RSA Access Manager 6.1
Upgrade Guide

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**

Trademarks

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

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 Security. To view the text of the license agreements applicable to third-party software in this product, click **Help > About** in the Administrative Console.

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.

August 2009

Contents

Preface

About This Guide

The Upgrade guide describes how to upgrade your:

- RSA ClearTrust 5.5.3 Servers, Data Adapters, LDAP data, and Administrative Console to RSA Access Manager 6.1.
- RSA Access Manager 6.0 and later Servers and Data Adapters to RSA Access Manager 6.1.

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 (DVD, CDs, licenses and documentation), specifies the location of documentation on the DVD, 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.

RSA 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	**www.rsasecured.com**

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

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

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

Before You Begin

RSA Access Manager 6.1 supports upgrades from RSA ClearTrust 5.5.3 and RSA Access Manager 6.0 and later.

Make sure that you upgrade to one of the supported operating systems for RSA Access Manager 6.1. To find out which operating systems are supported, see "Platform and Operating System Requirements" in the chapter "Preparing for Installation" in the *Servers Installation and Configuration Guide*.

To find out, which data store types are supported for upgrades from RSA ClearTrust 5.5.3 and RSA Access Manager 6.0 and later to RSA Access Manager 6.1, see "Supported Data Store Servers" in the chapter "Preparing for Installation" in the *Servers Installation and Configuration Guide*.

Important: During upgrade, the Sybase or PostgreSQL configuration files are not upgraded. You are prompted to enter the new data store details. The database schema update is not supported for Sybase and PostgreSQL. You must manually move to a supported data store.

Note: Throughout this document, RSA ClearTrust is referred to as RSA Access Manager, unless otherwise specified.

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 6.1 DVD is called ***DVD_ROOT***.

Overview of Upgrade Steps

You must perform the following steps to complete the upgrade process.

1. Upgrade your servers:
   - For information on Windows installations, see Chapter 2, "Upgrading Servers on Windows."
   - For information on UNIX installations, see Chapter 3, "Upgrading Servers on UNIX."
2. Upgrade your SQL or LDAP data stores:
   - For installations using Oracle, see Chapter 4, "Upgrading Database Schema on Oracle."
   - For installations using Microsoft SQL, see Chapter 5, "Upgrading Database Schema on Microsoft SQL Server."
   - For installations using Sun Java System Directory Server, see Chapter 6, "Upgrading Database Schema on Sun Java System Directory Server."
   - For installations using Active Directory, see Chapter 7, "Upgrading Database Schema on Active Directory."
   - For installations using Novell eDirectory, see Chapter 9, "Upgrading Database Schema on Novell eDirectory."
3. For Sun Java System Directory Server, Active Directory, and Novell eDirectory only, populate LDAP data for your LDAP data store. For more information, see Chapter 10, "Populating LDAP Data for Delegated Administration."
4. Upgrade your Entitlements Manager, if applicable. For more information, see Chapter 11, "Upgrading the Administrative Console."
5. Upgrade your APIs, if applicable. For more information, see Chapter 12, "Upgrading the APIs."

Upgrading Your Agents

You may need to upgrade your Agents for use with RSA Access Manager 6.1. To find out which Agent versions are compatible, see "Required Components" in the chapter "Preparing for Installation" in the *Servers Installation and Configuration Guide*. For Agent upgrade instructions, see your RSA Access Manager Agent documentation.

Next Steps

For instructions on upgrading your servers, see the following chapters:

- For Windows upgrades, see Chapter 2, "Upgrading Servers on Windows."
- For UNIX upgrades, see Chapter 3, "Upgrading Servers on UNIX."

2 Upgrading Servers on Windows

This chapter describes how to upgrade your RSA Access Manager for the following upgrade paths:

- RSA ClearTrust 5.5.3 to RSA Access Manager 6.1
- RSA Access Manager 6.0 and later to RSA Access Manager 6.1

Upgrading Your Servers

RSA recommends that you back up your existing installation of RSA Access Manager before upgrading your Access Manager servers.

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

Backing Up Your Existing Installation

To back up your existing installation:

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.
3. Make a backup copy of your existing RSA Access Manager installation (the entire contents of your ***AXM_HOME*** directory).

Important: The upgrade script migrates parameter values that have been encrypted using the RSA Access Manager Cryptedit tool. You must manually copy the encrypted stores (.enc files) from your existing Access Manager installation to the **conf** directory of your RSA Access Manager 6.1 installation. From the configuration files of your existing Access Manager installation, copy the parameters marked for encryption (using the .cleartext=false flag) to the RSA Access Manager 6.1 configuration files.

Running the Upgrade

To run the upgrade:

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 6.1 DVD, navigate to **\win32-x86\axm_servers**.
3. Double-click **Setup.exe**.
4. Click through the standard Windows installation dialog boxes for Welcome, Select Region, and License Agreement.
5. In the Installation Type dialog box, click **Upgrade > Next**.
6. In the Upgrade Version Selection dialog box, click **5.5** (5.5.3) or **6.0.x** (6.0 and later).
7. In the Current Installation Folder dialog box, specify the ***AXM_HOME*** directory, and click **Next**.

   For RSA ClearTrust 5.5.3, the typical path is **C:\Program Files\RSA\ClearTrust**. For RSA Access Manager 6.0 and later, the typical path is **C:\Program Files\RSA\ClearTrust Servers 6.0**.
8. In the Destination Folder dialog box, select the directory where you will install your RSA Access Manager 6.1 software, and click **Next**. This directory becomes your RSA Access Manager 6.1 root directory.
9. The installer's upgrade routine runs automatically. When it finishes upgrading the configuration files, do one of the following:
   - If the message "Upgrade procedure ... was successful" appears, click **OK**. Navigate to the **\logs** subdirectory in your RSA Access Manager 6.1 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 these steps to address the problem:
     - Navigate to the **\logs** subdirectory in your RSA Access Manager 6.1 root directory.
     - View the **upgrade.err** and **upgrade.log** files to find the nature of the problem.

– Fix the problem by editing your pre-upgrade configuration files.
– Rerun the upgrade.

Editing Your Configuration Files

To edit the configuration files:

Open your ***AXM_HOME*\conf\keyserver.conf** file, and edit the cleartrust.keyserver.token_lifetime and cleartrust.keyserver.session_key_life parameters, setting the session_key_life to half the token_lifetime. The default setting is:

```
cleartrust.keyserver.token_lifetime=1 hour
cleartrust.keyserver.session_key_life=30 mins
```

Providing the RSA ClearTrust Server Alias when Upgrading from RSA ClearTrust 5.5.3 to RSA Access Manager 6.1

If your installation includes RSA ClearTrust servers that communicate over mutually authenticated SSL, you must provide a server alias for your ClearTrust Server using the cleartrust.net.ssl.private.key_alias parameter.

Note: If you upgrade a Server installation with an incorrect cleartrust.net.ssl.private.key_alias setting, the Servers fail to start after the upgrade, and prints the following error: **javax.net.ssl.SSLException: No available certificate corresponds to the SSL cipher suites which are enabled. at com.sun.net.ssl.internal.ssl.SSLServerSocketImpl.a(Unknown Source) at com.sun.net.ssl.internal.ssl.SSLServerSocketImpl.accept(Unknown Source)**

To provide the server alias for your RSA Access Manager Server:

1. Run your upgraded RSA Access Manager Server with the flag **-Djavax.net.debug=all**.
2. Inspect the messages that display in the monitor window. The server alias name is specified on a line that reads:

   "found key for : *mykey*"

   where *mykey* is the name of your server.
3. Open the RSA Access Manager Server configuration file, and replace the value for the cleartrust.net.ssl.private.key_alias parameter with this new value. Note that this value is case-sensitive.

Next Steps

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

- Oracle. See Chapter 4, "Upgrading Database Schema on Oracle."
- Microsoft SQL Server. See Chapter 5, "Upgrading Database Schema on Microsoft SQL Server."
- Sun Java System Directory Server. See Chapter 6, "Upgrading Database Schema on Sun Java System Directory Server."
- Microsoft Windows Server 2003 Active Directory. See Chapter 7, "Upgrading Database Schema on Active Directory."
- Novell eDirectory. See Chapter 9, "Upgrading Database Schema on Novell eDirectory."

3 Upgrading Servers on UNIX

This chapter describes how to upgrade your software for the following upgrade paths:

- RSA ClearTrust 5.5.3 to RSA Access Manager 6.1 (Solaris 9)
- RSA Access Manager 6.0 to RSA Access Manager 6.1 (Solaris, Linux, and AIX)

Upgrading Your Servers

Perform the upgrade 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.

Important: Before you upgrade the AIX installations, download and install the AIX (64-bit or 32-bit) JDK 1.5 or 1.6. For more information, contact your IBM representative or go to **http://www.ibm.com/developerworks/java/jdk/**. Note the path where you installed the IBM AIX JRE (for example, /usr/java14/jre).

Running the Upgrade Script

In the following procedure, use the RSA Access Manager installation script upgrade routine. Valid input options for this script include **y** for yes and **n** for no. Press ENTER to accept default values in square braces (for example, [axm]).

Important: For AIX and Linux users only: Do not press CTRL+C to stop the installation. If you stop the installation script before completion, not all IBM install packages are installed on AIX, and not all rpm packages are installed on Linux. Problems could arise during future uninstallation and reinstallation attempts. If you have entered any incorrect information during installation, allow the install script to finish, and run **uninstall-server.sh** to make changes.

To run the upgrade script:

1. Log on as user root.
2. Stop all the RSA Access ManagerServers that are running.Shut down or redirect any RSA Access Manager Agents that rely on the Authorization Servers that you are upgrading.
3. Make a backup copy of your existing RSA Access Manager installation (the entire contents of your ***AXM_HOME*** directory).

Important: The upgrade script migrates parameter values that have been encrypted using the RSA Access Manager Cryptedit tool. You must manually copy the encrypted stores (.enc files) from the your existing Access Manager installation to the **conf** directory of your RSA Access Manager 6.1 installation. From the configuration files of your existing Access Manager installation, copy the parameters marked for encryption (using the .cleartext=false flag) to the RSA Access Manager 6.1 configuration files.

4. On the RSA Access Manager 6.1 DVD, navigate to the following:
   - For Solaris: **/solaris-sparc/axm_servers**
   - For AIX: **/aix-rs6000/axm_servers**
   - For Linux: **/linux-x86/axm_servers**

   By default, the Access Manager files are installed in one of these locations:
   - On Solaris: **/opt/axm/server-61**
   - On AIX: **/usr/axm/server-61**
   - On Linux: **/opt/axm/server-61**
5. Run the installation script:

   ```
   # ./install-server.sh
   ```
6. At **Is this a new installation or an upgrade**, enter **u** for upgrade.
7. At **Version of Access Manager servers to be upgraded**, enter one of the following:
   - **5.5**
   - **6.0.x** (6.0 and later)
8. Follow these prompts for directory information:
   - At **Where are the existing *OLD_VERSION* Access Manager Servers installed?**, enter the RSA Access Manager application root directory of the installation you are upgrading. For example, if you are upgrading a version 6.0 installation, this path typically is **/opt/ctrust** for Solaris and Linux, and **/usr/ctrust** for AIX.
   - At **Installation Base Directory**, specify the root directory for the new RSA Access Manager 6.1 installation. In a typical installation, accept the default value of **/opt/axm** for Solaris and Linux or **/usr/axm** for AIX.
9. Accept the license agreement.

10. At **Access Manager user**, enter **y** to enter new user account and **n** to continue using the existing RSA Access Manager UNIX user account. RSA recommends that you use the existing RSA Access Manager UNIX user account. The default account name is axmuser.
11. The script reports the following progress:
    - "Beginning Upgrade of Access Manager Servers from *OLD_VERSION* to 6.1" indicates the start of the Server upgrade.
    - "Upgrade Complete" indicates the software upgrade is complete.
    - "Installation completed" indicates that the installation is complete.
12. After the installation is complete, your newly created configuration files contain the parameter settings used in your RSA ClearTrust 5.5.3 or your RSA Access Manager 6.0 and later installation. If you want to reconfigure the upgraded Server installation, press ENTER to continue with the configuration. To stop the script, press any other key.

Note: For information on using the configuration script, see "Installing the RSA Access Manager Servers on UNIX" in the *Servers Installation and Configuration Guide*.

13. Navigate to the **/logs** subdirectory in your RSA Access Manager 6.1 root directory, and do the following:
    a. Inspect **upgrade.log** for a summary of the parameters that have changed.
    b. If there is an **upgrade.err** file, open the file, read the error log, edit your pre-upgrade configuration files to fix the problem, and rerun the installation script from step 5.

Editing Your Configuration Files

To edit the configuration files:

Open your ***AXM_HOME*/conf/keyserver.conf** file, and edit the cleartrust.keyserver.token_lifetime and cleartrust.keyserver.session_key_life parameters, setting the session_key_life to half the token_lifetime. The default setting is:

```
cleartrust.keyserver.token_lifetime=1 hour
cleartrust.keyserver.session_key_life=30 mins
```

Providing the RSA ClearTrust Server Alias when Upgrading from RSA ClearTrust 5.5.3 to RSA Access Manager 6.1

If your installation includes RSA ClearTrust Servers that communicate over mutually authenticated SSL, you must provide a server alias for your ClearTrust Server using the cleartrust.net.ssl.private.key_alias parameter.

Note: If you upgrade a Server installation with an incorrect cleartrust.net.ssl.private.key_alias setting, the Servers fail to start after the upgrade, and prints the following error: **javax.net.ssl.SSLException: No available certificate corresponds to the SSL cipher suites which are enabled. at com.sun.net.ssl.internal.ssl.SSLServerSocketImpl.a(Unknown Source) at com.sun.net.ssl.internal.ssl.SSLServerSocketImpl.accept(Unknown Source)**

To provide the server alias for your RSA ClearTrust Server:

1. Run your upgraded RSA Access Manager Server with the flag **-Djavax.net.debug=all**.
2. Inspect the messages that display in the monitor window. The server alias name is specified on a line that reads:

   `"found key for : mykey"`

   where *mykey* is the name of your server.
3. Open the RSA Access Manager Server configuration file, and replace the value for the cleartrust.net.ssl.private.key_alias parameter with this new value. Note that this value is case-sensitive.

Next Steps

See the instructions for your data store below:

- Oracle. See Chapter 4, "Upgrading Database Schema on Oracle."
- Microsoft SQL Server. See Chapter 5, "Upgrading Database Schema on Microsoft SQL Server."
- Sun Java System Directory Server. See Chapter 6, "Upgrading Database Schema on Sun Java System Directory Server."
- Microsoft Windows Server 2003 Active Directory. See Chapter 7, "Upgrading Database Schema on Active Directory."
- Novell eDirectory. See Chapter 9, "Upgrading Database Schema on Novell eDirectory."

4 Upgrading Database Schema on Oracle

This chapter describes how to upgrade the database schema from RSA ClearTrust 5.5.3 and RSA Access Manager 6.0 and later to RSA Access Manager 6.1 on Oracle. This upgrade consists of schema additions only. It does not change your data.

Important: This upgrade supports Oracle 10g2 and Oracle 10g RAC databases. If your installation is running on an earlier version of Oracle database, upgrade the database to Oracle 10g2 or Oracle 10g 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 ClearTrust 5.5.3 to RSA Access Manager 6.1:

1. Copy the upgrade script from the RSA Access Manager 6.1 DVD onto your machine:
   - On Windows:
     ***DVD_ROOT*\win32-x86\upgrade\oracle_55_to_61\update.sql**
   - On Solaris:
     ***DVD_ROOT*/solaris-sparc/upgrade/oracle_55_to_61/update.sql**
   - On AIX:
     ***DVD_ROOT*/aix-rs6000/upgrade/oracle_55_to_61/update.sql**
   - On Linux:
     ***DVD_ROOT*/linux-x86/upgrade/oracle_55_to_61/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 6.0 and later to RSA Access Manager 6.1:

1. Copy the upgrade script from the RSA Access Manager 6.1 DVD onto your machine:
   - On Windows:
     ***DVD_ROOT*\win32-x86\upgrade\oracle_60_to_61\update.sql**
   - On Solaris:
     ***DVD_ROOT*/solaris-sparc/upgrade/oracle_60_to_61/update.sql**
   - On AIX:
     ***DVD_ROOT*/aix-rs6000/upgrade/oracle_60_to_61/update.sql**
   - On Linux:
     ***DVD_ROOT*/linux-x86/upgrade/oracle_60_to_61/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 11, "Upgrading the Administrative Console."

5 Upgrading Database Schema on Microsoft SQL Server

This chapter describes how to upgrade your schema from RSA ClearTrust 5.5.3 and RSA Access Manager 6.0 and later to RSA Access Manager 6.1 on Microsoft SQL Server. The RSA Access Manager 6.1 schema includes additions to support delegated administration and changes to standardize column lengths.

Important: This upgrade supports Microsoft SQL Server 2005.

Note: Running the upgrade script results in an increase in the maximum size of your database because column lengths have changed in RSA Access Manager 6.1.

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 ClearTrust 5.5.3 to RSA Access Manager 6.1:

1. Copy the upgrade script from ***DVD_ROOT*\win32-x86\upgrade\mssql_55_to_61\update.sql** onto your machine.
2. Run the upgrade script.

To upgrade your schema from RSA Access Manager 6.0 and later to RSA Access Manager 6.1:

1. Copy the upgrade script from ***DVD_ROOT*\win32-x86\upgrade\mssql_60_to_61\update.sql** onto your machine.
2. Run the upgrade script.

To run the upgrade script on Microsoft SQL Server 2005:

1. Log on to Microsoft SQL Server 2005.
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 11, "Upgrading the Administrative Console."

6 Upgrading Database Schema on Sun Java System Directory Server

This chapter describes how to upgrade your schema from RSA ClearTrust 5.5.3 and RSA Access Manager 6.0 and later to RSA Access Manager 6.1 on the Sun Java System Directory Server. This upgrade consists of schema additions only. It does not change your data.

Before You Begin

RSA Access Manager 6.1 supports only Sun Java System Directory Server 5.2 and 6.3. If you are using an earlier version of Sun Java Directory Server, you must upgrade it to Sun Java System Directory Server 5.2 or 6.3, 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 ClearTrust 5.5.3 or RSA Access Manager 6.0 and later to RSA Access Manager 6.1:

1. Stop your Sun Java System Directory Server.
2. Make a backup copy of the RSA ClearTrust 5.5.3 or the RSA Access Manager 6.0 and later schema file.

   ***IPLANET-ROOT*/Servers/slapd-*SERVER-NAME*/config/schema/60rsa-cleartrust.ldif**
3. In the Sun Java System Directory Server schema directory, replace the existing schema file (.ldif file) with the RSA Access Manager 6.1 version. From the **data_adapters** directory on your RSA Access Manager 6.1 DVD, copy the 6.1 schema file:
   - For Windows:

     ***DVD_ROOT*\win32-x86\data_adapters\ldap\iplanet\61rsa-axm.ldif**
   - For Solaris:

     ***DVD_ROOT*/solaris-sparc/data_adapters/ldap/iplanet/61rsa-axm.ldif**

- For AIX:
  ***DVD_ROOT*/aix-rs6000/data_adapters/ldap/iplanet/61rsa-axm.ldif**
- For Linux:
  ***DVD_ROOT*/linux-x86/data_adapters/ldap/iplanet/61rsa-axm.ldif**

4. Restart your Sun Java System Directory Server.

Next Steps

You must populate the qualified name of existing administrative groups. For more information, see Chapter 10, "Populating LDAP Data for Delegated Administration."

Your schema upgrade is complete. For instructions on upgrading your Administrative Console, see Chapter 11, "Upgrading the Administrative Console."

7 Upgrading Database Schema on Active Directory

This chapter describes how to upgrade your schema from RSA ClearTrust 5.5.3 and RSA Access Manager 6.0 and later to RSA Access Manager 6.1 on Microsoft Windows Server 2003 Active Directory and 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 6.1 supports only Microsoft Windows Server 2003 Active Directory and Microsoft Windows Server 2008 Active Directory. If you are using Microsoft Windows 2000 Active Directory, you must upgrade it to Microsoft Windows Server 2003 Active Directory or 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 ClearTrust 5.5.3 to RSA Access Manager 6.1:

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 6.1 DVD, copy

   ***DVD_ROOT*\win32-x86\upgrade\ad_55_to_61\ad-upgrade.ldif**

   to

   ***AXM_HOME*\data_adapters\ldap\activedirectory\ad-upgrade.ldif**

4. From your RSA Access Manager 6.1, copy
   ***DVD_ROOT*\win32-x86\upgrade\ad_55_to_61\ad-upgrade.bat**
   to
   ***AXM_HOME*\data_adapters\ldap\activedirectory\ad-upgrade.bat**
5. Run the RSA Access Manager schema installation script. From a command prompt, change to the ***AXM_HOME*\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 ClearTrust 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 ***AXM_HOME*/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
   ```

To upgrade your LDAP schema from RSA Access Manager 6.0 and later to RSA Access Manager 6.1:

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 6.1 DVD, copy
   ***DVD_ROOT*\win32-x86\upgrade\ad_60_to_61\ad-upgrade.ldif**
   to
   ***AXM_HOME*\data_adapters\ldap\activedirectory\ad-upgrade.ldif**
4. From your RSA Access Manager 6.1, copy
   ***DVD_ROOT*\win32-x86\upgrade\ad_60_to_61\ad-upgrade.bat**
   to
   ***AXM_HOME*\data_adapters\ldap\activedirectory\ad-upgrade.bat**

5. Run the RSA Access Manager schema installation script. From a command prompt, change to the ***AXM_HOME*\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 ClearTrust 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 ***AXM_HOME*/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

You must populate the qualified name of existing administrative groups. For more information, see Chapter 10, "Populating LDAP Data for Delegated Administration."

Your schema upgrade is complete. For instructions on upgrading your Administrative Console, see Chapter 11, "Upgrading the Administrative Console."

8 Upgrading Database Schema on Active Directory-Active Directory Application Mode

This chapter describes how to upgrade your schema from RSA Access Manager 6.0 and later to RSA Access Manager 6.1 on Active Directory-Active Directory Application Mode.

Upgrading the Schema

To upgrade your schema from RSA Access Manager 6.0 and later to RSA Access Manager 6.1:

1. Enable schema modifications on your Active Directory-Active Directory Application Mode 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 6.1 DVD, copy

   ***DVD_ROOT*\win32-x86\upgrade\ad_60_to_61\ad-upgrade.ldif**

   to

   ***AXM_HOME*\data_adapters\ldap\activedirectory\ad-upgrade.ldif**

4. From your RSA Access Manager 6.1 DVD, copy

   ***DVD_ROOT*\win32-x86\upgrade\ad_60_to_61\ad-upgrade.bat**

   to

   ***AXM_HOME*\data_adapters\ldap\activedirectory\ad-upgrade.bat**

5. Run the Access Manager schema installation script. From a command prompt, change to the ***AXM_HOME*\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 Application Mode.

   This upgrades the Active Directory-Active Directory Application Mode schema.

6. Run the Access Manager schema installation script again. From a command prompt, change to the ***AXM_HOME*\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 Application Mode
   - *CN={CB3D888F-F638-4C4F-AC1A-2B78AF41E846}* is the last part of the schema DN of Active Directory-Active Directory Application Mode

   This upgrades the Active Directory-Active Directory Application Mode 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 Application Mode schema.

   Active Directory-Active Directory Application Mode schema update can be verified using the ADAM ADSI Edit.

8. Open your ***AXM_HOME*/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 Application Mode schema results in creating some unwanted classes and attributes in the Active Directory schema and Active Directory-Active Directory Application Mode schema. These are just dummy entries and would not be used to edit the **ldap.conf** files.

Next Steps

Upgrade your APIs. For more information, see Chapter 12, "Upgrading the APIs."

9 Upgrading Database Schema on Novell eDirectory

This chapter describes how to upgrade your schema from RSA ClearTrust 5.5.3 and RSA Access Manager 6.0 and later to RSA Access Manager 6.1 on Novell eDirectory. This upgrade consists of schema additions only. It does not change your data.

Before You Begin

RSA Access Manager 6.1 supports only Novell eDirectory 8.8. If you are using earlier versions of Novell eDirectory, you must upgrade it to Novell eDirectory 8.8 before you perform the schema and data upgrade. Refer your Novell documentation for upgrade instructions.

Upgrading the Schema

To upgrade your schema from RSA ClearTrust 5.5.3 to RSA Access Manager 6.1:

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**.

To upgrade your schema from RSA Access Manager 6.0 and later to RSA Access Manager 6.1:

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

You must populate the qualified name of existing administrative groups. For more information, see Chapter 10, "Populating LDAP Data for Delegated Administration."

Your schema upgrade is complete. For instructions on upgrading your Administrative Console, see Chapter 11, "Upgrading the Administrative Console."

10 Populating LDAP Data for Delegated Administration

In order to use the new delegated administration feature available in RSA Access Manager 6.1, you need to populate the qualified name of the existing administrative groups in your RSA ClearTrust 5.5.3 LDAP data store. For information on using delegated administration, see the chapter "Configuring Delegated Administration" in the *Administrator's Guide*.

Before You Begin

Make sure that you have successfully completed the upgrade installation process:

- For Windows upgrades, see Chapter 2, "Upgrading Servers on Windows."
- For UNIX upgrades, see Chapter 3, "Upgrading Servers on UNIX."

You must:

- Stop all the RSA Access Manager Servers that are running.
- Using your company's standard procedure, back up your database before you run the migration tool.
- Make sure that your LDAP data store is running.

Running the Migration Tool

From the RSA Access Manager 6.1 installation directory for your platform, locate the LDAP migration tool:

- For Windows: ***AXM_HOME*\upgrade\bin\ldap_55_to_61.bat**
- For UNIX: ***AXM_HOME*/upgrade/bin/ldap_55_to_61.sh**

To run the migration tool on Windows:

1. Open a command prompt, and change directory to ***AXM_HOME*\upgrade\bin**.
2. Type:

   ```
   ldap_55_to_61.bat
   ```

   After running the migration tool, the LDAP data store is updated with the new schema and data for delegated administration.

To run the migration tool on UNIX:

1. Open a shell, and change directory to ***AXM_HOME*/upgrade/bin/**.
2. Type:

   ```
   # ./ldap_55_to_61.sh
   ```

   After running the migration tool, the LDAP data store is updated with the new schema and data for delegated administration.

Note: You must run the tool from the specified location. To run properly, the tool needs configuration details and the JRE available in the RSA Access Manager 6.1 installation.

11 Upgrading the Administrative Console

The instructions in this chapter describe how to replace your existing Administrative Console with the RSA Access Manager 6.1 Administrative Console.

Upgrading the Administrative Console

This upgrade procedure applies to upgrades from RSA ClearTrust 5.5.3 and RSA Access MAnager 6.0 and later to RSA Access Manager 6.1.

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 6.1. To find out which Agent versions are compatible, see “Required Components” in the chapter “Preparing for Installation” in the *Servers Installation and Configuration Guide*. For Agent upgrade instructions, see your RSA Access Manager Agent documentation.

12 Upgrading the APIs

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

API Client Compatibility and Updates

The RSA Access Manager 6.1 Servers are compatible with the RSA ClearTrust 5.5.3 and RSA Access Manager 6.0 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 6.1 SDK on Windows and UNIX, see "Installing the RSA Access Manager SDK on Windows" and "Installing the RSA Access Manager SDK on UNIX" in the chapter "Installing the RSA Access Manager Servers" 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 6.1 DVD. 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**.