Readme
RSA Authentication Manager 6.1

October 26, 2005

Introduction

This document lists known issues, and includes other important information about RSA Authentication Manager 6.1. Read this document before installing the software. This document contains the following sections:

This *Readme* may be updated. The most current version can be found on RSA SecurCare Online https://knowledge.rsasecurity.com.

Known Issues

RSA RADIUS Server Support

RSA RADIUS Server 6.1 is not supported on HP or IBM AIX operating systems. For RSA RADIUS platform support, see the *RSA RADIUS Server 6.1Administrator's Guide*.

RSA RADIUS Server 6.1 does not support cross-realm authentication.

Tracking Number: 19263

RSA RADIUS Server installer -p option does not work. You must use TCP port 1813 (the default) as the administration communication port.

Tracking Number: 20188

If you make administrative changes on a Primary RADIUS Server at the same time that a Replica RADIUS Server is being nominated to become the new Primary, the changes are lost on the original Primary.

Workaround: Inform all administrators that you are nominating a Replica to become the new Primary RADIUS Server in the realm, and that they must terminate all administrative sessions on the original Primary.

RADIUS Server Does Not Uninstall When Uninstalling RSA Authentication Manager

Tracking Number: 19095

Problem: On UNIX and LINUX platforms, if a Primary RADIUS Server is on the same machine as a Replica Authentication Manager, the Primary RADIUS Server does not uninstall when you uninstall the Replica Authentication Manager. In addition, users will not be able to authenticate to the Primary RADIUS Server after you uninstall the Replica Authentication Manager.

Workaround: Do one of the following before you uninstall the Replica Authentication Manager:

- If you have Replica RADIUS Servers as part of a realm, nominate a Replica RADIUS Server to replace the original Primary RADIUS Server before you uninstall the Replica Authentication Manager. For more information, see the *RSA RADIUS Server 6.1 Administrator's Guide*.
- If you do not have a Replica RADIUS Server that you can nominate, reinstall the Primary RADIUS Server on a different machine before uninstalling the Replica Authentication Manager.

RSA RADIUS Server Administration Data Fields Do Not Update

Tracking Number: 20143

Problem: When you add a Replica RADIUS Server, the information for that Server is not updated in the RSA RADIUS Server Administration interface.

Workaround: Click **Refresh** after you add a Replica RADIUS Server.

RSA RADIUS Server Starts Automatically When Installed From Command Line

Tracking Number: 20104

Problem: When you install RSA RADIUS Server using the command line utility, it automatically starts as soon as the installation completes.

Workaround: Change the RSA RADIUS Server startup type from “Automatic” to “Manual”.

Windows Password Information Does Not Update When Offline Authentication is Unavailable

Tracking Number: 16941

Problem: When a user performs a local authentication and **Enable Offline Authentication at system level** checkbox is cleared, a user’s password may not be updated on the Windows Agent.

Workaround: Restart the Local Authentication Client computer.

Offline Authentication Service Port Must Be Changed Manually

Tracking Number: tst00041788

Problem: If you enable offline authentication at the system level, the database load utility uses port 5580 by default. Changing the authentication service port number on the Primary, then creating and sending a new Replica package to the Replicas, does *not* change the port number on the Replicas.

Workaround: To change the port number for this service to avoid conflicts with a third-party service, use the Configuration Management application on the Primary and on all Replicas.

Upgrading to Windows XP SP2 Closes Firewall Port Needed for Downloading Offline Data

Tracking Number: 13413

Problem: Upgrading machines running RSA Authentication Agent for Microsoft Windows to Windows XP SP2 enables the Windows Firewall, and closes port numbers 2334 and 2335, which are used to download offline logon data to the domain controller and the domain client.

Workaround: Perform the following procedure:

1. Click **Start** > **Control Panel**.
2. Click **Windows Firewall**.
3. Click the **Exceptions** tab.
4. Click **Add Port**.
5. In the Add a port dialog box, type **sdoad** in the **Name** box, and **2334** (on a domain client) or **2335** (on a domain controller) in the **Port number** box.
6. Click **TCP**.
7. Click **OK**.
8. Click **OK** again.

Automated Log Maintenance Fails to Create Archive File

Tracking Number: 14472

Problem: When configuring Automated Audit Log Maintenance, the name of the log archive file can contain letters and numbers only. Make sure the filename does not contain any of the following characters:

* “ < > |

RSA Authentication Manager accepts these characters, but does not create the archive file.

Workaround: Specify a name that contains letters and numbers only.

Cannot Replicate Database After Changing the Primary Name or IP Address

Tracking Number: 14994

Problem: When you change the name or IP address of the Primary, and Push DB-Assisted Recovery is enabled, the Replicas do not accept any changes from the Primary.

Workaround: Generate the Replica Package and manually deliver it to the Replica, or add the following environment variable to each Replica system: ACE_ALLOW_TAKEOVER, and set its value to 1. This environment variable allows the Replica to communicate with the Primary after you change the Primary name or IP address.

Upgrade Removes apidemon.ini File

Tracking Number: 19805

Problem: The upgrade from Authentication Manager 6.0 to Authentication Manager 6.1 on Windows machines removes the **apidemon.ini** file, which contains configuration settings for the Administration Toolkit and Quick Admin.

Workaround: Before performing the upgrade, back up **apidemon.ini**, typically located in **%SystemRoot%\system32** on the Primary or Replica. After the upgrade is complete, restore the backup copy of **apidemon.ini** to **%SystemRoot%\system32**.

sddump Fails if a Dump File Already Exists

Tracking Number: 21358

Problem: On Linux platforms, **sddump** fails if **sdserv.dmp** or **sdlog.dmp** already exists in ***ACEPROG***.

Workaround: Before running **sddump**, remove any existing **sdserv.dmp** or **sdlog.dmp** from ***ACEPROG***.

Documentation Items

RSA Authentication Manager 6.1 Administration Toolkit Reference Guide

Tracking Number: 19533

On page 209, the description of the port parameter for **Sd_SetAgentHostRADIUSInfo** states that the default RADIUS Server Agent Host connection port is 1830. The correct default port is 1813.

RSA Authentication Manager 6.1 Administrator's Guide

Tracking Number: 18966

On page 353, the error message "Iteration count out of range" does not include a trapping identification number. The number for this message is 1157.

Tracking Number: 16691

On page 141, under "Backing Up Data While RSA Authentication Manager Programs Are Running," the document states that the system prompts you before overwriting the backup file if one already exists. In fact, the system overwrites the backup file without warning.

RSA Authentication Manager 6.1 Administration Help

Tracking Number: 19900

In the Help topic "Getting Started with RSA Authentication Manager," the link to "Starting and Stopping the RSA Authentication Manager" opens the wrong topic. In addition, the topic that opens, "Starting and Stopping the RSA RADIUS Server," contains outdated information. The following instructions are correct.

To start or stop RSA RADIUS Server processes on the Primary:

1. Click **Start > Programs > RSA Security > RSA Authentication Manager Control Panel**.
2. In the Control Panel menu, click **Start & Stop RSA Authentication Manager Services**.
3. To automatically start RSA RADIUS Server when you start the authentication engine, under Service Management, select **Start and stop RADIUS Server together with authentication engine**. Then, under **Start Services**
   - To start all services, click **Start All**.
   - To stop all services, click **Stop All**.

4. To start and stop just RSA RADIUS Server, under Service Management, make sure **Start and stop RADIUS Server together with authentication engine** is not selected. Then, under **Start Services**
   - To start RSA RADIUS Server, click **Start RADIUS**.
   - To stop RSA RADIUS Server, click **Stop RADIUS**.

Getting Support and Service

RSA SecurCare Online: https://knowledge.rsasecurity.com

Customer Support Information: www.rsasecurity.com/support

Trademarks