Release Notes
RSA Authentication Agent API 8.6 for Java

August 2016

Revision 1

Introduction

The RSA Authentication Agent Application Programming Interface (API) 8.6 for Java enables developers to integrate RSA SecurID into custom or third-party applications. Use the RSA Authentication API 8.6 to integrate with Authentication Manager 8.1 Service Pack 1 or later.

This document lists what's new and changed in RSA Authentication Agent API 8.6 for Java as well as known issues. Read this document before installing the software. This document contains the following sections:

JDK Support

As of August 2016, the RSA Authentication Agent Application Programming Interface (API) 8.6 for Java supports the following versions of OpenJDK and the Oracle Java Platform, Standard Edition:

- Oracle JDK 1.6
- Oracle JDK 1.7
- OpenJDK 1.7
- Oracle JDK 1.8
- OpenJDK 1.8 on 64-bit systems

The *RSA Authentication Agent API 8.6 for Java Developer's Guide* will be updated in the next release.

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 *RSA Authentication Agent API 8.6 for Java Developer's Guide*.

FIPS Support

RSA Authentication Agent API 8.6 for Java includes the FIPS-compliant cryptographic library module RSA BSAFE® Crypto-J 6.1.3.3 (NIST Certificate # 2057). RSA Authentication Agent API 8.6 uses the Crypto-J 6.1.3.3 library that inherits its FIPS 140-2 status from the RSA BSAFE Crypto-J JSAFE and JCE Software Module 6.1. For more information, see the *RSA BSAFE Crypto-J JSAFE and JCE Software Module Security Policy Level 1* document at **https://community.rsa.com/docs/DOC-35791**.

Federal Information Processing Standards Publication 140-2 - Security Requirements for Cryptographic Modules (FIPS 140-2) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the NIST website: **http://www.nist.gov/**.

RSA Authentication Agent API 8.6 incorporates libraries that were independently audited by the NIST certified laboratory Gossamer laboratories Inc., an independent accredited lab under the National Voluntary Laboratory Accreditation Program (NVLAP Lab Code 200997-0). The base version of the cryptographic library incorporated into Authentication Manager was certified as FIPS compliant. This covers all algorithms that were required to be tested at the time of the certification.

RSA Authentication Agent API 8.6 incorporates Federal Information Processing Standards (FIPS)-compliant cryptographic library modules. The **lib** folder in the kit includes three files for FIPS support: **cryptojce-6.1.3.3.jar**, **crytocommon-6.1.3.3.jar**, and **jcmFIPS-6.1.3.3.jar**. The API requires all three files. A non-FIPS mode is not supported.

New Java Methods

The new RSA Authentication Agent API includes new Java Methods:

- **AuthSessionFactory::getAuthSDKVersion()** returns the version of the Authentication Agent SDK.
- **ServerInfo::getAddresses()** returns all of the IPv4 and IPv6 addresses for an RSA Authentication Manager replica instance.

Support for LINUX and Windows

This release supports Red Hat Enterprise Linux, SUSE Linux, and Microsoft Windows. Additional platform support will be provided in a future release. For more information, see the *Developer's Guide*.

Direct Migration from the SDK 8.1 and 8.5

You can migrate to SDK 8.6 from either SDK 8.1 or SDK 8.5. You can reuse your existing agent code which uses APIs from version 8.1 and 8.5. For information, see the *Developer's Guide*.

IPv6 Support

RSA Authentication SDK 8.6 implements the TCP protocol, instead of the traditional UDP protocol. RSA Authentication SDK 8.6 allows agent hosts to be on an IPv4, IPv6, or a dual-stack machine.

For information on the differences between the TCP protocol implemented in the SDK 8.6 and SDK 8.5, and the UDP protocol implemented in SDK 8.1, see the *Developer's Guide*.

Software Development Kit Contents

When you download and extract the SDK (.tar file), the SDK creates the directory structure outlined in the following table.

Directory	Contents
\doc\AuthAgentAPI_DevGuide	Contains *RSA Authentication Agent API 8.6 for Java Developer's Guide*.
\doc\Javadoc	Contains *RSA Authentication Agent API 8.6 Javadoc*
\examples	Contains the sample code, which includes examples that can be used to invoke the AuthAPI function calls and test the status of Authentication Manager.
\lib	Includes the libraries required for each of the supported operating systems.
\util	Contains the agent_nsload utility.

Product Documentation

The *RSA Authentication Agent API 8.6 for Java Developer's Guide* is included in the kit. Open **index.htm** in the **\doc\AuthAgentAPI_DevGuide** directory.

Fixed Issues

AAJAVA-311 — Fixed a load balancing issue. In certain circumstances, if the first RSA Authentication Manager server in the round-robin load balancing sequence was unreachable, the connection would fail, instead of failing over to the next server configured in **sdconf.rec**.

Known Issues

AceStatus does not display server status

Tracking Number: AAJAVA-374
Problem: Server status is not implemented in this release.
Workaround: There is no workaround for this issue.

IPv6 addresses are not supported for the RSA RADIUS Server

Tracking Number: AAJAVA-372
Problem: RSA RADIUS does not support IPv6 addresses on the server. In RSA Authentication Manager 8.1 Service Pack 1 or later, only RSA RADIUS clients can use IPv6 addresses.
Workaround: There is no workaround for this issue.

Error occurs when over 1000 authentications are attempted concurrently on a single instance

Tracking Number: AAJAVA-270
Problem: Some authentications do not succeed when too many authentications are attempted concurrently.
Workaround:

1. Do one of the following:
   - Add a replica instance.
   - Login to the AM server using SSH and locate **/opts/rsa/am/server/config/**.
2. Increase the max-open-sock-count property value to 2000 for biztier in the **config.xml** file.
3. Restart the processes with **/opt/rsa/am/server/rsaserv restart all**.

Support and Service

You can access community and support information on RSA Link at **https://community.rsa.com**. RSA Link contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

The RSA Ready Partner Program website at **www.rsaready.com** provides information about third-party hardware and software products that have been certified to work with RSA products. The website includes Implementation Guides with step-by-step instructions and other information on how RSA products work with third-party products.

Trademarks

Intellectual Property Notice