

Release Notes

RSA Authentication Agent API 8.5.1 for C



Introduction

The RSA Authentication Agent Application Programming Interface (API) 8.5.1 for C enables developers to integrate RSA SecurID into custom or third-party applications. Use the RSA Authentication Agent API 8.5.1 for C to integrate with Authentication Manager 8.x.

This document lists what's new and changed in RSA Authentication Agent API 8.5.1 for C, as well as workarounds for known issues. Read this document before installing the software. This document contains the following sections:

- [Software Development Kit Contents](#)
- [Product Documentation](#)
- [Fixed Issues](#)
- [Known Issues](#)
- [Support and Service](#)

Software Development Kit Contents

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

Directory	Contents
<code>\doc</code>	Contains the RSA Authentication Agent API 8.5 for C Developer's Guide in PDF format (auth_agent_API_C_dev_guide). This guide provides an overview of the RSA Authentication Agent API for C, and describes all the functions in detail.
<code>\inc</code>	Contains the header files required for integrating with the Authentication API.
<code>\lib</code>	Includes the libraries required for each of the supported operating systems.
<code>\samples</code>	Contains samples that illustrate the application of the API.
<code>\src</code>	Contains files used to modify the Message Catalog for windows and non-windows.
<code>\util</code>	Contains <code>acestatus</code> , <code>acetest</code> , and <code>ns_load</code> utility.

Product Documentation

The following documentation is in the *Auth SDK* in the `\doc` directory.

Title	Filename
<i>Developer's Guide</i>	<code>\doc\auth_agent_API_C_dev_guide.pdf</code>

Fixed Issues

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

AAC-695 — New PIN authentication through Citrix Web Interface failed when the Authentication Agent API was in TCP mode.

AAC-698 — Authentication failed in deployments with more than one instance if services were stopped on either the primary or replica instance.

AAC-704 — AceGetUserSelectable returned an incorrect value for a user's PIN creation method.

AAC-706 — In a planned promotion or disaster recovery situation, an agent sometimes attempted to contact an RSA Authentication Manager server that was no longer available, and the agent could not authenticate until the original message key expired.

AAC-708 — In some cases, Acelnitalize could not be called a second time if the first call failed.

AAC-786 — The implementation of the asynchronous APIs of RSA Authentication Agent API/SDK 8.5 and 8.6 for C did not properly handle error status for callback methods.

Known Issues

This section describes issues that remain unresolved in this release.

The agent auto-registration utility (sdadmreg) is not compatible with Authentication Agent API 8.5 or later versions

Tracking Number: AAC-784

Problem: Authentication Agent API 8.5 and later versions do not support integration with the agent auto-registration utility (sdadmreg).

Workaround: No workaround is available for this issue.

Intermittent connection problems occur when TCP agents using the Authentication Agent API attempt authentication with an Authentication Manager 8.2 SP1 Patch 4 instance that has been updated from version 8.2 SP1 Patch 2

Tracking Number: AAC-785

Problem: Due to a key negotiation error, TCP agents using the Authentication Agent API sometimes cannot connect to an Authentication Manager 8.2 SP Patch 4 instance that has been updated from version 8.2 SP1 Patch 2.

Workaround: No workaround is available for this issue.

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.

Copyright © 1994-2017 Dell Inc or its subsidiaries. All Rights Reserved.

November 2017

Trademarks

RSA, the RSA Logo, SecurID, and EMC are either registered trademarks or trademarks of Dell Inc throughout the world. All other trademarks used herein are the property of their respective owners. For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

Intellectual Property Notice

This software contains the intellectual property of Dell Inc or is licensed to Dell Inc from third parties. Use of this software and the intellectual property contained therein is expressly limited to the terms and conditions of the License Agreement under which it is provided by or on behalf of Dell Inc.

Open Source License

This product may be distributed with open source code, licensed to you in accordance with the applicable open source license. If you would like a copy of any such source code, EMC will provide a copy of the source code that is required to be made available in accordance with the applicable open source license. EMC may charge reasonable shipping and handling charges for such distribution. Please direct requests in writing to EMC Legal, 176 South St., Hopkinton, MA 01748, ATTN: Open Source Program Office.