

Release Notes

RSA Access Manager Server 6.2 SP2



September 29, 2014

Introduction

This document lists what's new and changed in RSA Access Manager 6.2 SP2. 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:

- [What's New in This Release](#)
- [Supported Platforms From Previous Releases](#)
- [Deprecated Components](#)
- [Fixed Issues](#)
- [Known Issues](#)
- [Support and Service](#)

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, see the appropriate RSA Access Manager Guides.

New user Registration in self-service module. RSA Access Manager Server 6.2 SP2 provides an provision for end user to register himself/herself to AxM system by using the New user registration module in self-service console.

Support to choose challenge method for Adaptive Authentication. RSA Access Manager Server 6.2 SP2 provides the flexibility for the user to select the challenge method while being challenged for Adaptive Authentication.

Support for automated patch upgrade. RSA Access Manager 6.2 SP2 supports automated patch upgrade.

Support for RSA Authentication Manager version 8.1. RSA Access Manager Server 6.2 SP2 supports integration with RSA Authentication Manager version 8.1.

Support for Windows Server 2012 Standard (64 bit) platform. RSA Access Manager Server 6.2 SP2 supports Windows Server 2012 Standard (64 bit) platform.

Support for Active Directory 2012 datastore. RSA Access Manager Server 6.2 SP2 supports Active Directory 2012 datastore.

Supported Platforms From Previous Releases

RSA Access Manager supports the following platforms.

- Microsoft Windows Server 2008 SP2 (x86)
- Microsoft Windows Server 2008 SP2 (x86-64 bit)
- Microsoft Windows Server 2008 R2 SP1 (x86-64 bit)
- Red Hat Enterprise Linux 5.0 (x86-64 bit)
- Red Hat Enterprise Linux 5.5 Enterprise Server (x86-64 bit)
- Red Hat Enterprise Linux 5.5 Enterprise Server (x86)
- Red Hat Enterprise Linux 6.0 (x86-64 bit)

RSA Access Manager Server 6.2 SP2 Release Notes

- Red Hat Enterprise Linux 6.3 (x86-64 bit)
- SUSE Linux Enterprise Server 10 (x86-64 bit)
- SUSE Linux Enterprise Server 11 (x86-64 bit)
- IBM AIX 6.1 PowerPC
- Oracle Solaris 10 (SPARC-64)
- Oracle Solaris 11 (SPARC-64)
- VMware vSphere 5.x

Supported Browsers for Self-Service Console and Admin Console

- Mozilla Firefox
- Microsoft Internet Explorer version 8 and 9
- Google Chrome
- Safari 6.0.5

Deprecated Components

None.

Fixed Issues

This section lists the issues that are fixed in this release under following sub-sections:

- [Fixed Issues in RSA Access Manager 6.2 SP2 Release](#)
- [Hot fixes rolled up in RSA Access Manager 6.2 SP2 Release](#)
- [New Enhancements in RSA Access Manager 6.2 SP2 Release](#)

Fixed Issues in RSA Access Manager 6.2 SP2 Release

None.

Hot fixes rolled up in RSA Access Manager 6.2 SP2 Release

Issue Number	Hot Fix	Description
CTSRV-6186	6.1.4.20	AxM cache issue with getUserProperties call on MSOL with upper case and lower case userID.
CTSRV-6191		Forgot Password flow issues in Self-service.
CTSRV-6131	6.1.4.21	RFE - AxM - Runtime API - LOCKOUT CONTROL calls to be available on RuntimeAPI.
CTSRV-6237	6.1.4.22	AxM 6.1.4 Runtime WebServices logging displays password in cleartext.
CTSRV-6222	6.1.4.23	SC_CUSTOM_DATA not retained.
CTSRV-6276	6.1.4.24	Patch to 6.1.4.21 throws error: SSL Handshake failed: javax.net.ssl.SSLPeerUnverifiedException: peer not authenticated.
CTSRV-6174	6.2.0.09	Session.hijacking=false causes expired session when you try to hit a page after logon.

Issue Number	Hot Fix	Description
CTSRV-6189	6.2.0.10	AxM cache issue with getUserProperties call on MSQl with upper case and lower case userID & certDN.
CTSRV-6230	6.2.0.11	AxM 6.2 Runtime WebServices logging displays password in cleartext.
CTSRV-6233		Code Signing Certificate Got Expired.
CTSRV-6192	6.2.0.12	SNMP alerts do not work with HP OPenview.
CTSRV-6256	6.2.0.13	LDAP failover error happened when LDAP group has a lot of users on Active Directory.
CTSRV-6264	6.2.0.14	ADMINGUI changed redirect behaviour after logging in.
CTSRV-6275	6.2.0.15	Patch to 6.2.0.11 throws error: SSL Handshake failed: javax.net.ssl.SSLPeerUnverifiedException: peer not authenticated.
CTSRV-6209	6.2.1.01	Port HF 6.1.4.20, 6.1.4.21, 6.2.0.09 and 6.2.0.10 to 6.2.1 release branch.
CTSRV-6205	6.2.1.02	RAD/OPenDJ will not work with Mixed case user ids.
CTSRV-6231	6.2.1.03	AxM 6.2 Runtime WebServices logging displays password in cleartext.
CTSRV-6235		Code Signing Certificate Got Expired.
CTSRV-6207		Slow resetting User's Password.
CTSRV-6256	6.2.1.04	Porting the HF 6.2.0.12 to 6.2.1 branch. Porting the HF 6.2.0.13 to 6.2.1 branch.

New Enhancements in RSA Access Manager 6.2 SP2 Release

Issue Number	Description
CTSRV-6212	AxM integration does not support AA API version 7.0
CTSRV-6215	AxM - AxM 6.2.1 is not passing AA 7.1 specific features

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.

Certificate Tool does not accept an underscore character.

Tracking Number: CTSRV-1743

Problem: When attempting to generate a keystore file, the certool prints the error message, "Error generating PKCS#12 file". The Certificate Tool (certool) does not accept any certificate authority common name that includes an underscore character.

Workaround: None.

Runtime API TOKEN_ERRORS contains insufficient information.

Tracking Number: CTSRV-1745

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:

RSA Access Manager Server 6.2 SP2 Release Notes

- `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: None.

Token problems can occur when running under Linux on VMware.

Tracking Number: CTSRV-2983

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.

Server side sorting is not supported for OpenDJ.

Tracking Number: CTSRV-5436

Problem: Server side sorting is not supported for OpenDJ. This is a limitation with SDK.

Workaround: None.

FIPS mode not supported for SecurID Authentication.

Tracking Number: CTSRV-5533

Problem: SecurID is not FIPS 140 compliant. For this reason, FIPS mode cannot be enabled for the Access Manager Server when SecurID authentication is configured.

Workaround: None.

Fix display of Breadcrumb Links on Admin GUI.

Tracking Number: CTSRV-5931

Problem: Breadcrumb links on Admin GUI pages needs to be changed as per UxD GTK standards

Workaround: None

In watcher list m/c Bind device option is displayed in the passcode page.

Tracking Number: CTSRV-6009

Problem: Remember me checkbox is displayed on the user's watcher machine list.

Workaround: None

uus.conf is added during upgrade to 6.2 even if Unique User Session is not configured in 6.1.

Tracking Number: CTSRV-6010

Problem: As per the expected behavior for upgrade, if Unique User Session is not configured in 6.1, the related conf file (`uus.conf`) should not be added to the conf folder in upgraded 6.2 servers.

Workaround: None

Special symbols appear in License agreement in the installers.

Tracking Number: CTSRV-6016

Problem: When you read through the license agreement in the installers, you will find some special symbols.

Workaround: None.

Apply Re-skinning to Online Help UI on the Access Manager Admin GUI.

Tracking Number: CTSRV-6022

Problem: The Online Help UI of Admin GUI does not have the same look-and-feel as the re-skinned UI.

Workaround: None

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

Copyright © 2014 EMC Corporation. All Rights Reserved.

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC trademarks, go to www.rsa.com/legal/trademarks_list.pdf.