Release Notes
RSA Access Manager 6.1 SP2

July 9, 2010

Introduction

This document lists what's new and changed in RSA Access Manager 6.1 SP2. It includes additional installation information, as well as workarounds for known issues. RSA recommends that you read this document before installing and using RSA Access Manager 6.1 SP2. 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. Or, you can print these *Release Notes*.

To view product documentation delivered in PDF format, you need the Adobe Acrobat Reader. To download the latest version of the Reader, go to www.adobe.com.

Note

The 3.5 RSA ClearTrust Web Server Agents and version 1 tokens are not supported from this release.

RSA Access Manager 6.1 now supports Windows 2008 SP2 operating system.

What's New in This Release

This section describes the major change introduced in this release. For detailed information, refer to the appropriate *RSA Access Manager guide*.

Support for Sybase. RSA Access Manager 6.1 SP2 supports Sybase 15.5 data store server.

Support for Sun Java System Directory Server. RSA Access Manager 6.1 SP2 supports Sun Java System Directory Server 7.0.

Hotfix

The following hotfix was made since RSA Access Manager 6.1 SP1 that has been integrated into RSA Access Manager 6.1 SP2.

Issue	Hotfix	Description
CTSRV-5002	6.0.4.46	When a user (who is also a member of a large static group) is deleted, it takes a very long time for the operation to complete.

^Top

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.

Installing Data Adapter on AD for an AD-ADAM installation

Tracking Number: 39827
Problem: If you choose not to use the Access Manager password policy and follow the procedure in "Optional Attributes for an RSA Access Manager User Entry" on page 73 of the Servers Installation and Configuration Guide, you do not need to install the Data Adapter on AD when setting up an AD-ADAM installation.
Workaround: In this case, do not follow the procedure given in "Installing the Data Adapter on Active Directory" on page 48.

Default value of cleartrust.data.ldap.entitlement.member has changed in the Active Directory

Tracking Number: 39824
Problem: RSA Access Manager 6.0 uses a new default value (ctscMember) for the cleartrust.data.ldap.entitlement.member parameter in ldap.conf when Active Directory is used as a data store. If performing an upgrade installation and this parameter value was not explicitly set previously, you need to set it to the old default value (member) in order to find existing user or group entitlements.
Workaround: Explicitly set the cleartrust.data.ldap.entitlement.member parameter value to member.

Certificate Tool does not accept an underscore character

Tracking Number: 9443
Problem: The Certificate Tool (certool) does not accept any certificate authority common name that includes an underscore character. When attempting to generate a keystore file, the certool prints the error message, "Error generating PKCS#12 file".
Workaround: There is no fix for this problem at this point of time.

Runtime API TOKEN_ERRORs can contain insufficient information

Tracking Number: 9448
Problem: If an API client program passes a broken token to the Runtime API, the API returns insufficient error details. The return values depend on the method called:

- isUserInGroup() and getGroupsForUser() returns an empty map.
- createToken(), getTokenValue(), getTokenValues(), setTokenValue(), setTokenValues(), and validateToken() throws a sirrus.runtime.TokenException.
- All other methods of sirrus.runtime.RuntimeAPI, which take a user argument, return the map with a single entry: { "EXCEPTION_MESSAGE", "<SOME TOKEN ERROR MESSAGE>" }. These methods are authenticate(), authorize(), getUserProperty(), and getUserProperties().

Workaround: There is no fix for this problem at this point of time.

Token problems can occur when running under Linux on VMware

Tracking Number: 20017
Problem: When running the Authorization Server under a Linux guest operating system on top of VMware, the RSA Access Manager token may not be updated as expected in response to Runtime API or Agent requests, even though the interval specified by .notouch_window has elapsed. This is due to a problem in VMware.
Workaround: For information, see this support page on the VMware web site, Clock in a Linux 2.6 Guest Runs Slowly Until Suspended and Resumed.

Special characters in User ID can cause loss of administrative privileges

Tracking Number: 39631
Problem: Administrators with special characters in their User IDs (for example, tom#22) can lose administrative privileges when their profiles are edited.
Workaround: Avoid special characters in User IDs.

Administrative Console fails to work when deployed on WebSphere 6.1

Tracking Number: 116577
Problem: The Administrative Console is not supported on WebSphere 6.1, when the **axm-admin-gui.war** file is deployed with anonymous SSL enabled. This is due to a limitation of Sun JRE 1.5.
Workaround: There is no fix for this problem at this point of time.

Administrative Console and User Self-Service Console is not working

Tracking Number: 121565
Problem: If the Access Manager Application Server Agent and the Administrative Console or the User Self-Service Console is installed on the same application server, the Administrative Console or the User Self-Service console does not work.
Workaround: There is no fix for this problem at this point of time.

User Self-Service Application fails to work when deployed on WebSphere 6.1

Tracking Number: 122735
Problem: The User Self-Service application, when deployed on WebSphere 6.1 does not work if the connection mode is set to Anonymous.
Workaround: There is no fix for this problem at this point of time.

User Self-Service Application fails to work when configured in Authentication mode

Tracking Number: 124935
Problem: If the User Self-Service application is configured in Authentication mode with self-signed PKCS #12 certificates, the WebLogic application server console displays an exception.
Workaround: Perform the following:

1. Go to your ***<domain name>*/bin** directory, where you have installed the User Self-Service application.
2. Open the **setDomainEnv.cmd** file.
3. In the POST_CLASSPATH variable, provide the location of the **cert.jar** file that comes packaged with the User Self-Service application.
4. Restart the WebLogic server.

^Top

Getting Support and Service

RSA SecurCare Online: https://knowledge.rsasecurity.com

Customer Support Information: www.rsa.com/support

RSA Secured Partner Solutions Directory: www.rsasecured.com

^Top

Trademarks

^Top