTF-8 strings. SiteMinder SAML consumers are now able to consume SAML assertions containing UTF-8 strings.

SAML 2.0 SSO Service Doing IP Checking When the Option Is Not Enabled (53983)

Symptom:

The SAML 2.0 Single Sign-on Service was performing IP checking even though the IP checking feature was not configured.

Solution:

IP checking is no longer performed unless the feature is configured.

Service Provider using SAML 2.0 Artifact Authentication Fails When It Is Behind a Proxy Server (54391)

Symptom:

The Service Provider configured to use a SAML 2.0 artifact authentication scheme fails when the Service Provider sits behind a proxy server.

Solution:

This is no longer an issue.

Web Agent Option Pack Log Shows Incorrect Product Update Version (54584)

Symptom:

In the AffWebServices log, the Web Agent Option Pack was showing the incorrect product update version.

Solution:

This is no longer a problem.

Web Agent Option Pack on Apache 2.x/Linux Fails to Load When the Web Server Starts (54795)

Symptom:

The SAML Affiliate Agent installed on an Apache 2.0 server running Linux fails to load when the Apache web server starts up.

Solution:

The Web Server and Agent start up with no problem.

Target Query String is Not Included in SAML 1.x and 2.0 IsProtected Call (55418)

Symptom:

When a SAML 1.x Consumer and SAML 2.0 Service Provider makes an IsProtected call, they do not include the target query string.

Solution:

The target query string is now included in the call.

Ampersand (&) Missing Between SAMLART and RelayState Query Parameters (55479)

Symptom:

The SAML 2.0 redirection to an Assertion Consumer URL is missing an ampersand (&) between the SAMLART and RelayState query parameters.

Solution:

The ampersand character is no longer missing.

IdP Discovery Redirect is Failing When an AuthnRequest Initiates SSO (55678)

Symptom:

The Identity Provider Discovery redirect is failing when using an AuthnRequest to initiate SAML 2.0 authentication.

Solution:

This is no longer a problem.

FWS Log Incorrectly Displayed Cause of Error (84060)

Symptom:

The FWS log was not correctly displaying the cause of Federation Web Services administration errors, if they occurred.

Solution:

The cause will now properly be displayed.

Single Sign-on Error Messages Displayed in the Browser Were Too Detailed (74355)

Symptom:

When requests to the SAML 2.0 Single Sign-on Service contain incorrect parameters for the Service Provider ID or the protocol binding in the request URL, an error message is displayed in the browser that contains too much detail and might allow an unauthorized user to gain information on which SP ID and protocol bindings are valid.

Solution:

The code has been modified to send a generic error message along with the HTTP error code to the browser and write the SiteMinder error detail only to the FWS Trace log.

SAML 2.0 Autopost Forms Required JavaScript (73858)

Symptom:

SAML 2.0 autopost forms require Javascript to be enabled in the browser for SAML 2.0 federations to work.

Solution:

The autopost forms used for SAML 2.0 have been enhanced so they do not require JavaScript to be enabled in a user's browser. In the case where Javascript is not available, an HTML page is displayed with a Continue butt that user can press to complete the federation.

SMSESSION Cookie Not Marked as Secure when UseSecureCookies Enabled (74449)

Symptom:

During SAML 2.0 federation transaction, the SMSESSION cookie is not marked as "secure" by the Assertion Consumer URL response.

Solution:

Ensure that when an SMSESSION cookie is being set in the user's browser for a SAML 2.0 federation, it is marked as Secure if the UseSecureCookies setting is enabled in the AgentConfigObject corresponding to Federation Web Services.

Transient IP Checking Was Not Operating Properly (75240)

Symptom:

SAML 2.0 single sign-on transaction fails if transient IP Checking is enabled and the Web Agent and the Web Agent Option Pack are running on different machines.

Solution:

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

Error Response to a Misconfigured Artifact Resolve Message Was Empty (74310)

Symptom:

When there is version mismatch between the configured version for the artifact binding in the affiliate object and the version of the artifact resolve request, an empty SOAP envelop is being sent to the SAML Affiliate Agent.

Solution:

When a misconfigured artifact resolve message requests an assertion for the wrong SAML version (such as 1.0 compared with SAML 1.1) a proper SAML error response inside the SOAP envelope is sent instead of sending an empty response.

Web Agent Option Pack on JBOSS Returns HTTP 500 Error (68878)

Symptom:

SAML 1.1 POST authentication fails with a 500 error because JBOSS throws a Java error when the user at the consumer is administratively disabled by SiteMinder.

Solution:

When a user is disabled at the consumer side, Federation Web Services redirects the user to a page that tells the user that he cannot access his account at this time.

Error Message Logged Mistakenly when RelayState Setting is Not Checked (66363)

Symptom:

Informational RelayState trace messages are being logged as errors in the Service Provider affwebserv.log for every request. This message was intended to be a warning and should not appear for every request.

Solution:

An error message is no longer logged every single time an assertion is processed (POST/Artifact) where the RelayState parameter contains a value but the RelayState overrides Target setting is checked in the SAML 2.0 Auth Scheme dialog.

Chapter 10: Defects Fixed in the Policy Server 6.0 SP4 Option Pack

This section contains the following topics:

Fixes for Policy Server 6.0 SP 4 Option Pack

The following are defects fixed for the Policy Server Option Pack.

100 Character Limit for User and DN Attributes Included in an Assertion (46237)

Symptom:

When you specify an Affiliate-HTTP-Cookie-Variable at the producer/Identity Provider to be included in an assertion sent to a consumer/Service Provider, there is a 100 character limit for a User Attribute or a DN Attribute. This limit does not occur when you configure a Static attribute.

Solution:

The character limit has been extended to 1000 characters.

SiteMinder 6.0 SP 3/6.x QMR 3 SAML 1.x Consumer Cannot Consume Assertions from a Producer of a Previous SiteMinder Version (45279)

Symptom:

A SAML 1.x consumer running SiteMinder 6.0 SP 3/6.x QMR 3 or later is unable to consume SAML assertions generated by a producer of an earlier version of SiteMinder.

Solution:

This is no longer an issue.

Relative URL Cannot Be Specified as the Target for Server Redirect Mode (41967)

Symptom:

When configuring the Server Redirect Mode for a SAML authentication scheme, you cannot specify a relative URL for the TARGET parameter.

Solution:

You can now specify a relative URL.

Policy Server Option Pack Variables are Not Accessible in Mixed Mode (44395)

Symptom:

Policy Server Option Pack variables are not accessible from a SiteMinder Policy Server User Interface when the system is running in mixed mode (a 6.x Policy Server running against a 5.x policy store).

Solution:

In mixed mode, the Option Pack variables are now properly accessed without error.

Affiliate Domain Objects Are Not Retrieved and Displayed Correctly (45693)

Symptom:

The affiliate objects are not retrieved and displayed correctly in the Policy Server User Interface.

Solution:

Affiliate domain objects are now correctly retrieved and displayed in the Policy Server User Interface.

The contents of any affiliate domain that were created on a version of the Policy Server running on a Japanese OS prior to 6.0 SP1 will not be displayed as a result of an upgrade to 6.0 SP 4. This is a known limitation of the product.

Error Occurs Using SMKeytool to List Microsoft Client Certificates (47337)

Symptom:

When you try to list Microsoft client certificates using SiteMinder's SMKeytool utility a "No Certificates available.Exception: 15" message is generated. The Microsoft certificates are imported, but they cannot be viewed or used properly with POST profile at the consumer/Service Provider.

Certificates that are created by a Sun Java Systems/Sun ONE Certificate Authority and Open SSL do not have the same issue.

Solution:

This is no longer a problem.

Chapter 11: Defects Fixed in the Web Agent 6.x QMR 4 Option Pack

This section contains the following topics:

Fixes for Web Agent 6.x QMR 4 Option Pack

The following are defects fixed for the Web Agent Option Pack.

SAML 1.x Assertion Not Returned if Affiliate Name has Mixed or Upper Case Letters (44705)

Symptom:

Federation Web Services fails to return an assertion using the SAML 1.x artifact profile if the affiliate name is specified using mixed or upper case characters at the producer or consumer sites.

Solution:

The affiliate name is no longer case sensitive.

SiteMinder 6.0 SP 3/6.x QMR 3 SAML 1.x Consumer Cannot Consume Assertions from a Producer of a Previous SiteMinder Version (45279)

Symptom:

A SAML 1.x consumer running SiteMinder 6.0 SP 3/6.x QMR 3 or later is unable to consume SAML assertions generated by a producer of an earlier version of SiteMinder.

Solution:

This is no longer an issue.

Relative URL Cannot Be Specified as the Target for Server Redirect Mode (41967)

Symptom:

When configuring the Server Redirect Mode for a SAML authentication scheme, you cannot specify a relative URL for the TARGET parameter.

Solution:

You can now specify a relative URL.

Web Server Appends Invalid Character as Part of SAML Response Body (47535)

Symptom:

SiteMinder appears to generate assertions with invalid characters appended to the SAML response body.

Solution:

The invalid characters are appended by web servers or network devices between SiteMinder and the assertion consumer. If SiteMinder is also acting as the consumer, SiteMinder removes the extra characters before parsing the XML body.

Chapter 12: Defects Fixed in the Policy Server 6.0 SP3 Option Pack

This section contains the following topics:

Fixes for Policy Server 6.0 SP3 Option Pack

The following sections list defects fixed for the Policy Server Option Pack.

Issuer URL Must Begin with HTTP for POST Authentication Scheme (42578)

Symptom:

The Issuer URL setting for the SAML POST Authentication Scheme configuration requires that the Issuer URL begin with http. The Policy Server User Interface does not let you enter a URL that does not begin with http.

Solution:

The name of the Issuer URL field has been changed to Issuer. Also, edit constraints were changed so that Issuer is no longer required to start with http. This change reflects that the issuer is not a URL, according to the SAML specification.

Chapter 13: Defects Fixed in the Web Agent 6.x QMR 3 Option Pack

This section contains the following topics:

Fixes for Web Agent 6.x QMR 3 Option Pack

The following sections list defects fixed for the Web Agent Option Pack.

SAML Credential Collector Redirects Users to Incorrect Targets (40123)

Symptom:

For SAML 1.x communication, the SAML credential collector redirects users to target destinations that are outside of the credential collector's own cookie domain.

Solution:

The SAML credential collector now only redirects within its cookie domain.

FWS Attribute Data is Not Propagated (41770)

Symptom:

The Federation Web Services (FWS) application does not propagate user attribute data if it is specified in a generic format in the SAML assertion.

Solution:

Attribute data may be propagated to target applications. In 302 - cookie data redirect mode, Federation Web Services issues a cookie for each generic attribute in a SAML assertion. In server side redirect mode, Federation Web Services passes a HashMap to the target application. The HashMap contains entries for each generic attribute in a SAML assertion; the name of the request attribute is Netegrity.AttributeInfo.

For the following assertion sample, SiteMinder can set attribute values for FirstName and LastName:

```
<saml:AttributeStatement>
        .
        .
        .
 <saml:Attribute AttributeName="FirstName"   AttributeNamespace="AttributeNS">
   <saml:AttributeValue>JOHN</saml:AttributeValue>
     </saml:Attribute>
 <saml:Attribute AttributeName="LastName"    AttributeNamespace="AttributeNS">
    <saml:AttributeValue>SMITH</saml:AttributeValue>
 </saml:Attribute>
</saml:AttributeStatement>
```

Server Certificates with a Key Usage Extension Rejected by SAML Assertion Retrieval Component (42663)

Symptom:

The Web Agent Option Pack expects the SSL server certificate to have digital signature extension set. The SSL standard specifies that digital signature key extension is optional for server certificates.

Solution:

This problem has been fixed.

Chapter 14: Defects Fixed in the Policy Server 6.0 SP2 Option Pack

This section contains the following topics:

Fixes for Policy Server 6.0 SP2 Option Pack

The following is the defect fixed for the Policy Server Option Pack.

SAML ID Values Do Not Conform with XML Scheme (34371)

Symptom:

Assertions contain SAML ID values that do not conform with the XML schema type NCName.

Solution:

The values now conform.

Chapter 15: Defects Fixed for the Web Agent 6.x QMR 2 Option Pack

This section contains the following topics:

Fixes for Web Agent v6.x QMR 2 Option Pack

The following sections list defects fixed for the Web Agent Option Pack.

SAML ID Values Do Not Conform with XML Scheme (34371)

Symptom:

Assertions contain SAML ID values that do not conform with the XML schema type NCName.

Solution:

The values now conform.

Assertions with Multiple HTTP Status Headers Are Not Consumed (34218)

Symptom:

SiteMinder fails to consume SAML assertions if multiple HTTP status headers are found. Also, Federation Web Services fails to connect with WebLogic Application Server over SSL.

Solution:

These issues are no longer a problem.

HTTP Response Body with Extra Characters Prevents SiteMinder from Consuming Assertions (30799)

Symptom:

SiteMinder fails to consume SAML assertions if the HTTP response body includes extra characters. Also, SiteMinder produces SOAP request messages with single quote instead of double quote characters, which cannot be consumed by some SAML consumers.

Solution:

Federation Web Services has been modified so that SiteMinder consumes SAML assertions with extra characters and produces SAML assertions with double quotes.

Back-channel Cert-based Authentication Fails on IIS 5.0 (30929)

Symptom:

Because of a known limitation, the IIS 5.0 Web Agent does not handle in-line client certificates over an SSL connection. When Federation Web Services (FWS) is installed and configured to consume assertions and the customer requires certificate authentication for back-channel requests to the SAML credential collector, the Web Agent is unable to protect FWS.

Solution:

Use the IIS 5.0 Web server to do client certificate authentication. FWS has been modified to obtain the client certificate from the HTTP request on IIS 5.0. This solution requires that the client certificate's subject DN value contain the affiliate name in the CN attribute field.

Federation Web Services Ignores CookieDomain and CookieDomainScope Settings (38373)

Symptom:

The Federation Web Services application ignores the CookieDomain and CookieDomainScope Web Agent parameters, which causes single sign-on to fail in certain configurations.

Solution:

Federation Web Services now uses these configuration parameters.

Federation Web Services Creates SMSESSION Cookie with Missing Data for Secure Proxy Agent (38419)

Symptom:

The Federation Web Services application generates an SMSESSION cookie that lacks the data required for interoperability with the Secure Proxy Agent.

Solution:

The SMSESSION cookie generated by Federation Web Services now contains the necessary data for the Secure Proxy Agent.

Chapter 16: 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.

SiteMinder has been internationalized and localized to the extent indicated in the platform support matrix for SiteMinder r6.0 SP6.

Chapter 17: Documentation

This section contains the following topics:

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.