07.06.16

RSA Access Manager Server 6.2 SP4 Release Notes

This document summarizes the features of RSA Access Manager Server 6.2 SP4 (Access Manager Server). It outlines the new features, platform information, and resolved and known issues.

Contents:

New Features

There are no new features in this release of Access Manager Server.

Changes

This release of Access Manager Server is designed to include the following changes:

- Support for RSA BSAFE® Crypto-J 6.2 (Crypto-J) and RSA BSAFE SSL-J 6.2.

  Refer to Crypto-J Security Policies for the supported algorithms and other FIPS related information.
- Support for RSA Common Security Toolkit (CST) 3.3.0.5.

  For Solaris, only CST v3.3.0 is supported.
- Support for RSA Adaptive Authentication 7.2 and 7.3.
- Support for Microsoft SQL Server 2014.
- Support for Novell SUSE Linux Enterprise Server 12.
- Fixes for specific issues.
  For more information, see Enhancements and Resolved Issues.

Supported Components

This section lists the versions of the components this release of Access Manager Server is designed to support. For installation and configuration information for these components, see the *RSA Access Manager Server Installation and Configuration Guide*.

Supported Operating Environments

This release of Access Manager Server is designed to support the following operating environments:

- Microsoft® Windows® Server 2008 SP2, 32-bit and 64-bit
- Microsoft Windows Server 2008 R2 SP1, 64-bit
- Microsoft Windows Server 2012 R2, 64-bit
- Microsoft Windows Server 2012 Standard, 64-bit
- Red Hat® Enterprise Linux 6.6, 64-bit
- Red Hat Enterprise Linux 7.0, 64-bit
- Novell® SUSE® Linux Enterprise Server 10, 64-bit
- Novell SUSE Linux Enterprise Server 11, 64-bit
- Novell SUSE Linux Enterprise Server 12, 64-bit
- IBM® AIX® 6.1 PowerPC®, 64-bit
- IBM AIX 7.1 PowerPC, 64-bit
- Oracle® Solaris® 10 on SPARC® v9, 64-bit
- Oracle Solaris 11 on SPARC v9, 64-bit
- VMware vSphere 5.x.

Platform-specific Issues

For customers developing applications using Access Manager Server C SDK on a Microsoft Windows operating system, the C-runtime DLLs are built using Microsoft Visual Studio® 2010 SP1, which requires the Microsoft Visual C++ 2010 SP1 Redistributable Package. On systems with an:

- x86 (32-bit) processor, the Redistributable Package (x86) is available at https://www.microsoft.com/en-au/download/details.aspx?id=8328
- x86_64 (64-bit) processor, the Redistributable Package (x64) is available at https://www.microsoft.com/en-au/download/details.aspx?id=13523

Discontinued Platforms

In this release, there are no discontinued platforms.

For subsequent releases of Access Manager Server going forward, where a vendor discontinues mainstream support for an operating system and platform combination, RSA discontinues support from the same date.

Supported Application Servers

This release of Access Manager Server is designed to support the following application server software for the User Self-Service Console and Administrative Console:

- Apache™ Tomcat™ 7.0 and 8.0
- IBM WebSphere® Application Server 7.0 and 8.0
- Red Hat JBoss® Enterprise Application Platform 6.2
- Oracle WebLogic® Server 11gR1 (10.3.6) and 12cR2 (12.1.3).

Note: Starting with Access Manager Server 6.2, RSA no longer provides Oracle WebLogic Application Server and supporting JDK's to existing and new customers. It is the customers responsibility to supply these technologies as environmental pre-requisites before deploying (for example, a fresh install or upgrade) Access Manager Server. Access Manager Server continues to be tested and supported on Oracle WebLogic Application Server and supporting JDK's. For specific platform information, see the Access Manager Server data sheet.

Supported Data Store Servers

This release of Access Manager Server is designed to support the following data store software:

SQL:

- Oracle Database SQL Language Reference 11g R2, 11g R2 RAC, and 12c
- Sybase® Adaptive Enterprise Server 15.5
- Microsoft SQL Server 2008, 2008 Release 2, 2012 SP2 and 2014.

LDAP:

- Microsoft Active Directory on Windows Server 2008, Windows Server 2012, and Windows Server 2012 R2
- Microsoft Active Directory Lightweight Directory Services on Windows Server 2008. This is in addition to existing support for Active Directory

- Microsoft Active Directory in combination with Microsoft Active Directory Lightweight Directory Services on Microsoft Windows Server 2008
- Oracle Directory Server 11.1.1.7.0
- Novell eDirectory 8.8.0
- OpenDJ 2.4.3 and 2.6.

Supported Browsers

This release of Access Manager Server is designed to support the following browsers for the User Self-Service Console and Administrative Console:

- Apple® Safari® 6.0.5
- Google™ Chrome™
- Microsoft Internet Explorer® 11
- Mozilla® Firefox®.

Discontinued Browsers

In this release, support is discontinued for Microsoft Internet Explorer 8, 9 and 10.

For subsequent releases of Access Manager Server going forward, where a vendor discontinues mainstream support for a browser, RSA discontinues support from the same date.

Supported Java Development Kit

From Access Manager Server 6.2 and later, the Java Development Kit (JDK) is not part of the standard shipment.

Ensure you use either a 32-bit or 64-bit JDK on a 64-bit operating system, and a 32-bit JDK on a 32-bit operating system.

This release of Access Manager Server is designed to support the following JDKs:

- IBM JDK 1.6 and 1.7
- Oracle JDK 1.7 and 1.8.

Note: Access Manager Server no longer supports Oracle JDK 1.6.

To successfully use the stronger cipher suites and encryption algorithms, the Unlimited Strength Jurisdiction Policy Files must be downloaded and installed. The JDK vendor and version determines the Jurisdiction Policy File to download.

Supported Access Manager Agents

This release of Access Manager Server is designed to support Access Manager Agent 5.0.x.

Supported Authentication Manager

This release of Access Manager Server is designed to support RSA Authentication Manager 8.1.

Supported Certificate Manager

This release of Access Manager Server includes a limited-license release of RSA Certificate Manager 6.8.

Supported Adaptive Authentication

This release of Access Manager Server is designed to support RSA Adaptive Authentication 7.2 and 7.3.

This release of Access Manager Server and Access Manager Agent 5.0 SP4 are compatible with Adaptive Authentication 7.2 and 7.3.

Enhancements and Resolved Issues

The following tables list the enhancements and resolved issues in this and previous releases of Access Manager Server.

Table 1 Enhancements and Resolved Issues

ID	Description
CTSRV-6608	Support for Novell SUSE Linux Server 12.
CTSRV-6587	Support for Adaptive Auth On-Premise 7.3.
CTSRV-6579	Support for Microsoft SQL Server 2014.
CTSRV-6560	Email recipients for password policy alerts get wiped when the ctrust service is reset.
CTSRV-6546	Support for Adaptive Auth On-Premise 7.2.
CTSRV-6545	Struts artifacts Upgrade for User Self-Service Console.
CTSRV-6543	Upgrade commons-collections.jar.
CTSRV-6535	The Authentication Server Watcher thread does not return a connection after validation.
CTSRV-6522, CTSRV-6003	Spring Framework artifacts upgrade for Access Manager.
CTSRV-6495	Upgrade CST library.
CTSRV-6479	Impact of Logjam Vulnerability.
CTSRV-6462	Access Manager SMTP Personal Address is hard coded to `ClearTrust System`.
CTSRV-6176	Deprecation of FIPS 186-2 algorithms. Use HMACDRBG256.
CTSRV-6065	Instrumentation Server logs a large volume of '=Row failed to update' errors.
CTSRV-5856	The `aserverMuxRequestPoolTable` should return only a single row.
CTSRV-5512	Add a startup switch to display full server version.

Table 2 Enhancements and Resolved Issues in release 6.2.2.0.7

ID	Description
CTSRV-6589	Administrative API `setSecretQuestionAnswers` is restricted to the Super Administrator. Request Non-Super Administrator ability to set secret question and answers.

Table 3 Enhancements and Resolved Issues in release 6.2.1.0.2

ID	Description
CTSRV-6224	Need Octal datatype support for LDAP Attribute - Object GUID. Required to support Office 365 Integration.

Table 4 Enhancements and Resolved Issues in release 6.2.0.20

ID	Description
CTSRV-6521	`ClassCastException` causes critical aserver failure

Known Issues

The following table lists the known issues in this release of Access Manager Server:

Table 5 Known Issues

ID	Description
CTSRV-6607	In the User Self-Service Console, the vulnerability CVE-2016-0785 "Forced double OGNL evaluation, when evaluated on raw user input in tag attributes, may lead to remote code execution" exists. **Workaround:** This vulnerability can be mitigated by adding the following `<constant>` tag inside `<struts>` tag available in the *selfservice-gui\WEB-INF\classes\struts.xml* file. `<constant name="struts.excludedClasses" value="java.lang.Object, java.lang.Runtime, java.lang.System, java.lang.Class, java.lang.ClassLoader, java.lang.Shutdown, java.lang.ProcessBuilder, ognl.OgnlContext, ognl.ClassResolver, ognl.TypeConverter, com.opensymphony.xwork2.ognl.SecurityMemberAccess, com.opensymphony.xwork2.ActionContext" />`
CTSRV-6591	The Administrative Console is unable to load class files from WEB-INF when deployed on Weblogic 12c. **Workaround:** Copy the *jcm-6.2.jar* present in the `WEB-INF/lib` directory to the respective `WLS_DOMAIN/lib` directory and restart the Weblogic Servers.
CTSRV-6566	The Patch Installer is dependent on the v6.2 installation. In v6.2, the `lockbox file` field name is not validated. Any modification of the default lockbox file name will result in a failure in the patch installation. **Workaround:** Ensure the lockbox file is created in the `/conf` directory prior to executing the patch installer.
CTSRV-6459	As part of the Access Manager Server qualification with JBoss EAP 6.2, deployment of the Administrative Console WAR file fails. **Workaround:** Deploy the WAR file manually by exploding it into a WAR folder, as specified in the JBoss Administrators Guide (https://docs.jboss.org/author/display/AS7/Admin+Guide#AdminGuide-FileSystemDeployments).
CTSRV-6022	Apply re-skinning to the Online Help UI on the Administrative Console. The Online Help UI of Administrative Console does not have the same look-and-feel as the re-skinned UI.
CTSRV-6016	There are special symbols present in License agreement in the installers.

Table 5 Known Issues

ID	Description
CTSRV-6010	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.
CTSRV-6009	In watcher list m/c Bind device option is displayed in the passcode page. The checkbox is displayed on the user's watcher machine list.
CTSRV-5931	Breadcrumb links on the Administrative Console pages must be changed as per UxD GTK standards.
CTSRV-5533	FIPS mode cannot be enabled for the Access Manager Server when SecurID authentication is configured.
CTSRV-5436	Server side sorting is not supported for OpenDJ. This is a limitation with the SDK.
CTSRV-2983	When running the Authorization Server under a Linux guest operating system on top of VMware, the 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 the support page on the VMware web site.
CTSRV-1745	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()`.
CTSRV-1743	When attempting to generate a keystore file, the Certificate Tool prints the error message, "Error generating PKCS#12 file". The Certificate Tool does not accept any certificate authority common name that includes an underscore character.

Documentation

The Access Manager Server documentation suite includes:

- This document, the *RSA Access Manager Server Release Notes*, in Portable Document Format (PDF), with the latest information on Access Manager Server.
- The *RSA Access Manager Server Administrator Guide* in PDF, with information to assist system administrators who need to plan, install and configure a Access Manager Server implementation.
- The *RSA Access Manager Server API Delta Document*. Provides information about the differences between previous and current versions of the APIs included with Access Manager Server.
- The *RSA Access Manager Server Developers Guide*. Provides information about developing custom programs using application programming interfaces (APIs) included with Access Manager Server.
- The *RSA Access Manager Server Getting Started,* in PDF. Lists the kit components (packages, licenses and documentation) and specifies the location of documentation in the installation kit.
- The *RSA Access Manager Server Installation and Configuration Guide*, in PDF, with instructions on how to install and configure Access Manager Server.
- The *RSA Access Manager Server Planning Guide,* in PDF. Provides a general understanding of Access Manager Server, its high-level architecture, its features, and deployment information.
- The *RSA Access Manager Server Security Configuration Guide,* in PDF. Provides an overview of the settings available in Access Manager Server and compatible Agents to ensure secure operation of the product.
- The *RSA Access Manager Server Troubleshooting Guide,* in PDF. Provides an overview of the settings available in Access Manager Server, RSA Access Manager Agent (Access Manager Agent), and their components to help ensure secure operation of the product.
- The *RSA Access Manager Server Upgrade Guide,* in PDF. Provides information about how to upgrade previous versions of Access Manager Server, data store schema, and data to the current version.
- The following online Help documents, in HTML:
  - The *RSA Access Manager Server Administrative Console Help*. Provides instructions on how to perform specific administrative tasks. To view Help, click the Help tab on Administrative Console screen.
  - The *RSA Access Manager Server User Self Service Console Help*. Describes day-to-day user tasks performed in the User Self-Service Console. To view Help, click the Help tab on the User Self-Service Console.

RSA Customer Support

Access these locations for help with your RSA product:

- RSA SecurCare Online

  RSA SecurCare Online offers a knowledge base that contains answers to common questions and solutions to known problems. It also offers information on new releases, important technical news, and software downloads.

- RSA Customer Support

  The RSA Customer Support site contains information on RSA support programs plus an extensive Content Library of product-related documents such as datasheets, guides and whitepapers.

- RSA Ready

  RSA Ready is a platform for customers, partners, and RSA enthusiasts to learn about products certified to interoperate with RSA products including access to integration guides.

Before You Call Customer Support

Make sure you have direct access to the computer running your RSA product software.

Please have the following information available:

- ❑ Your RSA Customer Serial Number.
- ❑ The software version number of your RSA product.
- ❑ The make and model of the machine on which the problem occurs.
- ❑ The name and version of the operating system under which the problem occurs.