AUTHORIZED DOCUMENTATION

Driver for RSA Implementation Guide

Novell®
Identity Manager

4.0.1

April 18, 2011

www.novell.com

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. For more information on exporting Novell software, see the Novell International Trade Services Web page (http://www.novell.com/info/exports/). Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see Novell Documentation (http://www.novell.com/documentation/).

Novell Trademarks

For Novell trademarks, see Novell Trademark and Service List (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide

This guide explains how to install, configure, and manage the Identity Manager Driver for RSA.

Audience

This guide is for Novell eDirectory and Identity Manager administrators who are using the Identity Manager Driver for RSA.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Use the User Comment feature at the bottom of each page of the online documentation, or go to www.novell.com/documentation/feedback.html and enter your comments there.

Documentation Updates

For the most recent version of this guide, see *Identity Manager 4.0.1 Driver for RSA* on the Identity Manager 4.0.1 Drivers Documentation Web site (http://www.novell.com/documentation/idm401drivers/index.html).

Additional Documentation

For information on Identity Manager and other Identity Manager drivers, see the Identity Manager 4.0.1 Documentation Web site (http://www.novell.com/documentation/idm401).

Understanding the RSA Driver

1

The Identity Manager Driver for RSA (RSA driver) synchronizes data between the Identity Vault and RSA Authentication Manager. The driver supports the Subscriber and Publisher channels, uses filters to control objects and attributes, and uses policies to control data.

1.1 Supported Software Versions

The following RSA Authentication Manager versions are supported:

- 6.1
- 7.1

The following Novell Identity Manager versions are supported:

- 3.5.1
- 3.6.1
- 4.0.1

1.2 RSA Driver Concepts

1.2.1 Synchronizing Data

The Identity Manager Driver for RSA synchronizes data between an Identity Vault and RSA Authentication Manager. The driver can run anywhere that a Metadirectory server or Identity Manager Remote Loader is running if you are connecting to RSA Authentication Manager 7.1. If you are connecting to RSA Authentication Manager 6.1, the driver can only run on a Metadirectory server or Identity Manager Remote Loader installed on a Microsoft Windows server running RSA Authentication Manager 6.1.

The driver uses RSA APIs to bidirectionally synchronize changes between an Identity Vault and the connected RSA Authentication Manager.

1.2.2 How the RSA Driver Works

Channels, filters and policies control data flow.

Publisher and Subscriber Channels

The RSA driver supports Publisher and Subscriber channels:

- The Publisher channel reads information from RSA Authentication Manager and submits that information to an Identity Vault via the Metadirectory engine.

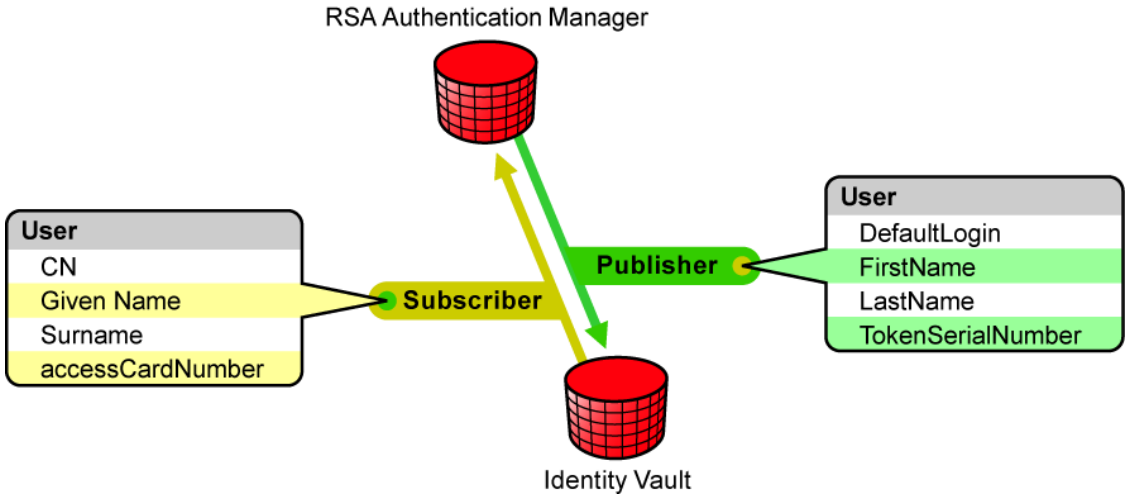
  By default, the Publisher channel checks for new RSA events every 3 minutes, processing up to 1000 entries at a time, starting with the first unprocessed entry.

- The Subscriber channel watches for additions and modifications to Identity Vault objects and issues RSA commands that make changes to RSA Authentication Manager.

Filters

Identity Manager uses filters to control which objects and attributes are shared. The default filter configurations for the RSA driver allow objects and attributes to be shared, as illustrated in the following figure:

Figure 1-1 *RSA Driver Filters*



Policies

Policies are used to control data synchronization between the driver and an Identity Vault.

The following table provides information on default policies. These policies and the individual rules they contain can be customized as explained in Chapter 6, “Synchronizing Data,” on page 27.

Table 1-1 *Default Policies*

Policy	Description
Schema Mapping	Maps the Identity Vault User object and selected properties to an RSA user object.
Publisher Create	Specifies that in order for a User to be created in an Identity Vault, the CN, Given Name, and Surname attributes must be defined.

Policy	Description
Matching	Specifies that a user object in an Identity Vault is the same object as an RSA user when the CN matches the RSA user's login.
Subscriber Create	Specifies that in order for a user to be created in RSA Authentication Manager, the CN, Given Name, and Surname attributes must be defined.

1.3 Support for Standard Driver Features

The RSA driver supports these standard driver features:

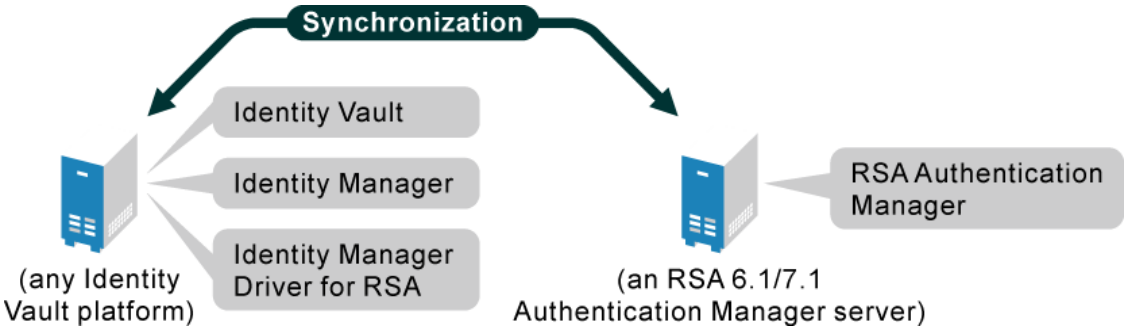
- Section 1.3.1, “Local and Remote Platforms,” on page 9
- Section 1.3.2, “Entitlements,” on page 9

1.3.1 Local and Remote Platforms

You can install the RSA driver locally or remotely.

An installation on the same computer where an Identity Vault and the Metadirectory engine are installed is referred to as a local configuration. The following figure illustrates a local configuration:

Figure 1-2 *A Local Configuration*



If platform or policy constraints prevent a local configuration, you can install the RSA driver on the server running the required platform or service. This installation is referred to as a remote configuration and requires the use of the Remote Loader service.

See “System Requirements” in the *Identity Manager 4.0 Integrated Installation Guide* for information about the supported platforms for the Metadirectory server and Remote Loader.

1.3.2 Entitlements

The RSA driver can be configured to use entitlements to manage user accounts in RSA Authentication Manager. When using entitlements, this driver works in conjunction with external services, such as the User Application or the Entitlements Service driver, to manage entitlement functionality. See the *Identity Manager 4.0 Entitlements Guide* for more information about entitlements.

Installing the Driver Files

2

The RSA driver files are not installed during the Identity Manager installation. Installation of these files must be performed manually.

If you are using the RSA driver to connect to an RSA Authentication Manager 7.1 environment, you also need to copy files and information from your RSA Authentication Manager environment into the Identity Manager installation.

If you are using the RSA driver to connect to an RSA Authentication Manager 6.1 environment, the driver must run directly on the RSA Authentication Manager server. Typically, you will run the driver within the Remote Loader in this scenario. For more information, see the *Identity Manager 4.0 Remote Loader Guide*.

The following sections explain how to install the RSA driver files from the Identity Manager installation media and how to install file dependencies for RSA Authentication Manager 7.1:

2.1 Installing the Driver Files

The RSA Driver files can be installed on multiple platforms.

2.1.1 Installing the Driver Files on Windows

This section contains instructions for copying the RSA driver files into your Identity Manager installation. The default installation locations are as follows:

- **Metadirectory Server:** `\Novell\NDS`
- **Remote Loader:** `\Novell\RemoteLoader`

To install the RSA driver files on Windows in one of the default locations:

1. Navigate to the `Additional Drivers\RSA` directory on the installation media.
2. Copy the following .jar files located in the `Additional Drivers\RSA` directory to the *installation*\lib directory:

   ```
   ACEShim.jar
   hsqldb.jar
   jace.jar
   jettison-1.2.jar
   ```

3 If you are installing RSA Authentication Manager 6.1, copy the `jace_api.dll` file contained in the `Additional Drivers\RSA` directory to the installation\ directory.

4 Continue with Section 2.2, “Copying Required Files and Information from RSA Authentication Manager 7.1,” on page 12.

2.1.2 Installing the Driver Files on SLES

To install the RSA driver files on SUSE Linux Enterprise Server (SLES):

1 At a root shell prompt, navigate to the `Additional Drivers\RSA` directory on the installation media.

2 Run the following command:

```
rpm -i novell-DXMLRSA.rpm
```

3 Continue with Section 2.2, “Copying Required Files and Information from RSA Authentication Manager 7.1,” on page 12.

2.1.3 Installing the Driver Files on Solaris

To install the RSA driver files on Solaris:

1 At a root shell prompt, navigate to the `Additional Drivers\RSA` directory on the installation media.

2 Run the following command:

```
pkgadd -d DXMLRSA.pkg
```

3 Continue with Section 2.2, “Copying Required Files and Information from RSA Authentication Manager 7.1,” on page 12.

2.2 Copying Required Files and Information from RSA Authentication Manager 7.1

Several files and authentication information from your RSA Authentication Manager 7.1 installation need to be copied to the Identity Manager installation. The following sections contain instructions for copying these files and pieces of information.

2.2.1 Copying RSA Files

The RSA Authentication Manager files must be copied to the appropriate Identity Manager driver library directory for your installation.

1 From a command prompt on your RSA Authentication Manager host, change directories to `RSA_AM_HOME/appserver/weblogic/server/lib/`.

2. At the command prompt, enter:

   ```
   java -jar ../../../modules/com.bea.core.jarbuilder_1.0.0.0.jar -profile
   wlfullclient
   ```

3. Change directories to RSA_AM_HOME/

4. At the command prompt, enter:

   ```
   appserver/jdk/bin/jar -xf components/ims/wars/console-ims.war WEB-INF/lib/
   ims-client.jar
   ```

5. At the command prompt, enter:

   ```
   appserver/jdk/bin/jar -xf components/ucm/console-ucm.war WEB-INF/lib/ucm-
   client.jar
   ```

6. Copy the following files in your RSA Authentication Manager server installation to the Identity Manager driver library directory:

   ```
   RSA_AM_HOME/appserver/license.bea
   RSA_AM_HOME/appserver/modules/com.bea.core.process_5.3.0.0.jar
   RSA_AM_HOME/appserver/weblogic/server/lib/wlfullclient.jar
   RSA_AM_HOME/appserver/weblogic/server/lib/wlcipher.jar
   RSA_AM_HOME/appserver/weblogic/server/lib/EccpressoAsn1.jar
   RSA_AM_HOME/appserver/weblogic/server/lib/EccpressoCore.jar
   RSA_AM_HOME/appserver/weblogic/server/lib/EccpressoJcae.jar
   RSA_AM_HOME/utils/jars/am-client.jar
   RSA_AM_HOME/utils/jars/systemfields-o.jar
   RSA_AM_HOME/utils/jars/thirdparty/axis-1.3.jar
   RSA_AM_HOME/utils/jars/thirdparty/commons-beanutils-1.7.0.jar
   RSA_AM_HOME/utils/jars/thirdparty/commons-discovery-0.2.jar
   RSA_AM_HOME/utils/jars/thirdparty/commons-lang-2.2.jar
   RSA_AM_HOME/utils/jars/thirdparty/commons-logging-1.0.4.jar
   RSA_AM_HOME/utils/jars/thirdparty/iScreen-1-1-0rsa-2.jar
   RSA_AM_HOME/utils/jars/thirdparty/iScreen-ognl-1-1-0rsa-2.jar
   RSA_AM_HOME/utils/jars/thirdparty/jdom-1.0.jar
   RSA_AM_HOME/utils/jars/thirdparty/jsafe-3.6.jar
   RSA_AM_HOME/utils/jars/thirdparty/jsafeJCE-3.6.jar
   RSA_AM_HOME/utils/jars/thirdparty/log4j-1.2.11rsa-3.jar
   RSA_AM_HOME/utils/jars/thirdparty/ognl-2.6.7.jar
   RSA_AM_HOME/utils/jars/thirdparty/spring-2.0.7.jar
   RSA_AM_HOME/WEB-INF/lib/ims-client.jar
   RSA_AM_HOME/WEB-INF/lib/ucm-client.jar
   ```

2.2.2 Exporting the Root Certificate

When you install RSA Authentication Manager, the system creates a self-signed root certificate and stores it in `RSA_AM_HOME/server/security/server_name.jks`. You must export this certificate from the server, and import it into a Java keystore file for the RSA driver. Use the Java keytool, as described below, to create the necessary Java keystore file for the RSA driver.

To export the server root certificate:

1. Change directories to `RSA_AM_HOME/appserver/`.
2. At the command prompt, enter:

   ```
   jdk/jre/bin/keytool -export -keystore RSA_AM_HOME/server/security/
   server_name.jks -file am_root.cer -alias rsa_am_ca
   ```

3. At the prompt for the keystore_password, press Enter without typing a password.

   A warning screen is displayed, but the server root certificate is still exported.

   The Java keytool outputs the certificate file to the directory specified in Step 1.

4. Import the certificate into a new Java keystore by entering:

   ```
   keytool -import -keystore trust.jks -storepass changeit -file am_root.cer
   -alias rsa_am_ca -trustcacerts
   ```

   You must provide a cacerts keystore password to import the server root certificate into a Java keystore. The Java default is `changeit`.

   The Java keytool displays a confirmation that the certificate was added to the keystore.

5. Copy the newly created `trust.jks` file to your driver library directory.

2.2.3 Obtaining the Command Client Username and Password

When you install RSA Authentication Manager, the system creates a command client username and password for secure connections to the command server. This username and password are randomly generated on creation, and are unique to each deployment.

You need to set command client and username values in the driver configuration for connection to the command server. Use the Manage Secrets utility as described in the following procedure to obtain these values from Authentication Manager.

1. From a command prompt on your RSA Authentication Manager host, change directories to `RSA_AM_HOME/utils`.
2. At the command prompt, enter:

   ```
   rsautil manage-secrets --action list
   ```

3. When prompted, enter your master password.

   The system displays the list of your internal system passwords.

4. Locate the values for your command client username and password. For example:

   Command Client User Name: CmdClient_vKr0bLK0

   Command Client User Password: f0SHbK2W4i

   These are the values that you must use for the driver configuration values for the command client username and password. Take note of these values for driver configuration. For more information, see Section A.1.5, “Driver Parameters,” on page 35.

IMPORTANT: Do not change the command client username and password. Any change to these values can cause serious issues in the operation of RSA Authentication Manager.

2.2.4 Setting Identity Manager Java Startup Properties for RSA Authentication Manager 7.1

For the RSA driver to communicate correctly with RSA Authentication Manager, Java startup properties for Identity Manager must be added.

In Windows

1. From the Control Panel, select the *System* icon.
2. Click the *Advanced* tab.
3. Click *Environment Variables*.
4. Do one of the following:
   - If the DHOST_JVM_OPTIONS variable exists, select it, then click *Edit* and proceed to Step 7.
   - If the DHOST_JVM_OPTIONS variable does not exist, proceed to Step 5.
5. Under *System Variables*, click *New*.
6. In the *Variable Name* field, enter:

   ```
   DHOST_JVM_OPTIONS
   ```

   IMPORTANT: The variable name must be all in capital letters.
7. In the *Variable Value* field, add the following text, ensuring that it is properly separated from any existing text by a space character:

   ```
   -Dsun.lang.ClassLoader.allowArraySyntax=true
   ```
8. Click *OK* in each dialog box until they are closed.

On Linux/Solaris

Set or modify the DHOST_JVM_OPTIONS environment variable to the following:

```
-Dsun.lang.ClassLoader.allowArraySyntax=true
```

Preparing RSA Authentication Manager

3

To prepare the RSA Authentication Manager server you are connecting to, you must create a user account through which the RSA driver can authenticate to the RSA Authentication Manager server.

The following sections provide instructions based on the version of RSA Authentication Manager you will be connecting to:

- Section 3.1, “Creating an RSA Authentication Manager 7.1 User Object with SuperAdminRole Rights,” on page 17
- Section 3.2, “Creating an RSA Authentication Manager 6.1 User Object with Administrator Rights,” on page 17

3.1 Creating an RSA Authentication Manager 7.1 User Object with SuperAdminRole Rights

You need to create an RSA Authentication Manager User object with SuperAdminRole rights for the RSA driver. Make sure the User object that the driver uses to authenticate with is not used for any other purpose.

The created credentials will be used while configuring the driver in Section 4.1.2, “Installing the Driver Packages,” on page 20.

1. Log in to the RSA Security Console with an account that has SuperAdminRole rights.
2. From the *Identity* menu, select *Users* > *Manage Existing*.
3. Select *Add New*.
4. Fill out the user information, then click *Save*.
5. From the *Administration* menu, select *Administrative Roles* > *Manage Existing*.
6. Select the *SuperAdminRole*, then click *Assign More*.
7. Search for the user you created for the service account.
8. Select the user, then click *Assign to Role*.

3.2 Creating an RSA Authentication Manager 6.1 User Object with Administrator Rights

You need to create an RSA Authentication Manager user that matches the RSA Authentication Manager Windows service account. Make sure the User object that the driver uses to authenticate with is not used for any other purpose.

1. On the RSA Authentication Manager server, open the Services tool found in the Administrative Tools section of the Windows Control Panel.
2. Select the *RSA Auth Mgr Daemon* service, then click *Action* > *Properties*.
3. Click the *Log On* tab.

4. Typically the service is set to log on as the Local System account. If the service is configured to use an account other than the Local System account, take note of the login used.
5. Exit the service properties and Services dialog box.
6. Start the RSA Authentication Manager Administration tool.
7. Click *User* > *Add User*.
8. Specify the First Name, Last Name, and Default Login, then click *OK*.

   If the service is using the Local System account for its service account, the Default Login should be set to SYSTEM. Otherwise, use the login noted in Step 4

   For example, First Name - Local, Last Name - System, Default Login - SYSTEM.
9. Click *User* > *Edit User*.
10. Select the *Default Login* field and deselect the *Last Name* field.
11. Specify the service account login in the *Default Login* field, then click *OK*.

    For example, SYSTEM.
12. In the Edit User dialog box, select *Administrative Role*, then click *OK*.
13. Click *OK* to exit the Edit User dialog box.

Creating a New Driver

4

After the RSA driver files are installed on the server where you want to run the driver (see Chapter 2, “Installing the Driver Files,” on page 11), you can create the driver in the Identity Vault. You do so by importing the driver packages and then modifying the driver configuration to suit your environment.

4.1 Creating the Driver in Designer

You create the RSA driver by installing the driver packages and then modifying the configuration to suit your environment. After you create and configure the driver, you need to deploy it to the Identity Vault and start it.

4.1.1 Importing the Current Driver Packages

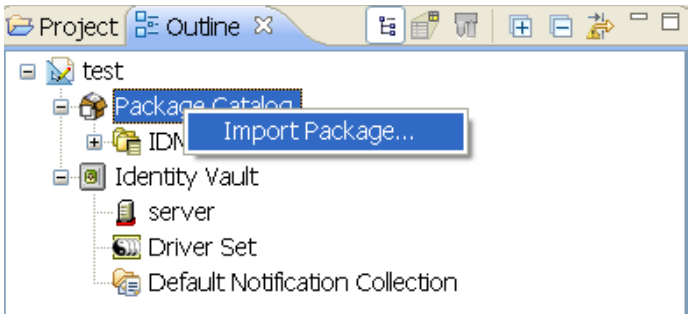
The driver packages contain the items required to create a driver, such as policies, entitlements, filters, and Schema Mapping policies. These packages are only available in Designer and can be updated after they are initially installed. You must have the most current version of the packages in the Package Catalog before you can create a new driver object.

To verify that you have the most recent version of the driver packages in the Package Catalog:

1. Open Designer.
2. In the toolbar, click *Help* > *Check for Package Updates*.
3. Click *OK* to update the packages

   or

   Click *OK* if the packages are up-to-date.
4. In the Outline view, right-click the Package Catalog.
5. Click *Import Package*.



6 Select any RSA driver packages

or

Click *Select All* to import all of the packages displayed.

By default, only the base packages are displayed. Deselect *Show Base Packages Only* to display all packages.

7 Click *OK* to import the selected packages, then click *OK* in the successfully imported packages message.

8 After the current packages are imported, continue with Section 4.1.2, “Installing the Driver Packages,” on page 20.

4.1.2 Installing the Driver Packages

After you have imported the current driver packages into the Package Catalog, you can install the driver packages to create a new driver.

1 In Designer, open your project.

2 In the Modeler, right-click the driver set where you want to create the driver, then click *New* > *Driver*.

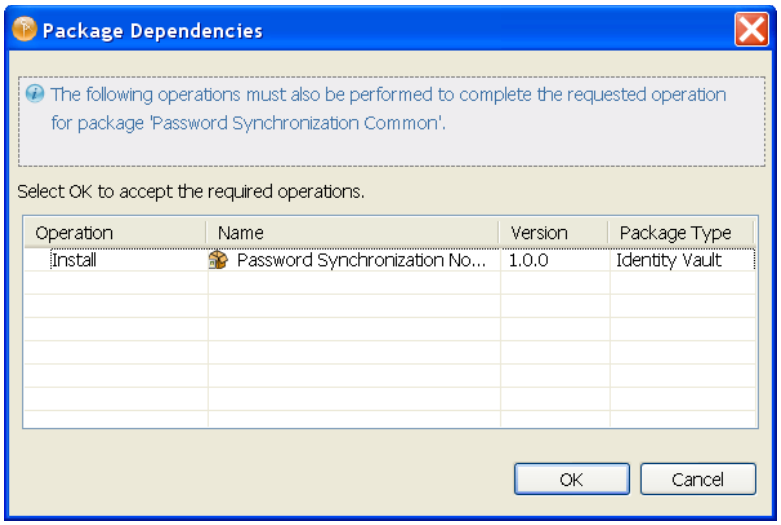
3 Select *RSA Base*, then click *Next*.

4 Select the default configuration for the RSA driver.

This package contains the default configuration information for the RSA driver. Always leave this option selected.

5 Click *Next*.

6 (Conditional) If there are package dependencies for the packages you selected to install, you must install them to install the selected package. Click *OK* to install the package dependencies that are listed.



7 (Conditional) If more than one type of package dependency must be installed, you are presented with these packages separately. Continue to click *OK* to install any additional package dependencies.

8 Click *Next*.

9 On the Driver Information page, specify a name for the driver, then click *Next*.

10 On the Application Authentication page, fill in the following fields:

Authentication ID: Specify the username for the RSA user created for the driver if the driver is connecting to RSA 7.1.This is the user created in Section 3.1, “Creating an RSA Authentication Manager 7.1 User Object with SuperAdminRole Rights,” on page 17. Leave this field blank for RSA 6.1.

Connection Information: Specify the connection information for the driver to connect to the RSA 7.1 server. Leave this field blank for RSA 6.1.

Password: Specify the password for the RSA user created for the driver if the driver is connecting to RSA 7.1. This is the password created in Section 3.1, “Creating an RSA Authentication Manager 7.1 User Object with SuperAdminRole Rights,” on page 17. Leave this field blank for RSA 6.1.

11 Click *Next*.

12 Fill in the following fields for Remote Loader information:

Connect To Remote Loader: Select *Yes* or *No* to determine if the driver will use the Remote Loader. For more information, see the *Identity Manager 4.0 Remote Loader Guide*.

If you select *No*, skip to Step 13. If you select *Yes*, use the following information to complete the configuration of the Remote Loader.

Host Name: Specify the IP address or DNS name of the server where the Remote Loader is installed and running.

Port: Specify the port number for this driver. Each driver connects to the Remote Loader on a separate port. The default value is 8090.

Remote Loader Password: Specify a password to control access to the Remote Loader. It must be the same password that is specified as the Remote Loader password on the Remote Loader.

Driver Password: Specify a password for the driver to authenticate to the Metadirectory server. It must be the same password that is specified as the Driver Object Password on the Remote Loader.

13 Click *Next*.

14 Review the summary of tasks that will be completed to create the driver, then click *Finish*.

15 After you have installed the driver, you must change the configuration for your environment. Proceed to Section 4.1.3, “Configuring the Driver,” on page 22.

4.1.3 Configuring the Driver

After importing the driver configuration file, you need to configure the driver before it can run. You should complete the following tasks to configure the driver:

- **Configure the driver parameters:** There are many settings that can help you customize and optimize the driver. The settings are divided into categories such as Driver Configuration, Engine Control Values, and Global Configuration Values (GCVs). Although it is important for you to understand all of the settings, your first priority should be to review the Driver Parameters located on the Driver Configuration page. The Driver Parameters let you configure the RSA API version and API version specific attributes. You can also configure the publisher options through the Driver Parameters.
- **Configure the driver filter:** Modify the driver filter to include the object classes and attributes you want synchronized between the Identity Vault and RSA Authentication Manager. For instructions, see Chapter 6, “Synchronizing Data,” on page 27.
- **Configure policies:** Modify the policies as needed. For information about the default configuration policies, see “Policies” on page 8.

After completing the configuration tasks, continue with the next section, Section 4.1.4, “Deploying the Driver,” on page 22.

4.1.4 Deploying the Driver

After a driver is created in Designer, it must be deployed into the Identity Vault.

1 In Designer, open your project.

2 In the Modeler, right-click the driver icon or the driver line, then select *Live* > *Deploy*.

3 If you are authenticated to the Identity Vault, skip to Step 5; otherwise, specify the following information:

Host: Specify the IP address or DNS name of the server hosting the Identity Vault.

Username: Specify the DN of the user object used to authenticate to the Identity Vault.

Password: Specify the user’s password.

4 Click *OK*.

5 Read through the deployment summary, then click *Deploy*.

6 Read the successful message, then click *OK*.

7 Click *Define Security Equivalence* to assign rights to the driver.

The driver requires rights to objects within the Identity Vault. The Admin user object is most often used to supply these rights. However, you might want to create a DriversUser (for example) and assign security equivalence to that user. Whatever rights that the driver needs to have on the server, the DriversUser object must have the same security rights.

7a Click *Add*, then browse to and select the object with the correct rights.

7b Click *OK* twice.

8 Click *Exclude Administrative Roles* to exclude users that should not be synchronized.

You should exclude any administrative User objects (for example, Admin and DriversUser) from synchronization.

8a Click *Add*, then browse to and select the user object you want to exclude.

8b Click *OK*.

8c Repeat Step 8a and Step 8b for each object you want to exclude.

8d Click *OK*.

9 Click *OK*.

4.1.5 Starting the Driver

When a driver is created, it is stopped by default. To make the driver work, you must start the driver and cause events to occur. Identity Manager is an event-driven system, so after the driver is started, it won't do anything until an event occurs.

To start the driver:

1 In Designer, open your project.

2 In the Modeler, right-click the driver icon or the driver line, then select *Live* > *Start Driver*.

For information about management tasks with the driver, see Chapter 5, "Managing the Driver," on page 25.

4.2 Creating the Driver in iManager

Drivers are created with packages, and iManager does not support packages. In order to create or modify drivers, you must use Designer. See Section 4.1, "Creating the Driver in Designer," on page 19.

4.3 Activating the Driver

If you created the driver in a driver set where you have already activated the RSA driver, the driver inherits the activation. If you created the driver in a driver set that has not had the RSA Driver activated, you must activate the driver within 90 days. Otherwise, the driver stops working.

For information on activation, refer to "Activating Novell Identity Manager Products" in the *Identity Manager 4.0 Integrated Installation Guide*.

Managing the Driver

5

As you work with the RSA driver, there are a variety of management tasks you might need to perform, including the following:

- Starting, stopping, and restarting the driver
- Viewing driver version information
- Using Named Passwords to securely store passwords associated with the driver
- Monitoring the driver's health status
- Backing up the driver
- Inspecting the driver's cache files
- Viewing the driver's statistics
- Using the DirXML Command Line utility to perform management tasks through scripts
- Securing the driver and its information
- Synchronizing objects
- Migrating and resynchronizing data
- Activating the driver

Because these tasks, as well as several others, are common to all Identity Manager drivers, they are included in one reference, the *Identity Manager 4.0 Common Driver Administration Guide*.

Synchronizing Data

6

The following sections provide information to help you control which classes and attributes are synchronized between your Identity Vault and the connected RSA Authentication Manager server. Not only can you choose which classes and attributes are synchronized, but you can also determine which direction they flow (Identity Vault to RSA, RSA to Identity Vault, or both).

6.1 Determining Which Objects Are Synchronized

Identity Manager uses the driver filter, located on both the Publisher and Subscriber channels, to control which objects are synchronized and to define the authoritative data source for these objects.

The following steps provide instructions for editing the filter in iManager. For information about editing the filter in Designer, see “Controlling the Flow of Objects with the Filter” in the *Policies in Designer 4.0* guide.

1. In iManager, open the RSA driver Overview page:
   - **1a** Click  to display the Identity Manager Administration page.
   - **1b** In the *Administration* list, click *Identity Manager Overview*.
   - **1c** If the driver set is not listed on the *Driver Sets* tab, use the *Search In* field to search for and display the driver set.
   - **1d** Click the driver set to open the Driver Set Overview page.
   - **1e** Click the RSA driver icon to display its Overview page.
2. Click the Publisher or Subscriber filter icon and make the appropriate changes.

   For every object and attribute selected in the filter, the Schema Mapping policy must have a corresponding entry unless the class or attribute names are the same in both directories (see Section 6.2, “Defining Schema Mapping,” on page 27). Before mapping an attribute, verify that a corresponding attribute actually exists in the target directory.

6.2 Defining Schema Mapping

When the driver is first started, it queries the server for the specific schema.

To define the schema mapping, you must be familiar with the characteristics of directory attributes and the RSA Authentication Manager attributes.

When you map attributes, follow these guidelines:

- Verify that every class and attribute specified in the Subscriber and Publisher policies is mapped in the Mapping policy unless the class or attribute names are the same in both directories.
- Before mapping a directory attribute to an RSA Authentication Manager attribute, verify that an RSA Authentication manager attribute actually exists. For example, the Full Name attribute is defined for a User object on an Identity Vault, but there is no equivalent attribute in RSA Authentication Manager.

The driver doesn't provide data conversion between different attribute types or conversions from multivalue to single-value attributes. The driver also doesn't understand structured attributes.

The following steps provide instructions for modifying the Schema Mapping Policy in iManager. For information about using Designer, see "Defining Schema Map Policies" in the *Policies in Designer 4.0* guide.

1. In iManager, open the RSA driver Overview page:
   - **1a** Click  to display the Identity Manager Administration page.
   - **1b** In the *Administration* list, click *Identity Manager Overview*.
   - **1c** If the driver set is not listed on the *Driver Sets* tab, use the *Search In* field to search for and display the driver set.
   - **1d** Click the driver set to open the Driver Set Overview page.
   - **1e** Click the RSA driver icon to display its Overview page.
2. Click the schema mapping icon on the Publisher or Subscriber channel.
3. Click the policy to display the editing page.
4. Edit the policy as appropriate for your setup.

6.3 Migrating and Resynchronizing Data

Identity Manager synchronizes data as the data changes. If you want to synchronize all data immediately, you can choose from the following options:

- **Migrate Data from the Identity Vault:** Allows you to select containers or objects you want to migrate from an Identity Vault to an RSA server. When you migrate an object, the Metadirectory engine applies all of the Matching, Placement, and Create policies, as well as the Subscriber filter, to the object.
- **Migrate Data into the Identity Vault:** Allows you to define the criteria that Identity Manager uses to migrate objects from an RSA Authentication Manager server into an Identity Vault. When you migrate an object, the Metadirectory engine applies all of the Matching, Placement, and Create policies, as well as the Publisher filter, to the object. Objects are migrated into the Identity Vault by using the order you specify in the Class list.
- **Synchronize:** Identity Manager looks in the Subscriber class filter and processes all objects for those classes. Associated objects are merged. Unassociated objects are processed as Add events.

1. In iManager, open the RSA driver Overview page:
   - **1a** Click  to display the Identity Manager Administration page.

1b In the *Administration* list, click *Identity Manager Overview*.

1c If the driver set is not listed on the *Driver Sets* tab, use the *Search In* field to search for and display the driver set.

1d Click the driver set to open the Driver Set Overview page.

1e Click the RSA driver icon to display its Overview page.

2 Click *Migrate*, then click the appropriate migration button.

Troubleshooting 7

This section describes common issues for driver configuration and provides information for resolving these issues.

7.1 Troubleshooting Driver Processes

Viewing driver processes is necessary to analyze unexpected behavior. To view the driver processing events, use DSTrace. You should only use it during testing and troubleshooting the driver. Running DSTrace while the drivers are in production increases the utilization on the Identity Manager server and can cause events to process very slowly. For more information, see “Viewing Identity Manager Processes” in the *Identity Manager 4.0 Common Driver Administration Guide*.

7.2 OutOfMemoryError

If the RSA driver shuts down with a java.lang.OutOfMemoryError:

1. Try setting or increasing the DHOST_JVM_INITIAL_HEAP and *DHOST_JVM_MAX_HEAP* environment variables.
2. Restart the driver.
3. Monitor the driver to make sure that the variables provide enough memory.

For more information, see “Configuring Java Environment Parameters” in the *Identity Manager 4.0 Common Driver Administration Guide*.

Driver Properties

A

This section provides information about the Driver Configuration and Global Configuration Values properties for the RSA driver. These are the only unique properties for drivers. All other driver properties (Named Password, Engine Control Values, Log Level, and so forth) are common to all drivers. Refer to "Driver Properties" in the *Identity Manager 4.0 Common Driver Administration Guide* for information about the common properties.

The information is organized according to tabs that display in iManager. If a field is different in Designer, it is marked with a Designer icon.

A.1 Driver Configuration

In iManager:

1. Click to display the Identity Manager Administration page.
2. Open the driver set that contains the driver whose properties you want to edit:
   - **2a** In the *Administration* list, click *Identity Manager Overview*.
   - **2b** If the driver set is not listed on the *Driver Sets* tab, use the *Search In* field to search for and display the driver set.
   - **2c** Click the driver set to open the Driver Set Overview page.
3. Locate the driver icon, then click the upper right corner of the driver icon to display the *Actions* menu.
4. Click *Edit Properties* to display the driver's properties page.

   By default, the Driver Configuration page is displayed.

In Designer:

1. Open a project in the Modeler.
2. Right-click the driver icon or line, then select click *Properties* > *Driver Configuration.*

The Driver Configuration options are divided into the following sections:

A.1.1 Driver Module

The driver module changes the driver from running locally to running remotely or the reverse.

Java: Used to specify the name of the Java class that is instantiated for the shim component of the driver. This class can be located in the `classes` directory as a class file, or in the `lib` directory as a `.jar` file. If this option is selected, the driver is running locally.

The name of the Java class is `com.trivir.idm.driver.ace.AceDriverShim`.

Native: This option is not used with the driver.

Connect to Remote Loader: Used when the driver is connecting remotely to the connected system. Designer includes two suboptions:

- **Remote Loader Configuration for Documentation:** Includes information on the Remote Loader client configuration when Designer generates documentation for the driver.
- **Driver Object Password:** Specifies a password for the Driver object. If you are using the Remote Loader, you must enter a password on this page. Otherwise, the remote driver does not run. The Remote Loader uses this password to authenticate itself to the remote driver shim.

A.1.2 Driver Object Password (iManager Only)

Driver Object Password: Use this option to set a password for the driver object. If you are using the Remote Loader, you must enter a password on this page. Otherwise, the remote driver does not run. The Remote Loader uses this password to authenticate itself to the remote driver shim.

A.1.3 Authentication

The Authentication section stores the information required to authenticate to the connected system.

Authentication information for server: Displays or specifies the IP address or server name that the driver is associated with

Authentication ID: Specifies the RSA Authentication Manager 7.1 administrative user that the driver will use for authentication. For example, `rsadriver`. This is the user created in Section 3.1, “Creating an RSA Authentication Manager 7.1 User Object with SuperAdminRole Rights,” on page 17. This field should be left blank for RSA Authentication Manager 6.1

Authentication Context: Specify the IP address or name of the RSA server.

Remote Loader Connection Parameter: Used only if the driver is connecting to the application through the Remote Loader. The parameter to enter is `hostname=xxx.xxx.xxx.xxx port=xxxx kmo=certificatename`, when the hostname is the IP address of the application server running the Remote Loader server and the port is the port the Remote Loader is listening on. The default port for the Remote Loader is 8090.

The `kmo` entry is optional. It is used only when an SSL connection exists between the Remote Loader and the Metadirectory engine.

Example: `hostname=10.0.0.1 port=8090 kmo=IDMCertificate`.

Application Password: Specify the password for the user object listed in the *Authentication ID* field. This is the password created in Section 3.1, “Creating an RSA Authentication Manager 7.1 User Object with SuperAdminRole Rights,” on page 17. This field should be left blank for RSA Authentication Manager 6.1.

Remote Loader Password: Used only if the driver is connecting to the application through the Remote Loader. The password is used to control access to the Remote Loader instance. It must be the same password specified during the configuration of the Remote Loader on the connected system.

Cache limit (KB): Specify the maximum event cache file size (in KB). If it is set to zero, the file size is unlimited. Click *Unlimited* to set the file size to Unlimited in Designer.

A.1.4 Startup Option

The Startup Option section allows you to set the driver state when the Identity Manager server is started.

Auto start: The driver starts every time the Identity Manager server is started.

Manual: The driver does not start when the Identity Manager server is started. The driver must be started through Designer or iManager.

Disabled: The driver has a cache file that stores all of the events. When the driver is set to *Disabled*, this file is deleted and no new events are stored in the file until the driver state is changed to *Manual* or *Auto Start*.

Do not automatically synchronize the driver: This option applies only if the driver is deployed and was previously disabled. If this option is not selected, the driver re-synchronizes the next time it is started.

A.1.5 Driver Parameters

The Driver Parameters section lets you configure the driver-specific parameters. When you change driver parameters, you tune driver behavior to align with your network environment. The parameters are divided into different categories:

- “Driver Options” on page 35
- “Subscriber Options” on page 36
- “Publisher Options” on page 36

Driver Options

RSA API Version: When you are connecting to RSA Authentication Manager 7.1, choose 7.1. When you are connecting to RSA Authentication Manager 6.1, choose 6.1.

RSA Command Client User (7.1): Specify the command client user for your RSA 7.1 installation. This information was gathered in “Obtaining the Command Client Username and Password” on page 14.

RSA Command Client Password (7.1): Specify the command client password for your RSA 7.1 installation. This information was gathered in “Obtaining the Command Client Username and Password” on page 14

RSA Realm (7.1): Specify the RSA realm containing the driver user specified in the Authentication ID.

Weblogic Library Directory (7.1): Specify the location of the RSA/Weblogic `.jar` files that were copied during “Copying RSA Files” on page 12.

RSA Keystore File (7.1): Specify the location of the keystore created during “Exporting the Root Certificate” on page 14.

Subscriber Options

The RSA driver does not currently have Subscriber Options.

Publisher Options

Disable Publisher: Specify whether the publisher polls RSA Authentication Manager for changes.

Polling Interval in Minutes: Specify the interval at which the driver checks RSA Authentication Manager for changes. When new changes are found, they are applied to the Identity Vault.

Heartbeat Interval in Minutes: Specify how many minutes of inactivity should elapse before this channel sends a heartbeat document. In practice, more than the number of minutes specified can elapse. That is, this parameter defines a lower bound.

A.1.6 ECMAScript

This section displays an ordered list of ECMAScript resource files. The files contain extension functions for the driver that Identity Manager loads when the driver starts. You can add additional files, remove existing files, or change the order the files are executed.

A.1.7 Global Configuration

This section displays an ordered list of Global Configuration objects. The objects contain extension GCV definitions for the driver that Identity Manager loads when the driver is started. You can add or remove the Global Configuration objects, and you can change the order in which the objects are executed.

A.2 Global Configuration Values

Global configuration values (GCVs) are values that can be used by the driver to control functionality. GCVs are defined on the driver or on the driver set. Driver set GCVs can be used by all drivers in the driver set. Driver GCVs can be used only by the driver on which they are defined.

The RSA driver does not currently ship with any GCVs. You can add your own if you discover you need additional values as you implement policies in the driver.

To access the driver’s GCVs in iManager:

1. Click  to display the Identity Manager Administration page.
2. Open the driver set that contains the driver whose properties you want to edit:
   2a. In the *Administration* list, click *Identity Manager Overview*.

2b If the driver set is not listed on the *Driver Sets* tab, use the *Search In* field to search for and display the driver set.

2c Click the driver set to open the Driver Set Overview page.

3 Locate the driver icon, click the upper right corner of the driver icon to display the *Actions* menu, then click *Edit Properties*.

or

To add a GCV to the driver set, click *Driver Set*, then click *Edit Driver Set properties*.

To access the driver's GCVs in Designer:

1 Open a project in the Modeler.

2 Right-click the driver icon or line, then select *Properties > Global Configuration Values.*

or

To add a GCV to the driver set, right-clickthe driver set icon , then click *Properties > GCVs*.

Trace Levels

B

The driver supports the following trace levels:

Level	Description
1	Minimal Tracing
2	Previous level and RSA API exceptions
3	Previous level and soft errors (unknown attribute, query errors)
4	Previous level and publisher event information.

For information about setting driver trace levels, see “Viewing Identity Manager Processes” in the *Identity Manager 4.0 Common Driver Administration Guide*.

RSA Object Schema

C

The RSA driver supports the following trace objects and attributes:

C.1 User Object

Unless otherwise stated, all time values are expressed as a ctime value - number of seconds elapsed since 00:00:00 on January 1, 1970 UTC.

The RSA User object supports the following attributes:

Attribute	Type	Description
UserNum	String	Internal ID for the user object (read-only)
DefaultLogin	String	User’s login ID
FirstName	String	User’s first name
LastName	String	User’s last name
TokenSerialNumber	String	Tokens assigned to user (multi-value)
MemberOf	String	Groups the user is a member of (multi-value)
DefaultShell	String	User’s default shell
ProfileName	String	Users RADIUS profile
TempUser	Boolean	Whether the user is a temporary user (TRUE/FALSE)
Start	Numeric	Time the account becomes active
End	Numeric	Time the account becomes inactive

C.2 Token Object

The RSA Token object supports the following attributes:

Attribute	Type	Description
SerialNum	String	Token serial number (read-only)
PIN	String	Token PIN
Disabled	Boolean	Token is disabled (TRUE/FALSE)
NewPINMode	Boolean	Token is in new PIN mode state (TRUE/FALSE)
PINClear	Boolean	Token has been cleared (TRUE/FALSE) (read-only)
NumDigits	String	Number of digits in token display (read-only)

Attribute	Type	Description
Interval	String	Number of seconds between display changes (read-only)
Birth	Numeric	Time the token was activated (read-only)
Death	Numeric	Time when the token will shut down (read-only)
LastLogin	Numeric	Time of the last login with this token (read-only)
Type	Numeric	Token type (read-only): 0 - RSA SecurID Standard Card 1 - RSA SecurID PINPad 2 - RSA SecurID Key Fob 4 - RSA SecurID Software Token 6 - RSA SecurID Modem
Hex	Boolean	Whether the display is hexadecimal (TRUE/FALSE)
Assigned	Boolean	Whether the token is assigned (TRUE/FALSE)
UserNum	String	Internal ID of the user to whom the token is assigned (read-only)
EmergencyAccess	String	Whether the token is enabled for emergency access (TRUE/FALSE)
BadTokenCodes	String	Number of bad token codes entered (read-only)
PINChangedDate	String	Time the PIN was last changed (read-only)
DisabledDate	Numeric	Time the token disabled state was changed
CountsLastModified	Numeric	Time the token counts were last modified
Protected	Boolean	Whether the software token was copy-protected on last deployment (TRUE/FALSE)
Deployed	Boolean	Whether the software token is currently deployed (TRUE/FALSE)
Count	String	Number of times the token has been deployed (read-only)
SoftPassword	String	Password stored in the software token (read-only)
KeyPad	Boolean	Whether the token has a keypad (read-only)
LocalPIN	Boolean	Whether the pin is stored locally on user’s computer (read-only)
Version	String	Token’s algorithm version (read-only)
FormFactor	String	Bitmask representing the form factor of the token (read-only)
PINType	Numeric	The PIN type for the token (read-only): 0-Token expects both a PIN and a token code 1-PIN only

Attribute	Type	Description
Assignment	Numeric	Time the token was assigned (read-only)
FirstLogin	Boolean	Whether the user has successfully authenticated (read-only)
EACExpires	Numeric	Time the assigned emergency token code expires
EACPasscode	String	Assigned emergency token code (read-only)