Release Notes
RSA Access Manager 6.1 SP3

December 15, 2010

Introduction

This document lists what's new and changed in RSA Access Manager 6.1 SP3. It includes additional installation information, as well as workarounds 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 appropriate *RSA Access Manager guide*.

Support for Adaptive Authentication Credential Type. RSA Access Manager 6.1 SP3 supports out-of-band phone Adaptive Authentication credential type.

Support for RSA Adaptive Authentication in SignIn Monitoring Deployment Mode. RSA Access Manager 6.1 SP3 supports RSA Adaptive Authentication SignIn Monitoring deployment mode.

E-mail Notification Support for Authorization Server Cache Leak. During the Authorization Server cache updates, if there is a cache leak, an e-mail notification is sent to the configured e-mail address.

Support for JRE 1.6.0.21. RSA Access Manager 6.1 SP3 has been qualified on Sun JRE 1.6.0.21 and IBM JRE 1.6 SR8 FP1.

Fixed Issues

This section lists the issues that have been fixed as hotfix in this release.

Issue	Hotfix	Resolution
CTSRV-5051	6.1.1.08	When a user is upgrading Access Manager Server 5.5.3 or 6.0 to 6.1 SP1, list of admin groups and password policies are not displayed in the Adminstrator's graphical user interface.
CTSRV-5088	6.1.2.02	When a user enters the user ID, the challenge page is displayed and further the user waits for 5 minutes for RSA Adaptive Authentication timeout and enters invalid answers to the challenge questions, the password page is displayed.
CTSRV-5066 and CTSRV-5041	6.1.2.03	After selecting the Automatically Unlock Users After option in the Default Password Policy field, the administrator user is unable to unlock users who have been locked out due to entering incorrect password more than the specified numebr of times. FAILED_COUNT is not incremented when incorrect password is entered in a specified time.

Issue	Hotfix	Resolution
CTSRV-5117	6.1.2.04	When a user enters the user ID, accesses the challenge questions page, and if the user enters invalid answers to the challenge questions, the password page is displayed.
CTSRV-5147	6.1.2.05	When aserver is configured in readonly mode, it contacts eserver to do failed count updates, causing unnecessary traffic to eserver even when the user authenticates successfully. This hotfix resolves this issue by properly managing the calls to eserver from aserver to do failed count updates.
CTSRV-5182		A single Auth server having problems, resulted in an intermittent interruption of services. Investigation suggested that there were duplicate entries found in the datastore when recovering a user account. There were also NullPointerExceptions generated by the ProtectedURLCache which may be significant.
CTSRV 5125		In addition to handling exceptions that were getting thrown in the eserver debug console and also in logs, a new properly formatted log message has been added. The error messages that appear on the admin GUI are more descriptive now. The following is the new log message format: GMT+05:30,conn=1,op=2,eventID=0a1ff5b815e112874750692920015,messageID =516,ip=127.0.0.1,uname=admin,msg=Login failed,msgtype=READ,user=admin This log message appears in eserver logs (log level 20 or above) when there is a login failure in the Access Manager Administrative Console.

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 77 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 50.

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.

RSA Access Manager integration adapter with RSA Adaptive Authentication OnPremise has a known issue pertaining to re-enrolled user.

Tracking Number: CTSRV-5191

Problem: If a previously unenrolled user reenrolls into the system with new Out of Band phone details, during subsequent Out of Band phone challenge the user is presented with updated phone numbers along with the phone numbers that were provided during earlier enrollment.

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**

Trademarks