RSA® Authentication Manager 6.1 to 8.0 Migration Preparation Guide

The goal of migrating from RSA® Authentication Manager version 6.1 to RSA® Authentication Manager version 8.0 is to recreate a functioning 6.1 environment within the new 8.0 framework. While many concepts are similar between versions 6.1 and 8.0, there are some significant differences in the data models. Whenever possible, the migration process automatically converts 6.1 data to fit into the 8.0 data model without affecting end user authentication or administrative control. However, this is not possible for all data. To ensure a successful migration, this document details a series of pre-migration steps to prepare the version 6.1 deployment for a successful migration to Authentication Manager 8.0.

Authentication Manager version 6.1 is the minimum version required to migrate to version 8.0.

This document only addresses migration from Authentication Manager version 6.1 to version 8.0. Migration from Authentication Manager version 7.1 to version 8.0 does not require the use of the migration assessment utility described in this guide, as the difference in data models between versions 7.1 and 8.0 is not significant. For more information on planning a migrating from version 7.1 to version 8.0, including minimum migration requirements, see the *RSA Authentication Manager 7.1 to 8.0 Migration Guide*.

Overview of the Migration Process

The process of migrating from version 6.1 to version 8.0 contains four main steps:

1. Deploy and configure an Authentication Manager 8.0 virtual appliance.
2. Use the Authentication Manager 6.1 export utility to export all relevant version 6.1 deployment data, including users, tokens, and agents, into a migration package.
3. Import the migration package into the version 8.0 deployment, which recreates the data from the version 6.1 deployment in the new deployment.
4. Choose one of the following:
    - Replace the existing 6.1 instances with the 8.0 instances by using the same IP address and hostname.
    - Replace the configuration of each agent to point to the new version 8.0 deployment.

RSA recommends thoroughly testing the version 8.0 deployment before migrating the production system. Before moving the version 8.0 system into production, verify that the data is properly migrated and become familiar with the operation of Authentication Manger 8.0.

Important Changes to Authentication Manager 8.0

There are several factors to consider before migrating. The following differences between Authentication Manager 6.1 and 8.0 may require your attention prior to migrating:

- The following characters that are supported in version 6.1 are not supported in version 8.0:

  `& < > % ‘`

- Unique identity attributes apply to all users in version 8.0, while version 6.1 supported individual user extension data.
- Some older agents are not supported in version 8.0. For information on supported agents in version 8.0, see “Authentication Agent Support” in the Planning for Migration chapter of the *RSA Authentication Manager 6.1 to 8.0 Migration Guide.*
- Version 8.0 integrates directly with LDAP directory servers, while version 6.1 supports periodic synchronization jobs. If you do not currently synchronize with an external LDAP directory server, consider whether you want to continue storing users in the internal database or integrate with an external LDAP directory server before you migrate.
- All version 6.1 custom applications or TCL scripts are incompatible with version 8.0. Call your sales representative if you need assistance regarding custom applications or scripts.
- Some version 6.1 data, such as reports, cannot be migrated to version 8.0 and must be recreated or reconfigured.
- Version 6.1 allowed administrators to manually enable the Set PIN to Next Tokencode feature on a specific token. This feature is not supported in version 8.0.
- Version 8.0 does not support the activation of individual users on authentication agents. Because of this change, the migration process creates user groups that contain the individual users that should have access to a given agent.
- Version 8.0 does not allow you to scope administrative roles to groups. Any version 6.1 administrative task list that is scoped to a group is not migrated to the version 8.0 deployment.
- The user interface is different between the two versions. Administrators must learn the new version 8.0 administrative interface. Some training may be necessary.

See the *RSA Authentication Manager 6.1 to 8.0 Migration Guide* for additional details on the differences between version 6.1 and version 8.0. This guide is included with the Authentication Manager 8.0 documentation set.

Recommended Pre-Migration Steps

Before you migrate to version 8.0, RSA strongly recommends that you run the RSA Authentication Manager 6.1 to 8.0 Migration Assessment Utility. This utility analyzes your database to determine if any issues must be addressed prior to migration, such as data incompatibilities or potential areas for cleanup, such as expired tokens. Addressing obsolete or incompatible data before migrating helps to ensure a successful migration to version 8.0.

The RSA Authentication Manager 6.1 to 8.0 Migration Assessment Utility

The RSA Authentication Manager 6.1 to 8.0 Migration Assessment Utility produces a summary report of the number of objects found in the database. It does not alter your data in any way. The report output is color-coded white, green, yellow, or red. These colors indicate whether action is needed before you proceed with the migration to version 8.0.

- **Red** indicates that a condition regarding the existing 6.1 data requires action before migration. Failure to correct the problem prior to migration may cause a migration failure or undesired results such as data loss. Specific guidance on how to address the condition is provided in the cell to the right.
- **Yellow** indicates a condition that you may want to address prior to migration. Objects with a yellow status will not prevent migration from succeeding, however, resolving the problem may expedite the migration and result in a "cleaner" post-migration 8.0 deployment. Specific guidance on how to address the condition is provided in the cell to the right.
- **Green** indicates that there is no problem with the object type.
- **White** indicates that the cell is informational only.

The following example displays some of the color-coded information from the migration summary report.

Token Related Information			
Token	451		This item is for information only.
Hardware Token	50		This item is for information only.
Software Token	400		This item is for information only.
Expired Token	0	Green(0<=count<=100), Yellow(count>100)	
Disabled Token	97 disabled_tokens_0217130124.csv	Green(0<=count<=100), Yellow(count>100)	
Agent Host Related Information			
Agent	2		This item is for information only.
Potential Legacy Agent	1 potential_legacy_agents_0217130124.csv	Green(count=0), Red(count>0)	Some older agents are not supported in AM 8.0. Be sure to investigate further and test these agents with AM 8.0 prior to migrating.
Unrestricted Agent Hosts with Groups Enabled	1 groups_on_unrestricted_agent_0217130124.csv	Green(count=0), Yellow(count>0)	You have agents that are currently open to local users and also have groups enabled. After the migration, these agents will be converted to restricted agents. Users that are not part of the enabled groups will not be able to authenticate and log on to these agents.

In addition to the summary, the utility creates a set of CSV files that list the specific records that may need attention prior to migration. The summary report directs you to the appropriate files to find the records in question.

Note: RSA recommends creating a test Authentication Manager 6.1 deployment complete with production data to test the cleanup operations to prevent any unforeseen problems on the production deployment.

Perform an Authentication Manager 6.1 to 8.0 Migration Assessment

Perform an Authentication Manager 6.1 Migration Assessment to determine the readiness of the version 6.1 data for migration into Authentication Manager 8.0.

Procedure

1. Go to **https://knowledge.rsasecurity.com/scolcms/set.aspx?id=9620** to download the RSA Authentication Manager 6.1 to 8.0 Migration Assessment Utility from SecurCare Online.
2. Extract the contents of the RSA Authentication Manager 6.1 to 8.0 Migration Assessment Utility zip file.
3. Log on to the version 6.1 primary system as an administrator.
4. Create a new local directory and copy the file **6.1_migration_assessment.tcl** to this directory.
5. If you are using a Unix/Linux system, verify that the **USR_ACE**, **VAR_ACE**, **DLC**, **PROPATH**, and **LD_LIBRARY_PATH** environment variables are configured correctly. Use the **admenv** utility to display the correct environment variable settings for your system. In the **/ace/utils** directory, run **admenv**, and set the environment variables according to the displayed information.
6. Open a command line shell and change the directory to the local directory that you created in step 4.
7. In the command line shell, run one of the following commands:
   - On Windows:

     ```
     "auth_mgr_install_dir\utils\tcl\bin\tcl-sd.exe"
     6.1_migration_assessment.tcl
     ```

   - On Unix/Linux:

     ```
     "auth_mgr_install_dir/utils/tcl/bin/tcl-sd"
     6.1_migration_assessment.tcl
     ```

   The utility generates a summary report with the filename **6.1_migration_assessment_*datetime*.html** , where *datetime* is the date and time when you ran the report. The utility also generates a set of time-stamped CSV files that provide information on specific records identified in the HTML report.

   The utility also generates a log file, **6.1_migration_assessment_*datetime*.log**, that records errors and results from running the utility.

Important: RSA strongly recommends securing the generated CSV files and deleting them after resolving any issues. These files may contain sensitive data.

8. Open the generated file **6.1_migration_assessment_*datetime*.html** to view the results.

After you address any problematic data in the deployment, you can perform an additional assessment of the 6.1 deployment to confirm that the problem has been resolved. If you have any questions or concerns about the migration of the version 6.1 deployment, contact RSA Customer Support.

If your migration assessment indicates multiple areas that require action, RSA recommends that you consider enlisting RSA Professional Services for assistance. If you are interested in engaging RSA Professional Services, contact your RSA representative.

Authentication Manager 8.0 Test Environments

Before you perform a production migration, you can obtain a free evaluation license from RSA and configure a test Authentication Manager 8.0 virtual appliance in minutes.

After you deploy a test environment and migrate the data from version 6.1, you can:

- Verify that the data is in place and organized and configured as you expect.
- Familiarize your administrators with the new administrative interface.
- Verify that the product functionality meets your needs.
- If you store users in the internal version 6.1 database and would like to integrate with an external LDAP directory server in 8.0, you can test the user mapping during migration testing.
- Implement custom applications using the 8.0 SDK.

Support and Service

RSA SecurCare Online	**https://knowledge.rsasecurity.com**
Customer Support Information	**www.emc.com/support/rsa/index.htm**
RSA Solution Gallery	**https://gallery.emc.com/community/marketplace/rsa?view=overview**

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

RSA Professional Services can provide additional assistance with Authentication Manager 8.0 migration preparation, planning, and implementation. Contact your RSA representative if you are interested in engaging RSA Professional Services.

March 2013

Trademarks