The Security Division of EMC

RSA Authentication Manager 7.1 SP2 Deployment Guide

This document provides instructions on upgrading an RSA Authentication Manager 7.1 deployment to Service Pack 2 (SP2).

Verify the Package Contents

The RSA Authentication Manager 7.1 SP2 Upgrade Kit can be either physical media or a download from RSA SecurCare Online. The kit contains:

- RSA Authentication Manager 7.1 Database Patch for your platform
- RSA Authentication Manager 7.1 SP2 Patch for your platform
- RSA Authentication Manager 7.1 SP2 for your platform (This is the full installation kit.)

Prepare for the Upgrade Process

Before you can upgrade RSA Authentication Manager 7.1 to SP2, complete the tasks in the following sections:

- "Remove Remote Databases and Server Nodes"
- "Configure All Server Instances and Remote RSA RADIUS Servers to Use a Time Server"
- "Identify Your SP2 Upgrade Process and Maintenance Window"
- "Gather the Installation Prerequisites"
- "Review All Release Notes"
- "Prepare to Create Backups Before and After You Install Each Update"

Remove Remote Databases and Server Nodes

RSA Authentication Manager 7.1 SP2 discontinues support for remote databases and server nodes. For information on removing these features from your deployment, contact RSA Customer Support. See "Getting Support and Service" on page 6.

Configure All Server Instances and Remote RSA RADIUS Servers to Use a Time Server

Configure all server instances and remote RSA RADIUS servers to use a Network Time Protocol (NTP) server. Synchronizing the system time on all server instances and remote RSA RADIUS servers prevents authentication failures and replication issues.

Important: If the time on a server instance or remote RSA RADIUS server differs from Coordinated Universal Time (UTC) by more than 10 minutes, contact RSA Customer Support before you do this procedure. See "Getting Support and Service" on page 6.

To configure a server instance or a remote RSA RADIUS server to use an NTP server:

1. Stop all RSA Authentication Manager services.
2. Synchronize the system time with the NTP server time.
3. Start all Authentication Manager services.
4. Repeat this procedure on all server instances and remote RSA RADIUS servers in the deployment.

For more information on these steps, see the *RSA Authentication Manager 7.1 Installation and Configuration Guide*.

Identify Your SP2 Upgrade Process and Maintenance Window

Identify your SP2 upgrade process for existing RSA Authentication Manager 7.1 server instances and remote RSA RADIUS, as well as new replica instances and remote RSA RADIUS.

Existing Server Instances

The following table shows all possible upgrade processes from RSA Authentication Manager 7.1 to RSA Authentication Manager 7.1 SP2.

Note: These time estimates are approximate. If you are installing an update on Solaris, add 45 minutes to each estimate for service startup.

RSA Authentication Manager 7.1 Server Instances	Upgrade Process	Estimated Installation Time
RSA Authentication Manager 7.1	1. Install the RSA Authentication Manager 7.1 Database Patch sequentially on all server instances. (If this patch has already been installed, you do not need to reinstall it.) **Note:** You must install the RSA Authentication Manager 7.1 Database Patch on all server instances before you install RSA Authentication Manager 7.1 SP2 Patch.	2 hours
	2. Install the RSA Authentication Manager 7.1 SP2 Patch sequentially on all server instances.	1 hour
Remote RSA RADIUS	No installation required.	

If you have more than one instance, your deployment can authenticate users during the upgrade process.

During an installation, users with tokens in New PIN mode may not be able to authenticate.

New Replica Instances and Remote RSA RADIUS Servers

To install a new replica instance or remote RSA RADIUS server:

1. Upgrade all server instances to RSA Authentication Manager 7.1 SP2.
2. Install the replica or remote RSA RADIUS using the RSA Authentication Manager 7.1 SP2 CD or download. (This full installation kit has the same updates that are included in the patches.)

For instructions on installing replica instances or remote RSA RADIUS, see the *RSA Authentication Manager 7.1 Installation and Configuration Guide*. For more information on locating this document, see "Locating the Documentation Set" on page 6.

Gather the Installation Prerequisites

To upgrade RSA Authentication Manager 7.1 to version 7.1 SP2, the following items are required.

Note: You must have an RSA SecurCare Online logon account to download the following required documentation and required updates.

Required Documentation

Download the following documents:

- *RSA Authentication Manager 7.1 Database Patch Release Notes:*
  https://knowledge.rsasecurity.com/docs/rsa_securid/rsa_auth_mgr/71db1/auth_manager_database_patch_release_notes.html
  (Required only if the RSA Authentication Manager 7.1 Database Patch has not been installed)
- *RSA Authentication Manager 7.1 SP2 Patch Release Notes*:
  https://knowledge.rsasecurity.com/docs/rsa_securid/rsa_auth_mgr/71sp2/auth_manager_SP2_release_notes.html
- *RSA Authentication Manager 7.1 Download Verification Guide*:
  https://knowledge.rsasecurity.com/docs/rsa_securid/rsa_auth_mgr/71sp2/download_verification_guide.pdf
  (Required only if you are downloading the updates from RSA SecurCare Online)

Required Updates

These updates are included in the RSA Authentication Manager 7.1 SP2 Upgrade Kit. If you do not have the physical media, download the following:

- RSA Authentication Manager 7.1 Database Patch for your server platform
  (Required only if the RSA Authentication Manager 7.1 Database Patch has not been installed)
- RSA Authentication Manager 7.1 SP2 Patch for your server platform
- RSA Authentication Manager 7.1 SP2 for your server platform

Required Administrative Access

You must have the following accounts to complete the upgrade process.

- **On Windows**:
  - Windows logon account that belongs to the Local Administrators group and was used to install RSA Authentication Manager 7.1
  - RSA Operations Console logon account
  - Super Admin account
  - Master password for the deployment

- **On Linux/Solaris**:
  - Root logon account
  - Logon account that was used to install RSA Authentication Manager 7.1
  - RSA Operations Console logon account
  - Super Admin account
  - Master password for the deployment

Review All Release Notes

Before you begin the upgrade process, read the release notes carefully. They contain instructions on installing the required updates, as well as lists of enhancements, fixed issues, and known issues.

Prepare to Create Backups Before and After You Install Each Update

You must create a backup using the RSA Operations Console before and after you install an update. Instructions for creating backups are provided in the release notes.

Before you install an update, you must create a backup. RSA Customer Support can use this backup to restore your deployment if an update fails.

When you finish installing an update, you must create another backup. This backup becomes your working backup.

When you complete the upgrade process, you should resume your normal backup routine.

Upgrade Your Deployment to SP2

To upgrade your deployment to SP2:

1. Install the RSA Authentication Manager 7.1 Database Patch sequentially on all server instances in the deployment. For instructions, see the *RSA Authentication Manager 7.1 Database Patch Release Notes*.

   Note: You must install the RSA Authentication Manager 7.1 Database Patch on all server instances before you proceed to the next step.

2. Install the RSA Authentication Manager 7.1 SP2 Patch sequentially on all server instances in the deployment. For instructions, see the *RSA Authentication Manager 7.1 SP2 Patch Release Notes*.

Locating the Documentation Set

The RSA Authentication Manager 7.1 SP2 documentation set is available on the RSA Authentication Manager 7.1 SP2 CD or download (from RSA SecurCare Online) in the **documentation** folder. The documentation includes updated instructions for installing and attaching replicas, as well as documentation enhancements and bug fixes.

Getting 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**

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

The RSA Secured Partner Solutions Directory provides information about third-party hardware and software products that have been certified to work with RSA products. The directory includes Implementation Guides with step-by-step instructions and other information about interoperation of RSA products with these third-party products.

©2009 RSA Security Inc. All rights reserved.

October 2009
P/N 5638A0

Trademarks

RSA and the RSA logo are registered trademarks of RSA Security Inc. in the United States and/or other countries. For the most up-to-date listing of RSA trademarks, go to **www.rsa.com/legal/trademarks_list.pdf**. EMC is a registered trademark of EMC Corporation. All other goods and/or services mentioned are trademarks of their respective companies.