RSA® Access Manager 6.2 Servers Upgrade Guide

Contact Information

Go to the RSA corporate website for regional Customer Support telephone and fax numbers:
www.emc.com/domains/rsa/index.htm

Trademarks

RSA, the RSA Logo and EMC are either registered trademarks or trademarks of EMC Corporation in the United States and/or other countries. All other trademarks used herein are the property of their respective owners. For a list of EMC trademarks, go to **www.emc.com/legal/emc-corporation-trademarks.htm#rsa**.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, 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 EMC.

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

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

March 2013

Contents

Preface

About This Guide

The Upgrade guide describes how to upgrade your:

- RSA Access Manager 6.1 and later Servers to RSA Access Manager 6.2.
- RSA Access Manager 6.1 and later database schema to RSA Access Manager 6.2 schema.
- RSA Access Manager 6.1 and later Web Applications to RSA Access Manager 6.2 Web Applications.

It is intended for security administrators and other trusted personnel. Do not make this guide available to the general user population.

Note: For information on upgrading RSA Access Manager Agents, see your RSA Access Manager Agent documentation.

RSA Access Manager Documentation

For more information about RSA Access Manager, see the following documentation:

Release Notes. Provides information about what is new and changed in this release, as well as workarounds for known issues. The latest version of the Release Notes is available from RSA SecurCare Online at **https://knowledge.rsasecurity.com**.

Getting Started. Lists what the kit includes (Licenses and documentation), specifies the location of documentation on the kit, and lists RSA Customer Support web sites.

Planning Guide. Provides a general understanding of RSA Access Manager, its high-level architecture, its features, and deployment information.

Servers Installation and Configuration Guide. Provides instructions for installing and configuring the RSA Access Manager Servers and additional components. This guide also contains descriptions for different configuration options, features, and production environment considerations.

Administrator's Guide. Provides information for security administrators about using the RSA Administrative Console to administer users, resources, and security policy in RSA Access Manager.

Developer's Guide. Provides information about developing custom programs using application programming interfaces (APIs) included with the RSA Access Manager Servers.

API Delta Document. Provides information about the differences between previous and current versions of the APIs included with the RSA Access Manager Servers.

Upgrade Guide. Provides information about how to upgrade from previous versions of the RSA Access Manager Servers, data store schema, and data to the current version.

Security Configuration Guide. Provides an overview of the settings available in the RSA Access Manager Server and compatible Agents to ensure secure operation of the product.

RSA Access Manager Administrative Console Help. Provides instructions on how to perform specific administrative tasks. To view Help, click the **Help** tab on the RSA Administrative Console.

RSA Access Manager User Self- Service Console Help. Describes day-to-day user tasks performed in the User Self-Service Console. To view Help, click the **Help** tab on the RSA User Self-Service Console.

Related Documentation

For more information about products related to RSA Access Manager, see the following:

RSA Access Manager Agents documentation set. The documentation related to agents is available from RSA SecurCare Online at **https://knowledge.rsasecurity.com**.

RSA Adaptive Authentication documentation set. The documentation related to RSA Adaptive Authentication is available from RSA SecurCare Online at **https://knowledge.rsasecurity.com**.

RSA Envision documentation set. The documentation related to RSA Envision is available from RSA SecurCare Online at **https://knowledge.rsasecurity.com**.

Getting Support and Service

RSA SecurCare Online	**https://knowledge.rsasecurity.com**
Customer Support Information	**www.rsa.com/support**
RSA Secured Partner Solutions Directory	**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 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 Access Manager software.

Please have the following information available when you call:

- Your RSA Customer/License ID.

  This is a paper license. You can find this number only on the license distribution medium. If you do not have access to the paper-based RSA Customer/License ID, contact RSA Customer Support.

- RSA Access Manager software version number and patch level.
- The make and model of the machine on which the problem occurs.
- The name, version, and patch level of the operating system under which the problem occurs.

1 Preparing to Upgrade

Upgrade Scenarios for Access Manager Server 6.2

This section describes the upgrade scenarios covering Access Manager Server, Agents, and Adaptive Authentication server that impact the upgrade flow for Access Manager Server version 6.2.

Before you begin the upgrade, you must understand the compatibility of the Agents and Adaptive Authentication server versions with the Access Manager Server 6.2. For more information see, Supported Agent and Adaptive Authentication Server Versions on page 9.

Supported Agent and Adaptive Authentication Server Versions

The following table lists the supported Agent and Adaptive Authentication Server versions that are compatible with respective Access Manager Server 6.1 and later versions:

Supported Version Matrix

Server	Adaptive Authentication Server	Application Agent	Web Agent	Inference
6.2	7.0	NA	5.0	This is the ideal deployment scenario of Access Manager Server 6.2.
6.2	None	4.7, 4.7 SP1, and 5.0	4.7, 4.8, 4.9 SP1, 4.9 SP2, 4.9 SP3	When AA is not used, this is the list of Agent versions that is supported on Access Manager Server 6.2
6.2	6.0 SP3 P2 , and 6.0 SP3 P3	NA	5.0	When AA is used, this is the list of Agent versions that is supported on Access Manager Server 6.2

Upgrade scenarios

The upgrade scenarios are based on how Access Manager is deployed. Following are examples of typical upgrade scenarios:

- **Upgrade to 6.2 Server when Agents and Adapative Authentication Server are on supported versions:**

  If the Agents and Adaptive Authentication Server versions in your deployment support Access Manager 6.2, then you can upgrade to 6.2 from prior version successfully.

- **Upgrade 6.2 Server with Agents or Adapative Authentication Server that are not supported:**

  If the Agents and Adaptive Authentication Server versions in your deployment do not support server 6.2 as mentioned in the above table, then you must upgrade the Agents and Adaptive Authentication Server to the least supported version of server 6.2 upgrade before upgrading the server to 6.2.

Use Cases

- If you have Server version as 6.1 SP4, Agents on version 4.9 SP3 and Adaptive Authentication server is not used, then you can upgrade to the server 6.2.
- If you want to deploy Adaptive Authentication server 7.0 in your deployment, then along with Server, you must also upgrade Agents to version 5.0.

Note: You must be aware that the latest Access Manager Server 6.2 version new functionality is available only after all the relevant Agent and other server components are updated.

Before You Begin

RSA Access Manager 6.2 supports upgrades from RSA Access Manager 6.1 and later.

Make sure that you upgrade to one of the supported operating systems for RSA Access Manager 6.2. To find out which operating systems are supported, see "Platform and Operating System Requirements" in the chapter "Requirements" in the *Servers Installation and Configuration Guide*.

To find out, which data store types are supported for upgrades from RSA Access Manager 6.1 to RSA Access Manager 6.2, see "Supported Data Store Servers" in the chapter "Requirements" in the *Servers Installation and Configuration Guide*.

Note: Throughout this document, the directory where you install Access Manager servers is called ***AXM_HOME*** and the base directory of the RSA Access Manager Server 6.2 is called ***Installer Directory.***

Upgrading Your Agents

You may need to upgrade your Agents for use with RSA Access Manager 6.2. To find out which Agent versions are compatible, see "Supported RSA Access Manager Agents" section in the chapter "RSA Access Manager 6.2 Server Installation and Configuration Overview" of the *Servers Installation and Configuration Guide*. For Agent upgrade instructions, see your RSA Access Manager Agent documentation.

Overview of Upgrade Steps

Perform the following steps to complete the upgrade process:

1. Upgrade your servers:
   - For instructions on Windows upgrade, see Upgrading Servers on Windows on page 13.
   - For instructions on UNIX upgrade, see Upgrading Servers on UNIX on page 17.
2. Upgrade your database schema:
   - For upgrading database schema on Oracle, see Chapter 4, Upgrading Database Schema on Oracle.
   - For upgrading database schema on Sybase, see Chapter 5, Upgrade Database Schema on Sybase.
   - For upgrading database schema on Microsoft SQL, see Chapter 6, Upgrading Database Schema on Microsoft SQL Server.
   - For upgrading database schema using Sun Java System Directory Server, see Chapter 7, Upgrading Database Schema on Sun Java System Directory Server.
   - For upgrading database schema using OpenDj Server, see Chapter 8, Upgrading Database Schema on OpenDJ Server.
   - For upgrading database schema using Active Directory, see Chapter 9, Upgrading Database Schema on Active Directory.
   - For upgrading database schema using Active Directory-Active Directory Lightweight Services, see Chapter 10, Upgrading Database Schema on Active Directory-Active Directory Lightweight Directory Services.
   - For upgrading using Novell eDirectory, see Chapter 11, Upgrading Database Schema on Novell eDirectory.
3. Upgrade your Web Applications:
   - For upgrading your Administrative Console, see Chapter 13, Upgrading the Administrative Console.
   - For upgrading your APIs, see Chapter 14, Upgrading the APIs.
   - For upgrading Self-Service console see, Chapter 15, Upgrading the User Self-Service Console.
   - For upgrading SNMPv3 or Instrumentation Server , see Chapter 16, Upgrading the SNMPv3.
4. Restart Access Manager Servers.

2 Upgrading Servers on Windows

This chapter describes how to upgrade your RSA Access Manager 6.1 and later servers to RSA Access Manager 6.2

Upgrading Your Servers

Before You Begin

To upgrade, initially you must perform the following tasks:

1. Stop all the RSA Access Manager Servers that are running.
2. During Upgrade shut down or redirect any RSA Access Manager Agents that rely on the Authorization Servers.

Upgrading to Access Manager Server 6.2 on Windows

To upgrade the Access Manager Server 6.2 on Windows:

1. Log on to your Windows machine as the Local Administrator, or as a user with sufficient file permissions to replace files in the RSA Access Manager installation directory.

   Note: RSA recommends that only the Local Administrator upgrade the RSA Access Manager Servers on Microsoft Windows. If the Domain Administrator installs the RSA Access Manager Servers, the Domain Administrator must have Full Control permission to the RSA Access Manager installation directory. If you encounter problems replacing your **KeyClient.sec** or **KeyServer.sec** files, make sure that your user has sufficient file permissions to perform the upgrade.

2. On the RSA Access Manager 6.2 Installer Directory, navigate to the directory where the installation package is placed.
3. Double-click **setup.exe**. The **Welcome** screen opens.

   Note: To run the installation script in Console mode, type `# ./setup.bin -i console` command.

4. Ensure that all the prerequisites tasks are met and note down the required information for upgrading the Access Manager Server. Click **Next**.

5. On the **License Agreement** screen, select I **accept the terms of this license agreement**, and click **Next.**
6. On the **Installation Type** screen, select **Upgrade** option.
7. On the **Location** screen, enter or browse to the appropriate existing Access Manager Server Installation location to upgrade the existing version of Access Manager server.
8. On the **Location** screen, enter or browse to the new Access Manager Server Installation location.
9. On the **Locations** screen, enter or browse to the **JDK Location** installed in the system and then click **Next**.

   Note: Make sure that JDK version 1.6 or higher is installed on the same system, where you are installing Access Manager Server.

   Note: Ensure that you use 64-bit JDK on 64-bit Operating System, and 32-bit JDK on 32-bit Operating system.

10. Review the Upgrade **Summary**, and click **Upgrade**, or click **Previous** to make any changes.
11. The Access Manager Upgrade software upgrades the existing files with new version files. When it finishes upgrading the files, do one of the following:
    - If the message “Upgrade procedure ... was successful” appears, click **OK**. Navigate to the **\Installationlogs** directory in your RSA Access Manager 6.2 installation directory, and open the **upgrade.log** file for a summary of the parameters that have changed.
    - If the message “Errors occurred during the upgrade procedure” appears, click **No** to stop the installer, and follow the below steps to address the problem:
      – Navigate to the **\Installationlogs** directory in your RSA Access Manager 6.2 installation directory.
      – View the **upgrade.log** file to find the nature of the problem.
      – Fix the problem by editing your pre-upgrade configuration files.
      – Rerun the upgrade.

Next Steps

For instructions on upgrading your data store, see the following chapters:

- On Oracle, see Chapter 4, Upgrading Database Schema on Oracle.
- On Sybase, see Chapter 5, Upgrade Database Schema on Sybase.
- On Microsoft SQL, see Chapter 6, Upgrading Database Schema on Microsoft SQL Server.

- On Sun Java System Directory Server, see Chapter 7, Upgrading Database Schema on Sun Java System Directory Server.
- On OpenDj Server, see Chapter 8, Upgrading Database Schema on OpenDJ Server.
- On Active Directory, see Chapter 9, Upgrading Database Schema on Active Directory.
- On Active Directory-Active Directory Lightweight Services, see Chapter 10, Upgrading Database Schema on Active Directory-Active Directory Lightweight Directory Services.
- On Novell eDirectory, see Chapter 11, Upgrading Database Schema on Novell eDirectory.

3 Upgrading Servers on UNIX

'This chapter describes how to upgrade your RSA Access Manager 6.1 and later Servers to RSA Access Manager 6.2 on Linux, Solaris and AIX.

Upgrading Your Servers

Perform the upgrade of Access Manager Server from a shell, such as the cmdtool, xterm, or the CDE terminal.

Note: Only the properties in the configuration files that are non-commented by default, are imported from the old installation during upgrade.

Before You Begin

Before you upgrade the Access Manager Server, you must perform the following tasks:

1. Stop all the RSA Access Manager Servers that are running.
2. Shut down or redirect any RSA Access Manager Agents that rely on the Authorization Servers, you are upgrading.

Upgrading to Access Manager Server 6.2 on UNIX

In the following procedure, use the RSA Access Manager installation script upgrade routine. Press ENTER to accept default values in square braces (for example, axm]).

Important: If you have entered any incorrect information during installation you can type **BACK** to go back to the previous prompt.

To upgrade the Access Manager Server 6.2 on UNIX:

1. Log on as a root user.
2. Stop all the RSA Access Manager Servers that are running. Shut down or redirect any RSA Access Manager Agents that rely on the Authorization Servers that you are upgrading.
3. On the RSA Access Manager 6.2 Installer Directory, navigate to the following:
   - For Solaris: **/solaris-sparc/axm_servers**
   - For AIX: **/aix-rs6000/axm_servers**
   - For Linux: **/linux-x86/axm_servers**
4. Run the installation script:

   ```
   # ./setup.bin
   ```

   Note: To run the installation script in Console mode, type `# ./setup.bin -i console` command. RSA recommends to use CLI mode on UNIX platforms.

5. Ensure that prerequsites for the upgrade are met before proceeding with installation. Press **Enter**.
6. Type **Y** to accept the License Agreement.
7. Select the number for installation type, it is 2 for upgrade.
8. Enter the existing RSA Access Manager Server Installation location you are upgrading. For example, if you are upgrading a version 6.1 installation, this path typically is **/opt/axm/server-61** for Solaris and Linux, and **/usr/axm/server-61** for AIX.
9. Enter the upgrade location for RSA Access Manager Server 6.2 installation.

   Note: By default, the Access Manager Server 6.2 files are installed in **/opt/axm/server-62** location.

10. Enter the **JDK Location** installed in the system and press **Enter**.

    Note: Make sure that JDK version 1.6 or higher is installed on the same system, where you are installing Access Manager Server.

    Note: Ensure that you use 64-bit JDK on 64-bit Operating System, and 32-bit JDK on 32-bit Operating system.

11. Review the Upgrade **Summary**, and press **Enter** for upgrade, or type **BACK** to make any changes.
12. The Access Manager Upgrade software upgrades the existing files with new version files. When it finishes upgrading the files, do one of the following:

- If the message “Upgrade procedure ... was successful” appears, press **Enter**. Navigate to the **\Installationlogs** directory in your RSA Access Manager 6.2 root directory, and open the **upgrade.log** file for a summary of the parameters that have changed.
- If the message “Errors occurred during the upgrade procedure” appears, click **No** to stop the installer, and follow the below steps to address the problem:
  - Navigate to the **\Installationlogs** directory in your RSA Access Manager 6.2 root directory.
  - View the **upgrade.log** file to find the nature of the problem.
  - Fix the problem by editing your pre-upgrade configuration files.
  - Rerun the upgrade.

Next Steps

See the instructions for your data store below:

- On Oracle, see Chapter 4, Upgrading Database Schema on Oracle.
- On Sybase, see Chapter 5, Upgrade Database Schema on Sybase.
- On Microsoft SQL, see Chapter 6, Upgrading Database Schema on Microsoft SQL Server.
- On Sun Java System Directory Server, see Chapter 7, Upgrading Database Schema on Sun Java System Directory Server.
- On OpenDj Server, see Chapter 8, Upgrading Database Schema on OpenDJ Server.
- On Active Directory, see Chapter 9, Upgrading Database Schema on Active Directory.
- On Active Directory-Active Directory Lightweight Services, see Chapter 10, Upgrading Database Schema on Active Directory-Active Directory Lightweight Directory Services.
- On Novell eDirectory, see Chapter 11, Upgrading Database Schema on Novell eDirectory.

4 Upgrading Database Schema on Oracle

This chapter describes how to upgrade the database schema from RSA Access Manager 6.1 and later to RSA Access Manager 6.2 on Oracle. This upgrade consists of schema additions only. It does not change your data.

Important: This upgrade supports Oracle 11g R2 and Oracle 11g RAC databases. If your installation is running on an earlier version of Oracle database, upgrade the database to Oracle 11g R2 or Oracle 11g RAC before you begin your RSA Access Manager schema upgrade.

Before You Begin

The administrator performing this upgrade must have:

- Full read/write privileges to the RSA Access Manager database
- Experience in administering SQL databases
- At least entry-level knowledge of the operating system (UNIX or Windows)

You must:

- Make sure that the Oracle SQL*Plus utility is available. For example:
  - From Windows: **%ORACLE_HOME%***server-dir***bin\sqlplus.exe**
  - From UNIX: **$ORACLE_HOME**/*server-dir*/**bin/sqlplus**

  where *server-dir* is the directory, where the Oracle server software resides.
- Stop all the RSA Access Manager Servers that are running.
- Using your company's standard procedure, back up your database before you begin the upgrade. For example, many installations use the Oracle EXPORT utility, which allows you to use the IMPORT utility if you need to restore the database from the backup.
- Set up the command shell window to have a sufficient history buffer (for example, 1000 lines) so that the session is preserved in case you need to call RSA Customer Support.

Upgrading the Schema

To upgrade your schema from RSA Access Manager 6.1 and later to RSA Access Manager 6.2:

1. Copy the upgrade script from the RSA Access Manager 6.2 Installer Directory onto your machine:
   - On Windows:
     ***Installer Directory*\win32-x86\upgrade\oracle_61_to_62\update.sql**
   - On Solaris:
     ***Installer Directory*/solaris-sparc/upgrade/oracle_61_to_62/update.sql**
   - On AIX:
     ***Installer Directory*/aix-rs6000/upgrade/oracle_61_to_62/update.sql**
   - On Linux:
     ***Installer Directory*/linux-x86/upgrade/oracle_61_to_62/update.sql**
2. Log on to Oracle SQL*Plus using the *CT_OWNER* account. Type:

   ```
   sqlplus>CT_OWNER@database name
   ```

   where *database_name* is the name of your RSA Access Manager database.
3. When prompted, enter the password of the *CT_OWNER* Oracle user.
4. Type:

   ```
   SQL>@update.sql
   ```
5. Check the log for error messages.
   If the script does not run completely due to some problem, identify the problem, address the issue, and rerun the script.

To upgrade your schema from RSA Access Manager 6.1 SP4 to RSA Access Manager 6.2:

1. Copy the upgrade script from the RSA Access Manager 6.2 Installer Directory onto your machine:
   - On Windows:
     ***Installer Directory*\win32-x86\upgrade\oracle_61_4_to_62\update.sql**
   - On Solaris:
     ***Installer Directory*/solaris-sparc/upgrade/oracle_61_4_to_62/update.sql**
   - On AIX:
     ***Installer Directory*/aix-rs6000/upgrade/oracle_61_4_to_62/update.sql**
   - On Linux:
     ***Installer Directory*/linux-x86/upgrade/oracle_61_4_to_62/update.sql**
2. Log on to Oracle SQL*Plus using the *CT_OWNER* account. Type:

```
sqlplus>CT_OWNER@database_name
```

where *database_name* is the name of your RSA Access Manager database.

3. When prompted, enter the password of the *CT_OWNER* Oracle user.
4. Type:

```
SQL>@update.sql
```

5. Check the log for error messages.

If the script does not run completely due to some problem, identify the problem, address the issue, and rerun the script.

Next Steps

Your schema upgrade is complete. For instructions on upgrading your Administrative Console, see Chapter 13, Upgrading the Administrative Console.

5 Upgrade Database Schema on Sybase

This chapter describes how to upgrade your schema from RSA Acess Manager 6.1 and later to RSA Access Manager 6.2 on Sybase 15.5. This upgrade consists of schema additions only. It does not change your data.

Before You Begin

The administrator performing this upgrade must have:

- Experience administering SQL databases
- At least entry-level knowledge of the operating system (UNIX or Windows)

You must:

1. Make sure your Sybase server version is 15.5.
2. Set your Sybase server to single-user mode.
3. Make sure the Sybase iSQL utility is available.
4. Stop all running RSA Access Manager Servers.
5. Using your company's standard database backup procedure, back up your database before you begin the upgrade.
6. Set up the command shell window to have a sufficient history buffer (for example, 1000 lines) so that the session is preserved in case you need to call RSA Customer Support.

Upgrading the Schema

To upgrade your schema from RSA Access Manager 6.1 and later to RSA Access Manager 6.2:

1. Copy the upgrade script from the RSA Access Manager 6.2 distribution onto your machine.
   - On Windows:
     ***Installer Directory*\win32-x86\upgrade\sybase_61_to_62\update.SQL**

     Note: For upgrade from Server 6.1 SP4 to 6.2, the upgrade scrpit is available in this location:**\win32-x86\upgrade\sybase_61_4_to_62\update.SQL**
   - On Solaris:
     ***Installer Directory*/solaris-sparc/upgrade/sybase_61_to_62/update.SQL**

- On AIX:
  ***Installer Directory*/aix-rs6000/upgrade/sybase_61_to_62/update.SQL**
- On Linux:
  ***Installer Directory*/linux-x86/upgrade/sybase_61_to_62/update.SQL**

2. The default name of the RSA Access Manager database is CT. If your database has a different name, edit the upgrade script, and enter the correct name.
3. Using iSQL, type:
   $isql -U sa -S sybase_server_name -D database_name -i update.SQL
4. Check the output of the script for any error messages.
   If problems have prevented the script from running completely, address the issues, and rerun the script.

Next Steps

Your schema upgrade is complete. See Chapter 13, Upgrading the Administrative Console.

6 Upgrading Database Schema on Microsoft SQL Server

This chapter describes how to upgrade your schema from RSA Access Manager 6.1 and later to RSA Access Manager 6.2 on Microsoft SQL Server 2008 R2. This upgrade consists of schema additions only. It does not change your data.

Before You Begin

The administrator performing this upgrade must have:

- Full read/write privileges to the RSA Access Manager database
- Experience in administering SQL databases
- At least entry-level knowledge of Microsoft Windows

You must:

- Stop all the RSA Access Manager Servers that are running.
- Using your company's standard procedure, back up your database before you begin the upgrade.

Upgrading the Schema

To upgrade your schema from RSA Access Manager 6.1 and later to RSA Access Manager 6.2:

1. Copy the upgrade script from ***Installer Directory*\win32-x86\upgrade\mssql_61_to_62\update.sql** onto your machine.

   Note: For upgrade from Server 6.1 SP4 to 6.2, the upgrade script is available in this location:**\win32-x86\upgrade\mssql_61_4_to_62\update.sql**

2. Run the upgrade script.

To run the upgrade script on Microsoft SQL Server 2008 R2:

1. Log on to Microsoft SQL Server 2008 R2.
2. From the directory tree in the left pane, select **CT**.
3. Click **New Query**.

4. Click **File > Open > File**.
5. Open **update.sql**.
6. Click **Connect** when prompted to connect to the Database Engine.
7. Click **Execute**.
   The script sets up the Access Manager schema additions to the existing schema.
8. Check the output of the script for any error messages.
   If the script does not run completely due to some problem, identify the problem, address the issue, and rerun the script.

Next Steps

Your schema upgrade is complete. For instructions on upgrading your Administrative Console, see Chapter 13, Upgrading the Administrative Console.

7 Upgrading Database Schema on Sun Java System Directory Server

This chapter describes how to upgrade your schema from RSA Access Manager 6.1 to RSA Access Manager 6.2 on the Sun Java System Directory Server 7.0. This upgrade consists of schema additions only. It does not change your data.

Before You Begin

RSA Access Manager 6.2 supports only Sun Java System Directory Server 7.0. If you are using an earlier version of Sun Java Directory Server, you must upgrade it to Sun Java System Directory Server 7.0, before you perform the schema and data upgrade. Consult your Sun Java System Directory Server documentation for Directory Server upgrade instructions.

Upgrading the Schema

To upgrade your schema from RSA Access Manager 6.1 and later to RSA Access Manager 6.2:

1. Stop your Sun Java System Directory Server.
2. Make a backup copy of the RSA Access Manager 6.1 and later schema file.
   ***IPLANET-ROOT*/Servers/slapd-*SERVER-NAME*/config/schema/61rsa-cleartrust.ldif**
3. In the Sun Java System Directory Server schema directory, replace the existing schema file (.ldif file) with the RSA Access Manager 6.2 version. From the **data_adapters** directory on your RSA Access Manager 6.2 Installer Directory, copy the 6.2 schema file:
   - For Windows:
     ***Installer Directory*\win32-x86\data_adapters\ldap\iPlanet\62rsa-axm.ldif**
   - For Solaris:
     ***Installer Directory*/solaris-sparc/data_adapters/ldap/iPlanet/62rsa-axm.ldif**

- For AIX:
  ***Installer Directory*/aix-rs6000/data_adapters/ldap/iPlanet/62rsa-axm.ldif**
- For Linux:
  ***Installer Directory*/linux-x86/data_adapters/ldap/iPlanet/62rsa-axm.ldif**

4. Restart your Sun Java System Directory Server 7.0.

Note: You can use **iplanet-upgrade.ldif** file to view the schema changes that has occurred from earlier version to current version.

Next Steps

Your schema upgrade is complete. For instructions on upgrading your Administrative Console, see Chapter 13, Upgrading the Administrative Console.

8 Upgrading Database Schema on OpenDJ Server

This chapter describes how to upgrade your schema from RSA Access Manager 6.1 to RSA Access Manager 6.2 on the OpenDJ Server 2.4 and later versions. This upgrade consists of schema additions only. It does not change your data.

Upgrading the Schema

To upgrade your schema from RSA Access Manager 6.1 and later to RSA Access Manager 6.2:

1. Stop your OpenDJ Server.
2. Make a backup copy of the RSA Access Manager 6.1 and later schema file.
   ***OPENDJ-ROOT*/Servers/slapd-*SERVER-NAME*/config/schema/61rsa-axm.ldif**
3. In the OpenDJ Server schema directory, replace the existing schema file (.ldif file) with the RSA Access Manager 6.2 version. From the **data_adapters** directory on your RSA Access Manager 6.2 Installer Directory, copy the 6.2 schema file:
   - For Windows:
     ***Installer Directory*\win32-x86\data_adapters\ldap\OpenDJ\62rsa-axm.ldif**
   - For Solaris:
     ***Installer Directory*/solaris-sparc/data_adapters/ldap/OpenDJ/62rsa-axm.ldif**
   - For AIX:
     ***Installer Directory*/aix-rs6000/data_adapters/ldap/OpenDJ/62rsa-axm.ldif**
   - For Linux:
     ***Installer Directory*/linux-x86/data_adapters/ldap/OpenDJ/62rsa-axm.ldif**
4. Restart your OpenDJ Server.

Note: You can use **OpenDJ-upgrade.ldif** file to view the schema changes that has occurred from earlier version to current version.

Next Steps

Your schema upgrade is complete. For instructions on upgrading your Administrative Console, see Chapter 13, Upgrading the Administrative Console.

9 Upgrading Database Schema on Active Directory

This chapter describes how to upgrade your schema from RSA Access Manager 6.1 to RSA Access Manager 6.2 on Microsoft Windows Server 2008 Active Directory. This upgrade consists of schema additions only. It does not change your data.

Before You Begin

RSA Access Manager 6.2 supports Microsoft Windows Server 2008 Active Directory. If you are using Microsoft Windows 2000 Active Directory or Microsoft Windows Server 2003 Active Directory, you must upgrade it to Microsoft Windows Server 2008 Active Directory before you perform the schema upgrade. Consult your Microsoft documentation for upgrade instructions.

Upgrading the Schema

To upgrade your LDAP schema from RSA Access Manager 6.1 and later to RSA Access Manager 6.2:

1. Enable schema modifications on your Active Directory machine.

   For more information, see "Enabling Schema Changes on Active Directory" in the chapter "Installing the LDAP Data Adapter" in the *Servers Installation and Configuration Guide*.
2. Log on to the primary domain controller (the Active Directory schema master machine) as an administrator.
3. From your RSA Access Manager 6.2 Installer Directory, copy

   ***Installer Directory*\win32-x86\upgrade\ad_61_to_62\ad-upgrade.ldif**

   to

   Installation Directory\data_adapters\ldap\activedirectory\ad-upgrade.ldif
4. From your RSA Access Manager 6.2 Installer Directory, copy

   ***Installer Directory*\win32-x86\upgrade\ad_61_to_62\ad-upgrade.bat**

   to

   Installation Directory\data_adapters\ldap\activedirectory\ad-upgrade.bat

5. Run the RSA Access Manager schema installation script. From a command prompt, change to the **Installation Directory\data_adapters\ldap\activedirectory** directory, and type:

   ```
   ad-upgrade "localhost:389""dc=domain,dc=com"
   ```

   where:

   - *localhost:389* is the hostname and port number of Active Directory
   - *domain* and *com* are the base DN where your RSA Access Manager schema is installed

6. In the Microsoft Management Console (MMC), right-click on the **Active Directory Schema** Snap-in, and select **Reload the Schema**.

7. Open your **Installation Directory/conf/ldap.conf** file, and check your cleartrust.data.ldap.user.basedn parameter setting.

   Pay close attention to the uppercase and lowercase characters. The case must match the DN as stored in the Active Directory. For example, if "Users" is capitalized in the base DN of your user store, set it as:

   ```
   cleartrust.data.ldap.user.basedn:cn=Users,
   dc=rsasecurity, dc=com
   ```

Next Steps

Your schema upgrade is complete. For instructions on upgrading your Administrative Console, see Chapter 13, Upgrading the Administrative Console.

10 Upgrading Database Schema on Active Directory-Active Directory Lightweight Directory Services

This chapter describes how to upgrade your schema from RSA Access Manager 6.1 and later to RSA Access Manager 6.2 on Active Directory-Active Directory Lightweight Directory Services.

Note: In this document, Active Directory-Active Directory Lightweight Directory Services (AD-AD LDS) is used in the context of Microsoft Windows Server 2008.

Upgrading the Schema

To upgrade your schema from RSA Access Manager 6.1 and later to RSA Access Manager 6.2:

1. Enable schema modifications on your Active Directory-Active Directory Lightweight Directory Services machine.

   For more information, see "Enable Schema Changes on Active Directory" in the chapter "Installing the LDAP Data Adapter" in the *Servers Installation and Configuration Guide*.

2. Log on to the primary domain controller (the Active Directory schema master machine) as an administrator.

3. From your RSA Access Manager 6.2 Installer Directory, copy

   ***Installer Directory*\win32-x86\upgrade\ad_61_to_62\ad-upgrade.ldif**

   to

   Installation Directory\data_adapters\ldap\activedirectory\ad-upgrade.ldif

4. From your RSA Access Manager 6.2 Installer Directory, copy

   ***Installer Directory*\win32-x86\upgrade\ad_61_to_62\ad-upgrade.bat**

   to

   Installation Directory\data_adapters\ldap\activedirectory\ad-upgrade.bat

5. Run the Access Manager schema installation script. From a command prompt, change to the **Installation Directory\data_adapters\ldap\activedirectory** directory, and type:

   ```
   ad-upgrade "localhost:389" "dc=domain,dc=com"
   ```

   where:

   - *localhost:389* is the hostname and port number of Active Directory
   - *domain* and *com* are the base DN where your Access Manager schema is installed in Active Directory-Active Directory Lightweight Directory Services.

   This upgrades the Active Directory-Active Directory Lightweight Directory Services schema.

6. Run the Access Manager schema installation script again. From a command prompt, change to the **Installation Directory\data_adapters\ldap\activedirectory** directory, and type:

   ```
   ad-upgrade "localhost:50000"
   "CN={CB3D888F-F638-4C4F-AC1A-2B78AF41E846}"
   ```

   where:

   - *localhost:50000* is the hostname and port number of Active Directory-Active Directory Lightweight Directory Services
   - *CN={CB3D888F-F638-4C4F-AC1A-2B78AF41E846}* is the last part of the schema DN of Active Directory-Active Directory Lightweight Directory Services

   This upgrades the Active Directory-Active Directory Lightweight Directory Services schema.

7. In the Microsoft Management Console (MMC), right-click on the **Active Directory Schema** Snap-in, and select **Reload the Schema** to verify Active Directory-Active Directory Lightweight Directory Services schema.

   Active Directory-Active Directory Lightweight Directory Services schema update can be verified using the ADSI Edit in Microsoft Windows Server 2008.

8. Open your **Installation Directory/conf/ldap.conf** file, and check your cleartrust.data.ldap.user.basedn parameter setting.

   The cleartrust.data.ldap.user.basedn parameter is case-sensitive. The case must match the DN as stored in the Active Directory. For example, if “Users” is capitalized in the base DN of your user store, set it as:

   ```
   cleartrust.data.ldap.user.basedn:cn=Users,
   dc=rsasecurity, dc=com
   ```

Note: Upgrading Active Directory-Active Directory Lightweight Directory Services schema results in creating some unwanted classes and attributes in the Active Directory schema and Active Directory-Active Directory Lightweight Directory Services schema. These are just dummy entries and should not be used to edit the **ldap.conf** files.

Next Steps

Your schema upgrade is complete. For instructions on upgrading your Administrative Console, see Chapter 13, Upgrading the Administrative Console.

11 Upgrading Database Schema on Novell eDirectory

This chapter describes how to upgrade your schema from RSA Access Manager 6.1 and later to RSA Access Manager 6.2 on Novell eDirectory 8.8 and later versions. This upgrade consists of schema additions only. It does not change your data.

Before You Begin

RSA Access Manager 6.2 supports only Novell eDirectory 8.8 and later versions. If you are using earlier versions of Novell eDirectory, you must upgrade it to Novell eDirectory 8.8 and later versions, before you perform the schema and data upgrade. Refer your Novell documentation for upgrade instructions.

Upgrading the Schema

To upgrade your schema from RSA Access Manager 6.1 and later to RSA Access Manager 6.2:

1. Open the Novell iManager utility.
2. From the left pane, click **Schema > Extend Schema**.
3. In the ICE Wizard, select **Add schema from a file**, and click **Next**.
4. From the File type drop-down list, select **LDIF**.
5. From the File to import field, browse to **edir-upgrade.ldif**, and click **Next**.
6. Under the Select the Server section, enter the following LDAP server information:
   - Server IP address
   - Port
   - Choose the appropriate **.der** file if you are using SSL
7. Select **Authenticated Login**, enter the administrator user DN and the password, and click **Next**.
8. Click **Finish**.

Next Steps

Your schema upgrade is complete. For instructions on upgrading your Administrative Console, see Chapter 13, Upgrading the Administrative Console.

12 Upgrading Database Schema on Active Directory Lightweight Directory Services (AD LDS)

This chapter describes how to upgrade your schema from RSA Access Manager 6.1 SP4 to RSA Access Manager 6.2 on Microsoft Windows Server 2008 Active Directory Lightweight Directory Services. This upgrade consists of schema additions only. It does not change your data.

Upgrading the Schema

To upgrade your AD LDS schema from RSA Access Manager 6.1 SP4 to RSA Access Manager 6.2:

1. Log on to the primary domain controller (the Active Directory Lightweight Directory Services schema master machine) as an administrator.
2. From your RSA Access Manager 6.2 Installer Directory, copy
   ***Installer Directory*\win32-x86\upgrade\adlds_61_4_to_62\adlds-upgrade.ldif**
   to
   Installation Directory\data_adapters\ldap\adlds\adlds-upgrade.ldif
3. From your RSA Access Manager 6.2 Installer Directory, copy
   ***Installer Directory*\win32-x86\upgrade\adlds_61_4_to_62\adlds-upgrade.bat**
   to
   Installation Directory\data_adapters\ldap\adlds\adlds-upgrade.bat
4. Run the RSA Access Manager schema installation script. From a command prompt, change to the **Installation Directory\data_adapters\ldap\adlds** directory, and type as per below example:

   ```
   adlds-upgrade "localhost:50000"
   ```

   CN={CB3D888F-F638-4C4F-AC1A-2B78AF41E846}

   where:

   - *localhost:50000* is the hostname and port number of AD LDS
   - *CN is the* is the last part of the schema DN that you copied and saved.
5. In the Microsoft Management Console (MMC), right-click on the **Active Directory Lightweight Directory Services Schema** Snap-in, and select **Reload the Schema**.

6. Open your **Installation Directory/conf/ldap.conf** file, and check your cleartrust.data.ldap.user.basedn parameter setting.

   Pay close attention to the uppercase and lowercase characters. The case must match the DN as stored in the Active Directory. For example, if "Users" is capitalized in the base DN of your user store, set it as:

   ```
   cleartrust.data.ldap.user.basedn:cn=Users,
   dc=rsasecurity, dc=com
   ```

Next Steps

Your schema upgrade is complete. For instructions on upgrading your Administrative Console, see Chapter 13, Upgrading the Administrative Console.

13 Upgrading the Administrative Console

The instructions in this chapter describe how to replace your existing Administrative Console with the RSA Access Manager 6.2 Administrative Console.

Upgrading the Administrative Console

This upgrade procedure applies to upgrades from RSA Access Manager 6.1 and later to RSA Access Manager 6.2.

To upgrade the Entitlements Manager:

1. On your application server machine, find the deployment directory of your existing Administrative Console application. For example, webapps/admingui.
2. Back up your Administrative Console configuration file, **admingui.cfg**.

Note: If the **admingui.cfg** file is not located in the deployment directory, open the Administrative Console **web.xml** file (typically, the path is similar to webapps/admingui/WEB-INF/web.xml), and check the setting of the web.config.directory parameter. This shows the path to **admingui.cfg**.

3. Remove your existing Administrative Console application from the application server, or rename the deployment directory so that the application can no longer be started. For example, you might rename the directory from “admingui” to “admingui-backup”.
4. Install the RSA Access Manager Administrative Console. For instructions, see the chapter “Installing the RSA Access Manager Administrative Console” in the *Servers Installation and Configuration Guide*.

Next Steps

Once you have completed the Administrative Console upgrade, you may need to upgrade your Agents for use with RSA Access Manager 6.2. To find out which Agent versions are compatible, see “Supported RSA Access Manager Agents” section in the chapter “RSA Access Manager 6.2 Server Installation and Configuration Overview” of the *Servers Installation and Configuration Guide*.

14 Upgrading the APIs

This chapter describes how to upgrade applications you have written using the RSA Access Manager APIs.

API Client Compatibility and Updates

The RSA Access Manager 6.2 Servers are compatible with the RSA Access Manager 6.1 and later Administrative and Runtime API clients. No replacement of .jar files or recompilation is necessary. For more information on installing the RSA Access Manager 6.2 SDK on Windows and UNIX, see "Install RSA Access Manager 6.2 SDK" in the chapter "Install RSA Access Manager 6.2 Servers on Windows" and "Install and Configure RSA Access Manager 6.2 Servers on UNIX" respectively, in the *Servers Installation and Configuration Guide*.

The DCOM Administrative and Runtime APIs have been deprecated and are not packaged in this release. For information on API changes, see the *Developer's Guide.* This guide is available in the SDK archive on your RSA Access Manager 6.2 Installer Directory. When you unpack the SDK archive, you can find the *Developer's Guide* at **SDK_HOME/sdk/docs/dev_guide/index.html** and the *API Delta Document* at **SDK_HOME/sdk/docs/api_delta/index.html**.

15 Upgrading the User Self-Service Console

This chapter describes how you can upgrade or replace your existing Self-Service Console with the RSA Access Manager 6.2 User Self-Service Console.

Upgrading the Self-Service Console

To upgrade your existing RSA Access Manager 6.1 Self-Service Console and later to RSA Access Manager 6.2:

Note: This upgrade step is applicable for upgrades from RSA Access Manager Server 6.1 SP1, SP2, and SP3 to RSA Access Manager Server 6.2.

Note: RSA recommends to backup existing data store connected by Entitlement server, as the user properties will be modified post upgrade.

1. Navigate to the **6.2 AXM_HOME/migration** directory.
2. Run the **self-service-users-migration-tool.bat** or **self-service-users-migration-tool.sh** file.
3. Enter the location of the existing self-service configuration file on the migration tool.

   A warning message appears stating that secret questions and answers for all the users registered with self service application will be upgraded.
4. Enter **Yes** to continue with the user migration.
5. Enter the passphrase to create new lockbox file.
6. Enter fully qualified hostname of the system where you want to deploy self-service console. For multiple hosts, enter comma separated fully qualified hostname, for example: aserver.axm.com.

   Result: The Self-Service Console Migration tool creates the configuration file and lockbox file in **AXM_HOME/migration** directory.

To upgrade your existing RSA Access Manager 6.1 SP4 Self-Service Console to RSA Access Manager 6.2:

1. Navigate to the **6.2 AXM_HOME/migration** directory.
2. Run the **self-service-users-migration-tool.bat** or **self-service-users-migration-tool.sh** file.
3. Enter the location of the existing self-service configuration file on the migration tool.
4. Enter the lockbox passphrase used to create the lockbox file during 6.1 SP4 upgrade.

Result: The Self-Service Console Migration tool creates the configuration file in **AXM_HOME/migration** directory.

You can use the latest configuration file and lockbox file to deploy Self-Service Console. For instructions see, chapter “Deploy RSA Access Manager User Self-Service Console” in *Server Installation and Configuration Guide*.

Post-Upgrade Task

After upgrading the **selfservice.conf** file and self-service console, you must perform the following steps, to complete upgrade successfully:

1. Update the environment variable (PATH in Windows, LIBPATH in AIX and LD_LIBRARY_PATH on other Unix platforms) to point to the **/cst** folder in **AXM_HOME** directory.
2. Restart the application server.

16 Upgrading the SNMPv3

As part of the RSA Access Manager 6.2 installation process, an Instrumentation Server is installed on each machine hosting Access Manager Servers. The Instrumentation Server enables network management using a third-party Network Management System (NMS) that communicates with the Access Manager Servers using Simple Network Management Protocol (SNMP). An NMS reveals how Access Manager Servers are functioning in a production environment.

This chapter describes how to upgrade SNMPv3 support for RSA Access Manager Server 6.2

To upgrade SNMPv3, complete the following steps:

1. Shut down the Instrumentation Server.
2. Edit **encryptutil.bat** file and set ***AXM_HOME*** to 6.2 installation directory.
3. Encrypt the following parameters in **snmp-access-policy.xml** file:
   - securityPassphrase
   - privacyPassphrase
4. Restart the Instrumentation Server.

Note: For information about SNMP connection parameters,see chapter "Simple Network Management Protocol Support" in *Server Installation and Configuration Guide*.