Release Notes
RSA® Federated Identity Manager 4.2

June 5th, 2013

Introduction

This document lists what's new and changed in RSA Federated Identity Manager. It includes a list of fixed issues and known issues, with workarounds provided for known issues. Read this document before installing the software. This document contains the following sections:

These *Release Notes* may be updated. The most current version can be found on RSA SecurCare® Online at **https://knowledge.rsasecurity.com**.

What's New in This Release

This section describes the major changes introduced in this release. For detailed information on each change, refer to the *Installation and Configuration Guide*.

Database failover. Federated Identity Manager supports database poolers for efficient connection pooling.

Support for Microsoft AD FS 2.0. Federated Identity Manager supports interoperability with Active Directory Federation Services (AD FS) 2.0.

New Supported Application Servers

Apache Tomcat 7.0. Federated Identity Manager can be installed on a Tomcat 7.0 application server with the SuSE Linux Enterprise 11 (64 bit, x86) platform.

Note: Starting in the RSA Federated Identity Manager 4.2 release, RSA will no longer provide Oracle WebLogic Application Server and supporting JRE's to existing and new customers. It will be the customers responsibility to supply these technologies as environmental pre-requisites before deploying (for example, fresh install or upgrade) RSA Federated Identity Manager. RSA Federated Identity Manager will continue to be tested and supported on Oracle WebLogic Application Server and supporting JRE's. Please refer to the RSA Federated Identity Manager data sheet for specific platform details.

Supported Platforms for Application Servers

Federated Identity Manager supports the following application servers:

- **IBM WebSphere 7.0.** Federated Identity Manager can be installed on a WebSphere 7.0 application server with Windows Server 2008 R2 SP1 (64 bit) platform.
- **Oracle WebLogic 10.3.2.** Federated Identity Manager can be installed on a WebLogic 10.3.2 application server with Windows Server 2008 R2 SP1 (64-bit).

- **Oracle WebLogic 10.3.5.** Federated Identity Manager can be installed on a WebLogic 10.3.5 application server with any of the following platforms:
  - SuSE Linux Enterprise 11 (64-bit, x86)
  - SuSE Linux Enterprise 10.3 (64-bit, x86)
- **Oracle WebLogic 10.3.6.** Federated Identity Manager can be installed on a WebLogic 10.3.6 application server with any of the following platforms:
  - Windows Server 2008 R2 SP1 (64 bit)
  - Oracle Solaris 10 (SPARC) (64 bit)
  - Red Hat Enterprise Linux 6 ES (64 bit, x86)
  - SuSE Linux Enterprise 10 SP1 (64 bit, x86)
  - SuSE Linux Enterprise 11 (64-bit, x86)

Supported Datastores

Following list includes the supported datastores:

- PostgreSQL 9.1.x
- Derby 10.8.2
- Oracle RAC 11g R2

Package Contents

Your product CD folder contains:

- Installers for the supported platforms
- License Agreement

Product Documentation

The following documentation is provided with this release in the /docs folder:

Title	Filename
RSA® Federated Identity Manager 4.2 Getting Started	**getting_started.pdf**
RSA® Federated Identity Manager 4.2 Release Notes	**rel_notes.pdf**
RSA® Federated Identity Manager 4.2 Planning Guide	**plan.pdf**
RSA® Federated Identity Manager 4.2 Installation and Configuration Guide	**install_config.pdf**
RSA® Federated Identity Manager 4.2 Troubleshooting Guide	**troubleshooting.pdf**
RSA® Federated Identity Manager 4.2 Security Configuration Guide	**security_config.pdf**

Title	Filename
RSA® Federated Identity Manager 4.2 Administrator's Guide	**admin.pdf**

Fixed Issues

This section lists the issues that have been fixed in this release. The issues are grouped into the following categories:

Issues Fixed in Version 4.2

This section lists the issues that have been fixed in Federated Identity Manager 4.2.

Tracking Number	Description
SAML-4294	Source ID should be based on the user configurable value in the Issuer ID.
SAML-4113	Request qualification of FIM 4.1 on Windows 2008 R2 platform.
SAML-4135 (DOC)	SLO URLS wrong in Installation and Configuration Guide.
SAML-4116 (DOC)	FIM Standalone JNDI URL for SSL in fim.properties is incorrectly specified.

Hotfixes Included in Version 4.2

This section lists the issues that were resolved in FIM 4.1 Hotfix 43, and are included in FIM 4.2.

Hotfix	Description
FIM-HF 41	• The database backup is now the first step, then copy jars followed by restore. • OneTimeUse is now part of idpssosettings in the association.
FIM-HF 42	• Qualified for WebSphere 7.0 over RHEL5.x • The missing classes are included in the rsaIntercepter.jar • The JAVA_HOME can now be passed as argument or as specified in the intall_config.pdf
FIM-HF 43	• Added 'Override Audience Element' option in IDPSSO Settings (saml 2.0) so that IDPs can now override default audience element. • Replaced getUser() with testServer() in getConnection() method in CTAdminApiPool to improve performance.
FIM-HF 44	Removed redundant queries, closed the queries and the persistent managers, enabled lazy loading of FIMConfig objects in the Admin commands and removed the unnecessary looping of FIMConfig objects
FIM-HF 45	Now the Skew in the System Settings page applies to both requests and responses. In case of responses received, it is applied to the NotBefore field before accepting the responses.
FIM-HF 46	FIM querystring parameters are now appended with '&' instead of '?', when the partner's endpoint url already contains some querystring.

Hotfix	Description
FIM-HF 47	• Removed redundant queries, closed the queries and the persistant managers, enabled lazy loading of FIMConfig objects in the Admin commands and removed the unnecessary looping of FIMConfig objects. • Now the Skew in the System Settings page applies to both requests and responses. In case of responses received, it is applied to the NotBefore field before accepting the responses. • FIM querystring parameters are now appended with '&' instead of '?', when the partner's endpoint url already contains some querystring.
FIM-HF 48	• Handled SAML1.1 and SAML2.0 Subject NameId flows in incoming requests (SAMLResponse, AuthRequest, ManageNameIDRequest, LogoutRequest) to set Format as urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified as default. Later processing of NameID element will have this format into effect, this will also fix the plugin loading with unspecified nameID support.
FIM-HF 49	Logout request defect with use of Apache xmlsec.jar file.
FIM-HF 50	• FIM - unicode characters not encoded correctly in WSFEDPOSTBinding.jsp, and POSTBinding.jsp • WSFEDPOSTBinding.jsp XML form values not escaped.
FIM-HF 51	Temporary User Account Management causing performance issues.

New Enhancements in Version 4.2

Tracking Number	Description
SAML-4275	Support for all http cookies be issued with the secure flag set.
SAML-4267	Include option to set secure flag in CTSESSION cookies.

Known Issues

This section describes issues that remain unresolved in this release. Wherever a workaround or fix is available, it has been noted or referenced in detail. For many of the workarounds in this section, you must have administrative privileges. If you do not have the required privileges, contact your administrator.

FIM uses different version of Derby jars instead of one installed with Websphere 7 default installation.

Fix

1. After installing FIM manually or using install script, replace Derby jars shipped with Websphere with the one shipped with FIM.
2. Copy the following files from **<PROFILE_DIR>\rsa-fim-config\lib directory** and replace the jar files in **<APP-SERVER-INSTALL-DIR>\derby\lib** directory:
   - derby.jar
   - derbyclient.jar
   - derbynet.jar
   - derbytool.jar

FIM ships few endorsed jars for Websphere 7.0.

Symptom

FIM ships few endorsed jars for Websphere 7.0.

- Websphere 7 uses only upgrade jars present in **<CDIMAGE>\WAS\WAS7-endorsed-lib** directory.

Fix

1. After installation on Websphere 7, go to **<APP-SERVER-INSTALL-DIR>\java\jre\lib\endorsed** directory and delete the following files:
   - xalan.jar
   - xercesImpl.jar
2. Copy the following files from **CDIMAGE>\WAS\WAS7-endorsed-lib** directory to **<APP-SERVER-INSTALL-DIR>\java\jre\lib\endorsed** directory:
   - xalan-2.7.1.jar
   - xercesImpl-2.9.1.jar
   - xmlsec-1.5.1.jar

Reducing the startup time of Tomcat 7 application server during deployment.

Symptom

Tomcat 7 application server scans all the jar files during deployment, leading to increase in the startup time.

Fix

1. Update the below mentioned list for the following property **tomcat.util.scan.DefaultJarScanner.jarsToSkip** in the **catalina.properties** file.

```
tomcat.util.scan.DefaultJarScanner.jarsToSkip=org.springframework.aop-3.1.1.RELEAS
E.jar,\
org.springframework.asm-3.1.1.RELEASE.jar,\
org.springframework.beans-3.1.1.RELEASE.jar,\
org.springframework.context-3.1.1.RELEASE.jar,\
org.springframework.core-3.1.1.RELEASE.jar,\
org.springframework.expression-3.1.1.RELEASE.jar,\
org.springframework.web.servlet-3.1.1.RELEASE.jar,\
org.springframework.web-3.1.1.RELEASE.jar
```

2. Add one of the below property:
   - Djava.security.egd=file:/dev/./urandom (SystemProperty)

   (or)
   - securerandom.source=file:/dev/./urandom (jre/lib/security/java.security file)
3. Add the following attribute to <web-app> element in the web.xml- <web-app metadata-complete="true">
4. For Authentication Authority verification on Tomcat, remove the axis.jar from demo.war file to avoid Connection Reset Exception.

Menu items are not populating properly with FIM- Admin GUI on Microsoft Internet Explorer version 9

Tracking Number: SAML-4419

Problem: FIM 4.2 Admin GUI's menu items are not accessible in Microsoft Internet Explorer 9 browser due to Cross-Site Request Forgery (CSRF) security guard. The CSRF security guard introduces the javascript error in Microsoft Internet Explorer 9 and the menu items do not populate properly.

Workaround: For Proper Functioning of Admin GUI menus with Microsoft Internet Explorer 9, you must disable the CSRF guard.

FIM is unable to populate elements in fimconfig from database on SUSE11 Patch 0 environment.

Tracking Number: SAML-4375

Workaround: None.

Legacy Known Issues from Version 4.1

Association is saved even without specifying the signing/encryption keystore, in the case of a local entity that supports multiple keystores.

Tracking Number: 73174

Problem: When the user selects multiple keystores for the local entity but does not specify the signing or encryption keystore, while creating an association, the association is saved successfully.

An association with a local entity in the attribute requestor role is saved even if the association uses a signing and encryption policy and the entity does not have a keystore assigned.

Tracking Number: 73175

Problem: An association created between a local entity having the attribute requestor role and a partner entity is saved, even if the association uses a signing and encryption policy and no keystore is selected for the local entity.

WebIDSession plug-in does not verify the user in Authentication Manager on the service provider side.

Tracking Number: 71976

Problem: The WebIDSession plug-in does not verify if users exist in the Authentication Manager on the service provider side before creating the WebIDCookie.

Workaround: Modify the existing plug-in or write a new plug-in with validation code.

User cannot set up SAML 1.1 entity from the dashboard

Tracking Number: 71875

Problem: The user cannot use the Configure My System wizard in the Administration Console to set up a SAML 1.1 entity.

Workaround: To set up a SAML 1.1 entity, click Entities > Local Entities > Add New in the Administration Console.

Import/Export support for SAML 1.1 Source ID

Tracking Number: 72164

Problem: When a SAML 1.1 identity provider has a proprietary Source ID in a Federated Identity Manager 4.1 system, the exported metadata of this entity would not have the Source ID. So the administrator needs to send the Source ID out of band. This has no impact if the partner system does not support importing metadata.

Similarly, when partner metadata is received with a proprietary Source ID, the metadata must be imported into a Federated Identity Manager 4.1 system and then the Source ID must be updated by editing the partner entity.

Workaround: If you need to import a SAML 1.1 partner (hosted on Federated Identity Manager), which has proprietary Source ID, get the Source ID out of band. After importing the partner metadata, manually edit the partner entity to have the desired Source ID.

All the field values are cleared in the page after an error in the page

Tracking Number: 98343

Problem: While configuring plug-ins, if there is an error, the User Interface (UI) screen loses data that was previously entered.

Workaround: Re-enter the configuration data

Unable to delete the Attribute Set

Tracking Number: 98784

Problem: When an attribute set that was previously used by an association, is selected for deletion, the system throws an error message indicating that the attribute set is still being used.

Federation gets deleted even though the user gets an exception

Tracking Number: 72855

Problem: The federation gets deleted even though the system throws an exception.

Workaround: If any transient failure occurs while trying to delete the federation, delete the federation using the admin utility provided.

Single logout does not work after WS-Federation IdP-initiated SSO

Tracking Number: 98226

Problem: The user cannot perform single logout operations on the service provider side after a WS-Federation IdP-initiated single sign-on (SSO) session.

There is no way to verify the metadata signature of a DMX document

Tracking Number: 70163

Problem: While adding a partner entity using a published metadata URL, if the metadata XML is signed, there is no way to verify the validity of the signature.

Workaround: Access the metadata URL and save the document as an XML file. Use this file to create a partner by clicking Entities > Partner Entities > Add Partner Entity.

Discovery will not work with the token sample

Tracking Number: 73163

Problem: IdP Discovery service does not work with the token sample provided.

The demo application and actual federation do not work simultaneously

Tracking Number: 60566

Problem: Federated Identity Manager 4.1 can work with only one web agent plug-in at a time. The web agent plug-in is configured in the System Settings page. Also, the Configure My System wizard creates the right web agent plug-in for ClearTrust and makes relevant changes such that Federated Identity Manager uses the ClearTrust web agent plug-in. The demo application and ClearTrust set up use different web agent plug-ins, so after running the Configure My System wizard, the demo application does not work.

Workaround: After running the Configure My System wizard, if you want to run the demo application, change the fields on the System Settings page to use the demo web agent plug-in. You also need to change the custom web pages in the System Settings page to the relevant demo pages. It may also be helpful to make a note of the configuration values on the System Settings page before running the Configure My System wizard.

Export this page: CSV | Excel | XML" link is boken

Tracking Number: 73386

Problem: When the number of associations or partners in the association or partner listing pages goes beyond 10, the page displays a link to export the listed information to a csv/excel/xml file. This link is broken.

Errata SAML: AllowCreate=false is not handled as per the Errata sepcification

Tracking Number: 60892

Problem: Setting the AllowCreate attribute to "False" throws an exception

Workaround: Always use AllowCreate=true in the very first sign-on request (AuthnRequest). Subsequently, you can use AllowCreate=false.

Spec 2.0 Diff: Partial Logout not supported

Tracking Number: 61006

Problem: Federated Identity Manager 4.1 does not support partial logout.

Workaround: If any transient failure occurs during logout, delete the cookie from the browser.

AP attribute plug-in may not require values in the Attribute Name Mapping fields

Tracking Number: 70069

Problem: When you add an AP attribute plug-in in the Administration Console, you must enter values for the fields in the Attribute Name Mapping section, which are marked as required fields. The AP attribute plug-in may not always require name mapping. You may want to use the same name in the SAML message as in the attribute set.

Workaround: If you do not want any attribute mapping, provide a dummy attribute mapping value while creating the attribute plug-in.

DMX updates for metadata specification compliance

Tracking Number: 69698

Problem: Metadata produced by DMX in a Federated Identity Manager 4.1 system delivers an XML file over HTTP(S) with the following MIME content type: "application/xml". In a strictly followed SAML system, this document may not be good for consumption, because SAML mandates that the content type must be "application/samlmetadata+xml".

Workaround: Browse the DMX URL of your partner using the browser and save the document as an XML file. Use this file to create a partner connection.

After the session expires, NIM still functions properly and the user is not challenged for credentials

Tracking Number: 59109

Problem: After the user session expires, NameID management operations function properly without challenging the user for credentials.

List of service providers that belong to an affiliation should be checked by the identity provider

Tracking Number: 59081

Problem: When an identity provider receives an AuthnRequest with an AffiliationID in it, it should check whether the service provider making the request belongs to that affiliation before issuing a SAML assertion.

Multiple NameIDs in association not required for WS-Federation protocol

Tracking Number: 60764

Problem: For a WS-Federation association, the user may not be required to choose multiple NameID plug-ins in the General Settings page of the association.

Workaround: If the local system is a WS-Federation identity provider, choose the NameID plug-in that corresponds to the preferred NameID format (configured in the association's identity provider settings page). If the local system is a WS-Federation service provider, choose the NameID plug-in that you expect your partner to send as part of the WS-Federation token.

Generic attributes should have XML AttributeValue instead of String values

Tracking Number: 69156

Problem: Generic attributes assume all attributes to be of String type, though the attributes should be of type AttributeValue according to the SAML 1.1 and SAML 2.0 specification.

Workaround: Users can pass attribute values of primitive data types. Primitive data types are integer, string, float, and double. Complex data types such as image, blob, or clob are not supported.

Derby user name and password update

Tracking Number: 63363

Problem: Federated Identity Manager is shipped with a default user name and password for the Derby database. The user cannot change the user name and password.

Assertion API test clients do not work in WebSphere application server and WS interface does not have access control

Tracking Number: 59061

Problem: Test client scripts function when using BEA WebLogic server, but they must be modified to function with the IBM WebSphere application server.

Workaround: Updated test client scripts are provided in the buildtools\assertionapiTestClients directory of the Developer's Guide, available at RSA SecurCare Online.

Association cannot be deleted

Tracking Number: 68698

Problem: Association cannot be deleted from the stack menu that appears in the top frame while editing the association.

Workaround: Delete the association from the associations listing page.

Authentication denied by WebLogic server console in IE while configuring the WebLogic server for Desktop Federation

Tracking Number: 60588

Problem: If you use Desktop Federation (IWA) with WebLogic, the login to the WebLogic console using admin credentials is denied in Internet Explorer 6.0.

Workaround: You can access the WebLogic console with admin credentials from Internet Explorere 7.0 or Firefox.

Proprietary Source ID of a SAML 1.1 identity provider gets overwritten

Tracking Number: 99436

Problem: A SAML 1.1 identity provider (local entity), which has a proprietary Source ID configured on the SAML 1.1 IDP Role page loses the Source ID if the basic data of the entity entity is edited in the Edit Basic UI and saved.

Workaround: Edit the SAML 1.1 identity provider role of the local entity and supply the intended Source ID. This needs to be done every time the user saves the basic data of the entity on the Edit Basics page.

Search based on the Partner Entity name does not work in the Partner Listing page

Tracking Number: 100248

Problem: In the Partner Listing page (Entities > Partner Entities > Manage Existing), the search mechanism does not work as expected when the "name" is used as the search criterion.

Rejecting federation consent throws error message

Tracking Number: 111576

Problem: When the user rejects Federation consent, an error message is displayed.

Not able to delete AR role from SP

Tracking Number: 109620

Problem: Unable to delete AR role from SP local entity.

Attribute plug is not populating attribute values in Assertion

Tracking Number: 110921

Problem: Attribute values are not populating in Assertion .

Authentication Authority Descriptor does not have the KeyDescriptor tag

Tracking Number: 113705

Problem: KeyDescriptor is not present in the Authentication Authority Descriptor.

In the Cluster Environment, Weblogic Built-in Proxy throws NullPointerException

Tracking Number: SAML-4349

Problem: Weblogic Built-in Proxy throws NullPointerException in the Cluster Environment.

Workaround: Use Apache HTTP proxy for load balancing.

Support and Service

RSA SecurCare Online	**https://knowledge.rsasecurity.com**
Customer Support Information	**www.emc.com/support/rsa/index.htm**
RSA Solution Gallery	**https://gallery.emc.com/community/marketplace/rsa?view=overview**

Trademarks