

# **RSA Authentication Manager 7.1 Sample Migration**



**The Security Division of EMC**

## **Contact Information**

Go to the RSA corporate web site for regional Customer Support telephone and fax numbers: [www.rsa.com](http://www.rsa.com)

## **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](http://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.

## **License agreement**

This software and the associated documentation are proprietary and confidential to RSA, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

## **Third-party licenses**

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed in the [thirdpartylicenses.pdf](#) file.

## **Note on encryption technologies**

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

## **Distribution**

Limit distribution of this document to trusted personnel.

## **RSA notice**

The RC5™ Block Encryption Algorithm With Data-Dependent Rotations is protected by U.S. Patent #5,724,428 and #5,835,600.

# Contents

- Preface**..... 5
  - About This Guide..... 5
  - Getting Support and Service ..... 5
    - Before You Call Customer Support..... 6
- Chapter 1: Introduction**..... 7
  - About the Migration Procedure..... 7
- Chapter 2: Capturing Current Data**..... 9
  - Dumping the Database and Log Files ..... 9
  - Copying Selected Program Files..... 13
  - Transferring Files to Your New Installation..... 14
- Chapter 3: Testing the Migration** ..... 15
- Chapter 4: Performing the Migration**..... 21
  - Preparing the RSA Authentication Manager 7.1 Server ..... 21
  - Backing Up the RSA Authentication Manager 7.1 Database ..... 21
  - Migrating the RSA Authentication Manager 6.1 Database ..... 23
  - Migrating the Log Files..... 27
- Appendix A: Restoring the RSA Authentication Manager 7.1 Database**..... 29



# Preface

---

## About This Guide

This guide provides information for migrating data from RSA Authentication Manager 6.1 to a newly installed instance of RSA Authentication Manager 7.1 on a Windows server.

The guide supplements, but does not replace, the *RSA Authentication Manager 7.1 Migration Guide*. Administrators can use this guide to get an overview of the migration procedure. However, RSA recommends that you consult the *Migration Guide* before migrating to a production deployment of RSA Authentication Manager 7.1.

Topics such as migrating RSA RADIUS data or data from an LDAP directory are not covered in this guide. Also, it does not provide information on the issues that might arise in cleaning up data prior to migration. For more information, see the *RSA Authentication Manager 7.1 Migration Guide*.

---

## Getting Support and Service

RSA SecurCare Online	<a href="https://knowledge.rsasecurity.com">https://knowledge.rsasecurity.com</a>
Customer Support Information	<a href="http://www.rsa.com/support">www.rsa.com/support</a>
RSA Secured Partner Solutions Directory	<a href="http://www.rsasecured.com">www.rsasecured.com</a>

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.

## Before You Call Customer Support

Make sure that you have direct access to the computer running the RSA Authentication Manager software.

Please have the following information available when you call:

- Your RSA Customer/License ID. You can find this number on your license distribution media, or in the RSA Security Console by clicking **Setup > Licenses > Status > View Installed Licenses**.
- The RSA Authentication Manager software version number.
- 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.

# 1

## Introduction

This chapter provides a high-level overview of the migration from RSA Authentication Manager 6.1 to RSA Authentication Manager 7.1.

---

### About Migration Planning

RSA Authentication Manager 7.1 introduces a number of new features that enhance and simplify the administration of an Authentication Manager deployment. Among these are security domains, server nodes, and linking to an external identity source (instead of copying and periodically synchronizing user records). A complete list of the RSA Authentication Manager 7.1 changes is included in the *RSA Authentication Manager 7.1 Migration Guide*.

Simply migrating RSA Authentication Manager 6.1 data to version 7.1 is a straightforward process. However, you must devise a strategy for re-creating the behavior of your existing deployment in the version 7.1 environment and for how to take advantage of the version 7.1 features to improve your deployment.

For example, RSA Authentication Manager 7.1 allows you to use only user groups when restricting access to authentication agents, rather than configuring an agent to admit or exclude individual users. To re-create your previous access restrictions, you need to add users to user groups, and reconfigure the agents with the appropriate group access restrictions.

Configuring access to agents is only one of the issues you need to consider as part of a migration strategy. For example, you need to consider whether you want to migrate all or just some of your current data, how you will handle the assignment of users to identity sources in the upgraded deployment, and whether you want to migrate data into a particular version 7.1 security domain.

---

### About the Migration Procedure

This guide describes a sample migration procedure. It is intended as an orientation for the migration planning process. After you read this guide, read the *RSA Authentication Manager 7.1 Migration Guide*, and plan your approach carefully before performing an actual migration.

The migration described in this guide is limited to the following situation:

- RSA Authentication Manager 7.1 is newly installed on a Windows server.
- The migration involves data from an RSA Authentication Manager 6.1 primary server, without RADIUS or any LDAP synchronization jobs.

The migration procedure described in the following chapters consists of these basic steps:

1. Capture data from the RSA Authentication Manager 6.1 deployment, and copy it to the Windows server where RSA Authentication Manager 7.1 is installed.
2. Test the migration without actually changing the version 7.1 instance.
3. Perform and verify the migration.

The actual migration, simply illustrates the migration procedure. You might want to perform an actual migration in a test bed. RSA recommends that you do not migrate to a production deployment until you have read the *Migration Guide* and developed your strategy.



# 2

## Capturing Current Data

This chapter describes the procedure for capturing data from your RSA Authentication Manager 6.1 primary server.

You must capture:

- The Authentication Manager database
- The Authentication Manager log files
- Certain program files that Authentication Manager needs to use the data

---

### Dumping the Database and Log Files

You need to shut down Authentication Manager when you perform the dump procedure so that the dump is an accurate snapshot of the database. Try to schedule the dump procedure for a time that is the least disruptive, and warn users of the temporary outage.

- 
1. Log on as an administrator to the server where RSA Authentication Manager 6.1 is installed.
  2. Create a directory, for example, C:\temp\dump.

---

**Note:** Because a data dump has a default destination, it is not essential to create this directory. However, it is convenient to place all the files needed for the migration in the same directory.

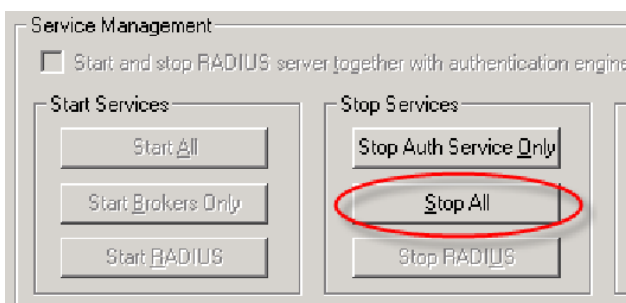
---

3. Click **Start > Programs > RSA Security > RSA Authentication Manager Control Panel**.



4. On the RSA Authentication Manager Control Panel page, click **Start & Stop RSA Auth Mgr Services**.

5. In the Service Management dialog box, click **Stop All**.

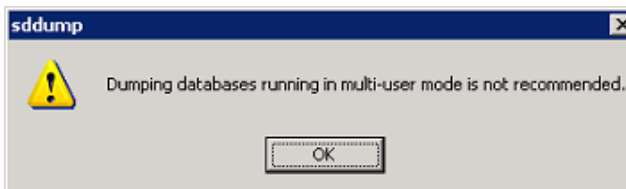


6. Click **Close**.

7. On the RSA Authentication Manager Control Panel page, click **Exit**.

8. To open the database dump utility on the Windows server, click **Start > Programs > RSA Security > RSA Authentication Manager Database Tools > Dump**.

A warning appears recommending that you stop all Authentication Manager services.

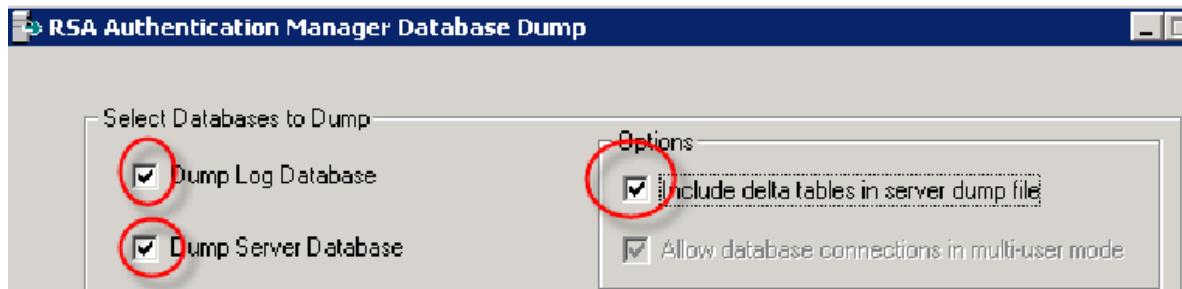


9. Click **OK**.

The Authentication Manager Database Dump page is displayed.

10. Under **Select Databases to Dump**, select the following to capture all your data:

- **Dump Log Database**
- **Dump Server Database**
- **Include delta tables in server dump file**

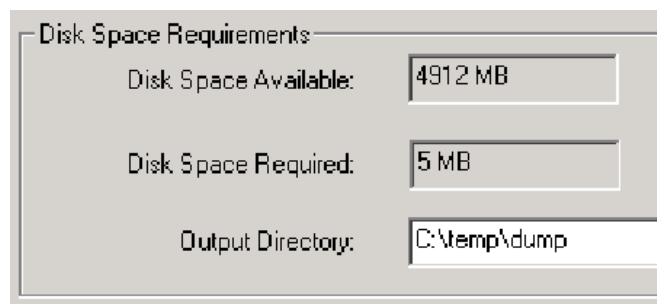


**Note:** The delta tables contain data in the primary server database that has not yet been replicated to replica servers.

11. Under **Disk Space Requirements**, do the following:

- Verify that there is sufficient disk space for the dump.
- In the **Output Directory** field, specify the directory you created in [step 2](#).

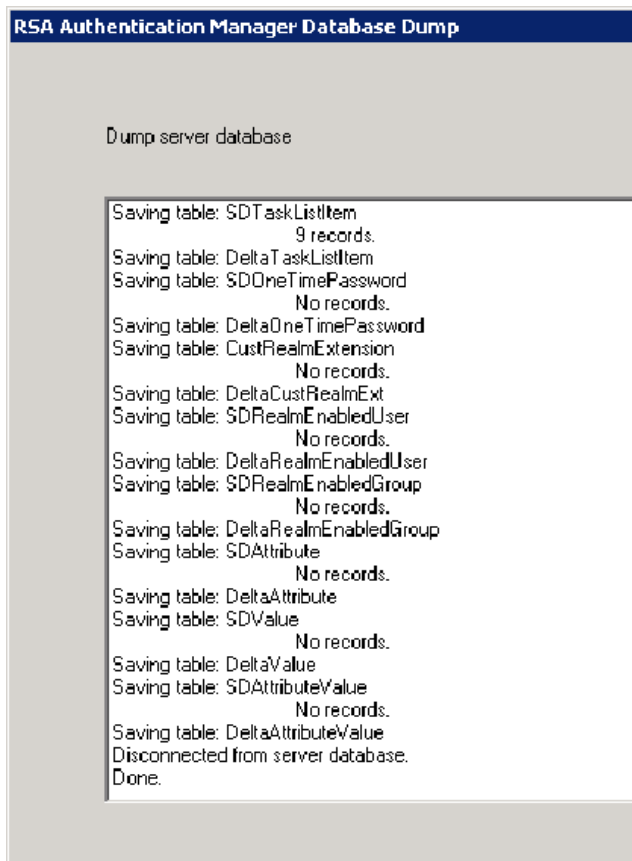
**Note:** If you specify a directory other than the default destination, make sure the directory exists.



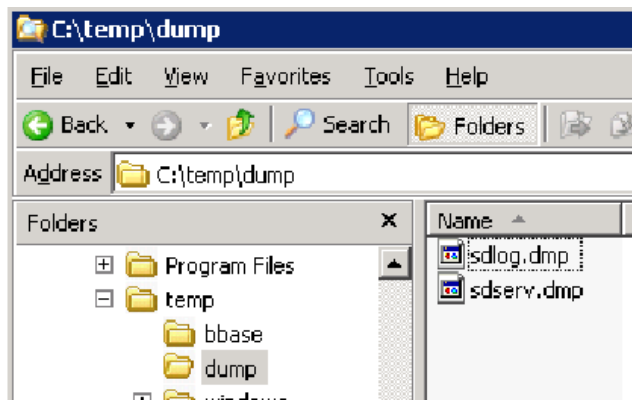
12. Click **OK**.

The RSA Authentication Manager Database Dump page is displayed.

13. When the dump is complete, do one of the following:
  - Click **Close** to exit the database dump utility.
  - Click **Save As**, specify a path to save the status report, and click **Close**.



- **sdserv.dmp** - the database file
- **sdlog.dmp** - the logs file



## Copying Selected Program Files

Certain program files must accompany the RSA Authentication Manager 6.1 data to the new version. For example, the license.rec file is always required. In some situations, other files are needed as shown in the following table.

The following table lists the program files, each with its location and purpose. If you are gathering the migration-related files in a single directory, such as C:\temp\dump, copy the file or files there.

The following files are located in the Authentication Manager installation directory. By default, this directory is **C:\Program Files\RSA Security\RSA Authentication Manager**.

File	Purpose	Location
<b>license.rec</b>	The RSA Authentication Manager 6.1 license file. It decrypts certain fields in the database.	<b>\data\license.rec</b>
<b>startup.pf</b>	This file specifies the language used by the system. Copy this file if your deployment uses Chinese, Japanese, Korean, or Spanish.	<b>\rdbms32\startup.pf</b>
<b>active.map</b> <b>sunone.map</b>	These files specify the location of LDAP directories containing user information. Copy one or both of these files if you are migrating LDAP user data.	<b>\utils\toolkit\active.map</b> <b>\utils\toolkit\sunone.map</b> [not used in this sample migration]
<b>cert7.db</b> <b>key3.db</b>	These certificates are required to establish SSL connections to LDAP directory servers. Copy both of these files if you are migrating LDAP user data.	<b>\data\cert7.db</b> <b>\data\key3.db</b> [not used in this sample migration]

---

## Transferring Files to Your New Installation

Your migration-related directory on the RSA Authentication Manager 6.1 server now contains the following files:

- **sdserv.dmp**
- **sdlog.dmp**
- **license.rec**
- [optional program files]

Transfer these files to a directory on the server where RSA Authentication Manager 7.1 is installed, for example, C:\temp\dump.

# 3

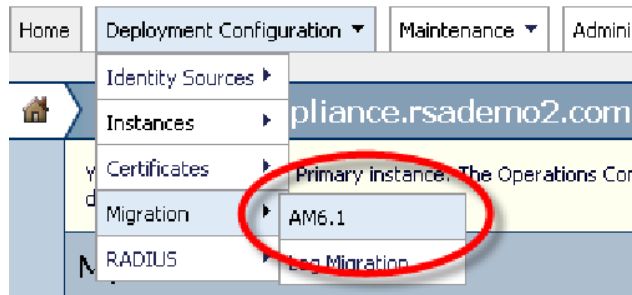
## Testing the Migration

A test migration shows you a migration without actually changing the RSA Authentication Manager 7.1 instance in any way. The test migration procedure generates a report that details the changes an actual migration would make.

The test migration is usually an iterative process. That is, you normally perform the test two or more times, checking for and correcting data problems in between iterations.

This chapter describes the steps for performing a test migration from RSA Authentication Manager 6.1 to version 7.1.

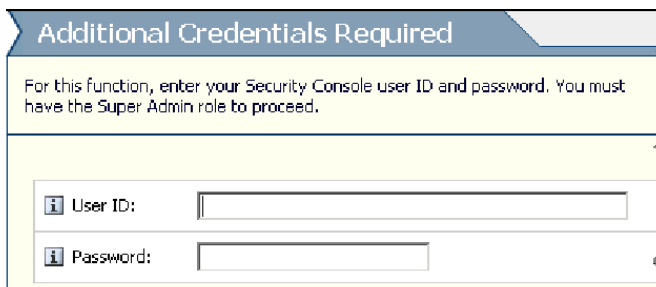
1. Log on to the RSA Operations Console.
2. Click **Deployment Configuration > Migration > AM6.1**.



The Additional Credentials Required page is displayed.

**Note:** You must be a Super Admin to perform this task.

3. Log on again.



The Upload Files page is displayed.

- On the Upload Files page, specify the location of the files you copied from RSA Authentication Manager 6.1, or click **Browse** to search for them.

### Upload Files for Authentication Manager 6.1 Log Migration

	Database Dump File Location: *	<input type="text" value="C:\temp\dump\sdserv.dmp"/>	<input type="button" value="Browse..."/>
	License Record Location: *	<input type="text" value="C:\temp\dump\license.rec"/>	<input type="button" value="Browse..."/>
	Language of Installation:	<input type="checkbox"/> Installing in Japanese, Chinese, Korean, or Spanish	

- Click **Scan Dump File**.

- On the Scan Results page, verify that the data found in the dump file is the data that you want to migrate.

### Scan Results

Found (migrated by default):	<ul style="list-style-type: none"> <li>● Agents</li> <li>● Custom Extensions</li> <li>● Users</li> <li>● Tokens</li> <li>● Groups</li> </ul>
Found (optionally migrated):	<ul style="list-style-type: none"> <li>● Administrative Roles</li> <li>● Delta Records</li> <li>● System Settings</li> </ul>
Not Found:	<ul style="list-style-type: none"> <li>● One-Time Passwords</li> <li>● RADIUS Profiles</li> <li>● Cross Realm</li> </ul>

- In the **Migration Mode** section, select **Custom Mode**.

- Click **Next**.

\*  Typical Mode (Migrate all objects found in scan with settings)

Custom Mode (Selectively migrate objects found in scan, perform test migration and other settings)

Rolling Upgrade Mode (Migrate delta records only)

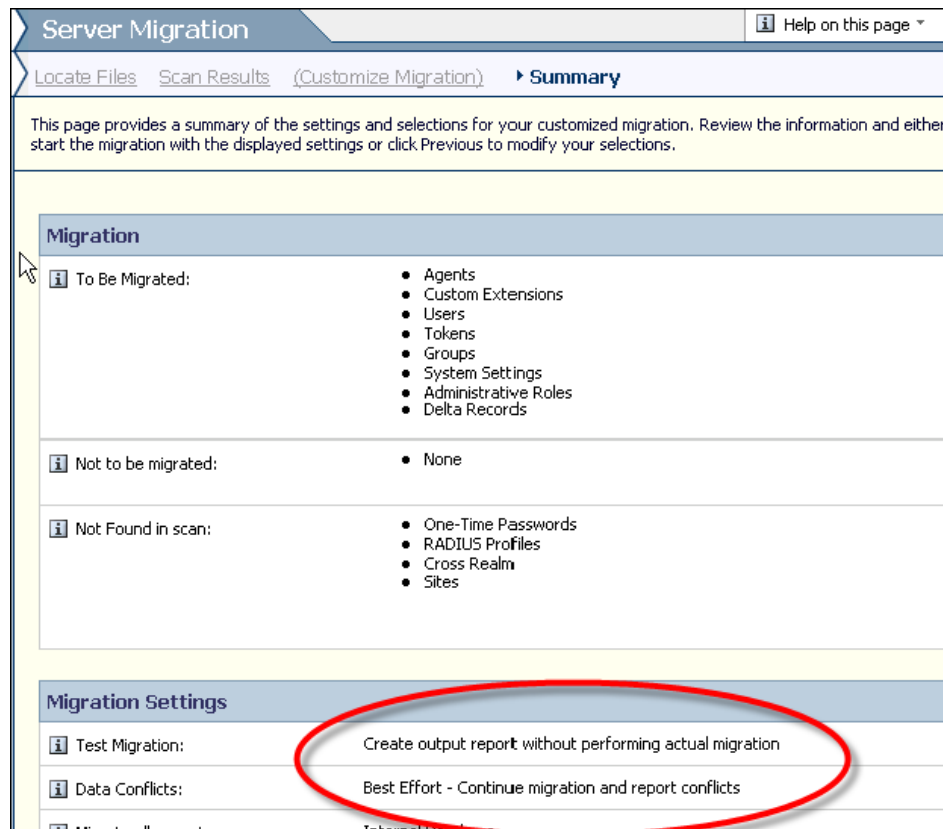


9. On the Migration Settings page, select **Create output report. . .**



10. Click **Next**.

The Server Migration page is displayed, showing a summary of the parameters you chose for the migration (including the defaults).



11. At the bottom of the page, click **Start Test Server Migration**.

The Server Migration Status page is displayed, showing the progress of each migration task.

Server Migration Status	
Task ( 8 of 38 )	
1. Analyzing Dump File	
2. Unsupported character check	
3. System settings	

When the test migration is complete, the Test Server Migration Results page is displayed.

12. In the **Migration Report** section, click the report that you want to view. You can also save the reports to your hard drive.

The migration reports alert you to possible problems with the RSA Authentication Manager 6.1 data.

13. Click **Done**.

Migration was successful.

#### Summary

- Migration completed successfully
- User "kflanagan" cannot be activated on an open agent "saalem.arist"
- User "ebcadmin" cannot be activated on an open agent "saalem.arist"
- System settings from AM 6.1 have been applied to this installation.
- User "mhuckaby" cannot be activated on an open agent "saalem.arist"
- AM61 task lists have been migrated to administrative roles. Please r administrative roles

#### Next Steps

- Review migrated admin roles: Administration -> Administrative Roles
- Review migrated system settings: Setup -> Authentication Methods Authentication Manager

#### Migration Report

	Results Directory:	C:\Program Files\RSA Security\RSA Authentic \080213050512
	Report:	<a href="#">migration_summary.html</a>
	Verbose Report:	<a href="#">migration_detail.zip</a>

---

14. If data problems are reported, return to RSA Authentication Manager 6.1 to resolve them.

---

**Note:** For information on solving data problems, see the *RSA Authentication Manager 7.1 Migration Guide*.

---

---

15. After fixing any data problems, repeat the test migration procedure until you are satisfied with the results.

---



# 4

## Performing the Migration

This chapter describes the procedure for migrating the data from an RSA Authentication Manager 6.1 primary server to a newly installed instance of RSA Authentication Manager 7.1 on a Windows server.

You can review this chapter as part of the migration planning process, and perhaps perform the migration in a test bed. However, RSA recommends that you do not migrate to a production deployment until you have read the *RSA Authentication Manager 7.1 Migration Guide* and developed your migration strategy.

The high-level steps for performing an actual migration are:

1. Synchronize the clocks of the servers where RSA Authentication Manager 6.1 and version 7.1 are installed.
2. Back up the RSA Authentication Manager 7.1 database (in case you need to undo the migration).
3. Migrate data.
4. Examine the migration report for problems.
5. If problems are found, restore the version 7.1 database, resolve the version 6.1 data problems, and repeat the migration.
6. When the database migration is satisfactory, migrate the RSA Authentication Manager 6.1 log files.

---

### Preparing the RSA Authentication Manager 7.1 Server

Before performing a migration, log on to the server where RSA Authentication Manager 7.1 is installed, and perform the following steps:

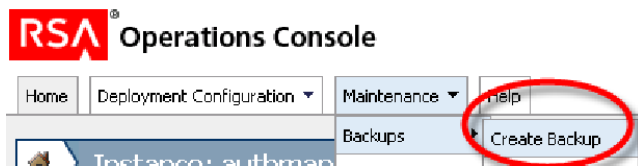
1. Make sure the clock is synchronized with the clock on the server where RSA Authentication Manager 6.1 is installed.  
This step ensures that time-based tokens will still work correctly with version 7.1.
2. Create a directory to store the backup of the RSA Authentication Manager 7.1 database, for example, C:\temp\backup.

---

### Backing Up the RSA Authentication Manager 7.1 Database

The Authentication Manager database contains some predefined entities, such as administrative roles and authentication policies. RSA recommends that you back up the database before migrating RSA Authentication Manager 6.1 data into it, so that you can undo the migration if you find data problems after the migration.

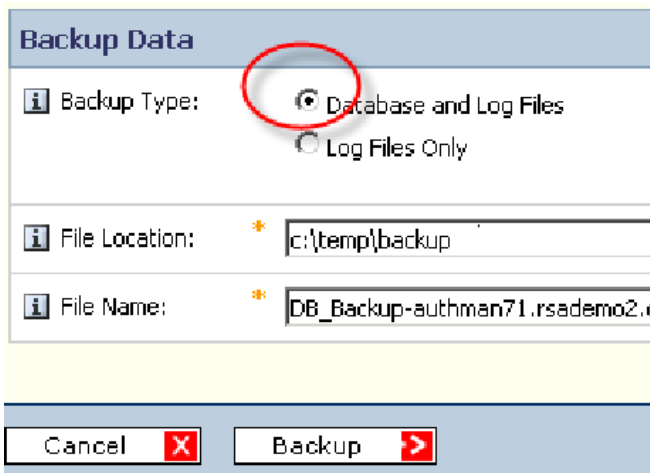
1. Log on to the RSA Operations Console.



2. Click **Maintenance > Backups > Create Backup**.

3. On the Backup Data page, specify the backup options:

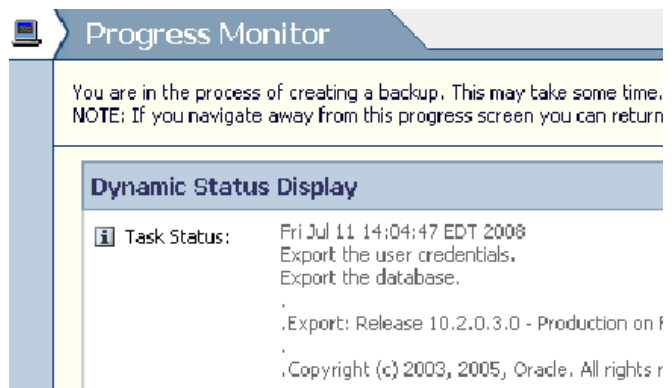
- For Backup Type, select **Database and Log Files**.
- For File Location, specify the directory you created to store the backup file.
- For File Name, supply a name for the backup file.



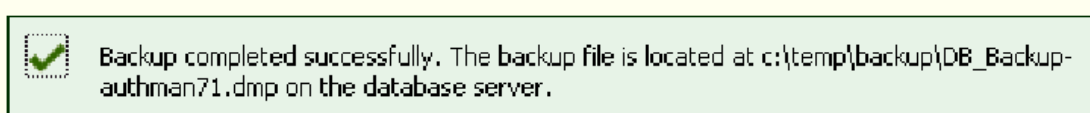
4. Click **Backup**.

The Progress Monitor page is displayed

5. When the backup is complete, click **Done**.



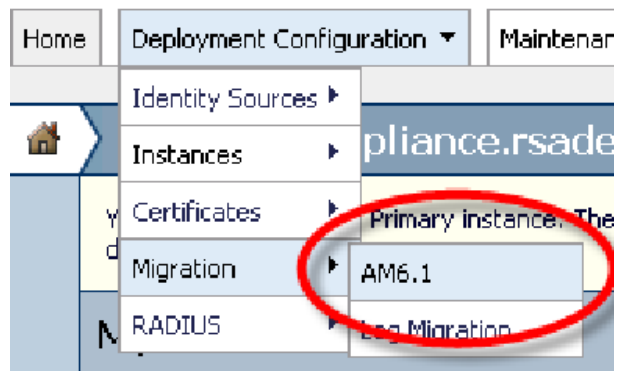
6. On the Backup Completed page, click **Cancel** to exit the backup utility.



## Migrating the RSA Authentication Manager 6.1 Database

The procedure for an actual migration is the same as that described previously for a test migration, except that you do not select the Test Migration option.

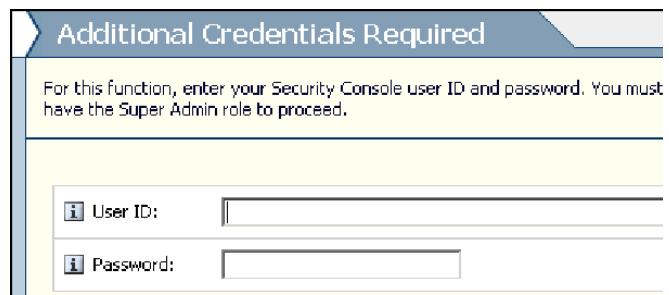
1. Log on to the RSA Authentication Manager 7.1 RSA Operations Console.
2. Click **Deployment Configuration > Migration > AM6.1**.



The Additional Credentials Required page is displayed.

**Note:** You must be a Super Admin to perform this task.

3. Log on again.



The Upload Files page is displayed.

- On the Upload Files page, specify the location of the files you copied from RSA Authentication Manager 6.1, or click **Browse** to search for them.

- Click **Scan Dump File**.

- On the Scan Results page, verify that the data found in the dump file is the data you want to migrate.

- In the **Migration Mode** section, select **Typical Mode**.

**Note:** Select **Custom Mode** if you want to specify any non-default migration options, such as which data to migrate, where to migrate the data, and whether to stop the process if data conflicts occur.

- Click **Next**.



The Server Migration page is displayed, showing the migration options you chose (in this example, the defaults).

- At the bottom of the page, click **Start Server Migration**.

**Migration**

**To be migrated:**

- Agents
- Custom Extensions
- Users
- Tokens
- Groups
- Administrative Roles
- Delta Records
- System Settings

**Not Found in scan:**

- One-Time Passwords
- RADIUS Profiles
- Cross Realm

**Migration Settings**

**Data Conflicts:** Best Effort - Continue migration

**User Migration:**

**User ID Format (Internal Database):** NTLM

**Migration Report**

**Results Directory Location:** C:\Program Files\RSA Security\Authentication Manager\utils\migration\

**Verbose Report:** Include extra detail in the report

Cancel [X] [Back] Start Server Migration

The Server Migration Status page is displayed, showing the progress of each migration task.

**Server Migration Status**

Task ( 8 of 38 )


1. Analyzing Dump File	<div style="width: 0%;"></div>
2. Unsupported character check	<div style="width: 0%;"></div>
3. System settings	<div style="width: 0%;"></div>

When the migration is complete, the Server Migration Results page is displayed.

- In the **Migration Report** section, click the report that you want to view. You can also save the reports to your hard drive.

The migration reports alert you to possible problems with the RSA Authentication Manager 6.1 data.

- Click **Done**.

 Migration was successful.

### Summary

- Migration completed successfully
- User "kflanagan" cannot be activated on an open agent "saalem.arista"
- User "ebcadmin" cannot be activated on an open agent "saalem.arista"
- System settings from AM 6.1 have been applied to this installation. Please review administrative roles
- User "mhuckaby" cannot be activated on an open agent "saalem.arista"
- AM6.1 task lists have been migrated to administrative roles. Please review administrative roles

### Next Steps

- Review migrated admin roles: Administration -> Administrative Roles -
- Review migrated system settings: Setup -> Authentication Methods and Authentication Manager

### Migration Report

i	Results Directory:	C:\Program Files\RSA Security\RSA Authentication Manager\080213050512
i	Report:	<a href="#">migration_summary.html</a>
i	Verbose Report:	<a href="#">migration_detail.zip</a>

- Do one of the following:

- If your migration report is satisfactory, proceed to ["Migrating the Log Files"](#) on page 27.
- If your migration reveals data problems that did not appear in the test migration, you must:
  - a. Return to RSA Authentication Manager 6.1, and resolve the problems. For more information, see the *RSA Authentication Manager 7.1 Migration Guide*.
  - b. Restore the RSA Authentication Manager 7.1 database to its initial state. See Appendix A, ["Restoring the RSA Authentication Manager 7.1 Database."](#)
  - c. Repeat the database migration until the outcome is satisfactory, and then proceed to ["Migrating the Log Files"](#) on page 27.

## Migrating the Log Files

When the database migration report is satisfactory, perform the following steps:

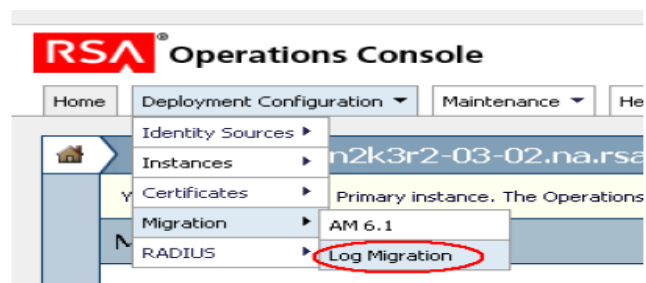
- Verify the migration from the RSA Security Console.
- Migrate the RSA Authentication Manager 6.1 log files.

While the database migration might be performed several times, the log file migration is performed only once. If you migrate log files more than once, you create duplicate log entries.

1. Log on to the RSA Authentication Manager 7.1 RSA Security Console.
2. Review the imported data (for example, users, user groups, agent hosts, and administrative roles) to verify its accuracy.

3. Log on to the RSA Authentication Manager 7.1 RSA Operations Console.

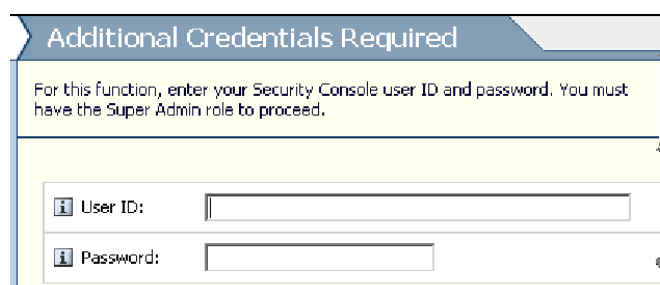
4. Click **Deployment Configuration > Migration > Log Migration**.



The Additional Credentials Required page is displayed.

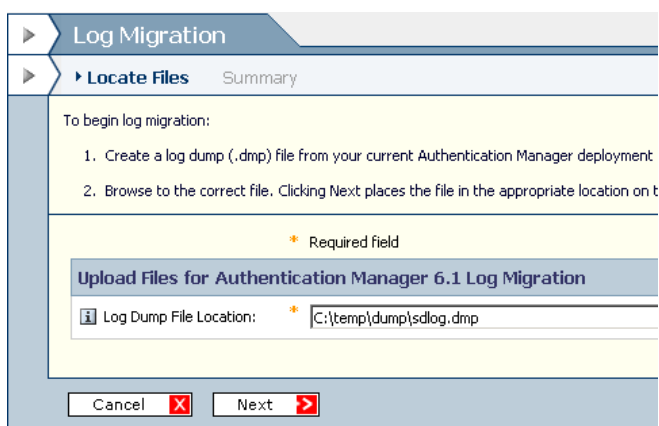
**Note:** You must be a Super Admin to perform this task.

5. Log on again.



- On the Log Migration page, in the **Log Dump File Location** field, enter the path name of the log dump file (**sdlog.dmp**), or click **Browse** to search for it.

- Click **Next**.



The Log Migration Summary page is displayed.

- Click **Start Log Migration**.

The Log Migration Status page is displayed, reporting the progress of the log migration. When the migration completes, the Log Migration Results page is displayed.

- On the Log Migration Results page, click **migrate.log** to view the log migration report.
- Click **Done** to exit the migration utility.

# A

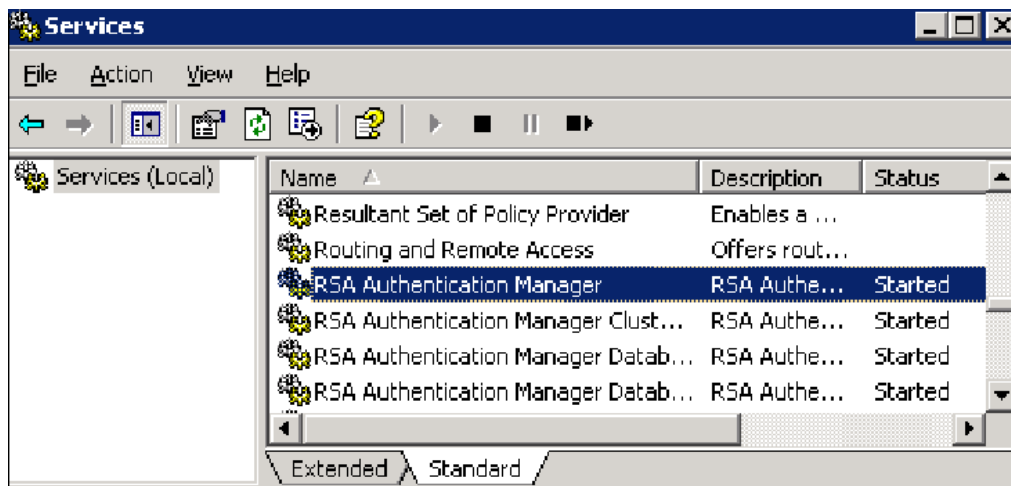
## Restoring the RSA Authentication Manager 7.1 Database

If you discovered and resolved data problems in the RSA Authentication Manager 6.1 data after the migration, you must restore RSA Authentication Manager 7.1 to its initial state, and then repeat the migration.

To restore version 7.1 to its initial state, you restore the database backup created in [“Backing Up the RSA Authentication Manager 7.1 Database”](#) on page 21. Because this procedure overwrites all the data in the database, it removes any changes made by the first migration.

This appendix provides instructions for restoring the RSA Authentication Manager 7.1 database.

1. Log on to the Windows server where RSA Authentication Manager 7.1 is installed.
2. Click **Start > Administrative Tools > Services**.



3. Stop all RSA Authentication Manager Services except the internal database and the database listener. To stop a service, right-click on the service name, and on the pop-up, click **Stop**.

- 
4. On the Windows server, click **Start > Run**.
  5. In the **Open:** field, type **cmd**.
  6. Click **OK** to open the command line utility.

- 
7. Change directories to **\Program Files\RSA Security\RSA Authentication Manager\utils**.

- 
8. To remove the primary metadata, type:

```
rsautil setup-replication -a
remove-primary
```

9. At the “Enter password” prompt, enter the RSA Operations Console password.

10. At the “Are You Sure. . .?” prompt, enter y.

```
C:\Program Files\RSA Security\RSA Authentication Manager\utils>rsautil setup-rep
lication -a remove-primary
Enter password: *****

Setup Replication ins-2.0.0-build20080429174900
Copyright (C) 2008 RSA Security Inc. All rights reserved.

%% running at: authman71:[od8b7d3p] %%

=====
%      Removing a Primary Site      %
=====
Type      Instance name      Hostname      DBname
-----
Primary  authman71.rsademo2.com  authman71.rsademo2.com  od8b7d3p
Are you sure you want to remove this primary? (Y/N): y

%% Starting configuration
-- Status: Removing queues at [od8b7d3p]
Done...

C:\Program Files\RSA Security\RSA Authentication Manager\utils>_
```

- 
11. To import the backup files into the database, type:

```
rsautil manage-backups -a
import -D -f absolute
path\dumpfile
```

For example: rsautil manage-backups -a  
import -D -f C:\temp\backup\  
DB\_Backup-authman71.dmp

12. At the “Enter password” prompt, enter the RSA Operations Console password.
13. At the “Are You Sure . . .?” prompt, enter y.

```
C:\Program Files\RSA Security\RSA Authentication Manager\utils>rsautil manage-backups -a import -f C:\temp\backup\DB_BACKUP-AUTHMAN71.DMP -D
Enter master password.: *****
Are you sure you want to import the file and overwrite the existing data in the
database? (Y/N): y
Operation started : FRI JUL 11 14:47:51 EDT 2008
Import the user credentials.
Import the database.

flashback is turned on.
Reset the IMS console meta data
Rename URL-based config values
All of data except the log data has been imported, and it is OK to start the system.
Operation completed : FRI JUL 11 14:58:01 EDT 2008
C:\Program Files\RSA Security\RSA Authentication Manager\utils>
```

14. To reset the primary metadata, type:

```
rsautil setup-replication -a
set-primary
```

15. At the “Enter password” prompt, enter the RSA Operations Console password.

16. At the “Is this correct. . .” prompt, confirm that the database name and hostname are correct, and enter y.

```
C:\Program Files\RSA Security\RSA Authentication Manager\utils>rsautil setup-rep
lication -a set-primary
Enter password: *****

Setup Replication ims-2.0.0-build20080429174900
Copyright (C) 2008 RSA Security Inc. All rights reserved.

%% running at: authman71:[od8b7d3p] %%

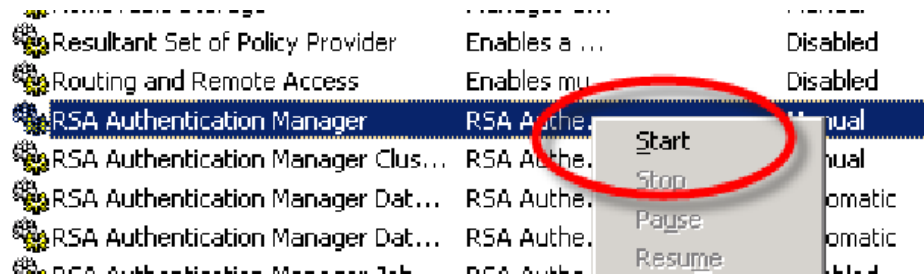
=====
%      Setting up Primary Site      %
=====
[Primary]
Port      : 2334
DB name   : od8b7d3p
DB host   : authman71.rsademo2.com
Instance : authman71.rsademo2.com
Site name : authman71.rsademo2.com

Is this correct (Y/N): y

%% Starting configuration
-- Status: Changing capture retention time [od8b7d3p]
-- Registering primary information
Done...
```

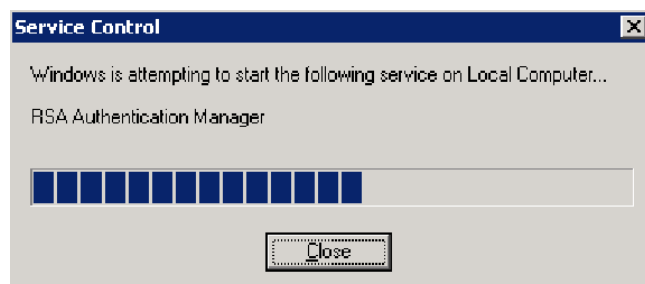


17. To restart the Authentication Manager services, click **Start > Administrative Tools > Services**.
18. Right-click on RSA Authentication Manager, and on the pop-up, click **Start**.

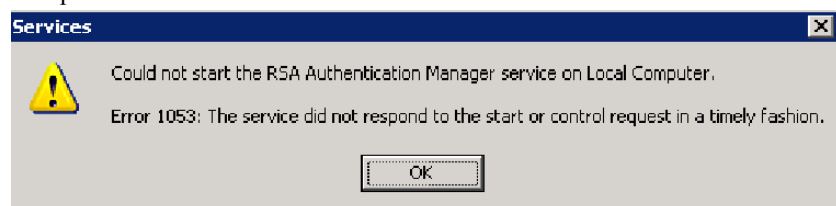


**Note:** When you start the RSA Authentication Manager service, it starts all the related services.

As RSA Authentication Manager starts up, a progress window is displayed. Startup might take several minutes.



The following error may appear. The message indicates that the Windows GUI timed out waiting for the startup process to complete.



19. Click **OK**.

Upon completion, the RSA Authentication Manager status and its related services' status are **Started**.

 RSA Authentication Manager Node Manager	RSA RSA A	Started	Automatic	Local Sy
 RSA Authentication Manager Operations Console	RSA Aut e...	Started	Automatic	Local Sy
 RSA Authentication Manager Proxy Server	RSA Auth...	Started	Automatic	Local Sy