**Driver for RSA**

**Implementation Guide**

**Identity Manager 4.0.2**

**August 2013**



**Legal Notice**

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON‐DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON‐DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ʺAS ISʺ WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material (ʺModuleʺ) is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non‐disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202‐4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non‐DOD acquisitions), the government’s rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

**© 2013 NetIQ Corporation and its affiliates. All Rights Reserved.**

For information about NetIQ trademarks, see <https://www.netiq.com/company/legal/>.

**Contents**

**About this Book and the Library 5**

**About NetIQ Corporation 7**

**1 Understanding the RSA Driver 9**

1.1 Supported Software Versions . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 9

1.2 RSA Driver Concepts . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 9

1.2.1 Synchronizing Data . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 9

1.2.2 How the RSA Driver Works . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 10

1.3 Support for Standard Driver Features . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 11

1.3.1 Local and Remote Platforms . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 11

1.3.2 Entitlements . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 11

**2 Installing the Driver Files 13**

2.1 Installing the Driver Files . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 13

2.2 Copying Required Files and Information from RSA Authentication Manager 7.1 . . . . . . . . . . . . . . . 13

2.2.1 Copying RSA Files . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 14

2.2.2 Exporting Root Certificate . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 15

2.2.3 Obtaining the Command Client Username and Password . . . . . . . . . . . . . . . . . . . . . . . . . 15

2.2.4 Setting IDM Java Startup Properties for RSA Authentication Manager 7.1 . . . . . . . . . . . . . 16

**3 Preparing RSA Authentication Manager 17**

3.1 Creating an RSA Authentication Manager 7.1 User Object with SuperAdminRole Rights. . . . . . . . . 17

3.2 Creating an RSA Authentication Manager 6.1 User Object with Administrator Rights. . . . . . . . . . . . 18

**4 Creating a New Driver 19**

|  |  |  |
| --- | --- | --- |
| 4.1 | Creatin  4.1.1 | g the Driver in Designer . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 19  Importing the Current Driver Packages . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 19 |
|  | 4.1.2 | Installing the Driver Packages . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 20 |
|  | 4.1.3 | Configuring the Driver . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 22 |
|  | 4.1.4 | Deploying the Driver . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 22 |
|  | 4.1.5 | Starting the Driver . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 23 |

4.2 Creating the Driver in iManager . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 23

4.3 Activating the Driver . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 23

**5 Managing the Driver 25**

**6 Synchronizing Data 27**

6.1 Determining Which Objects Are Synchronized . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 27

6.2 Defining Schema Mapping . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 27

6.3 Migrating and Resynchronizing Data . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 28

**7 Troubleshooting 31**

7.1 Troubleshooting Driver Processes . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 31

7.2 OutOfMemoryError. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 31

7.3 Invalid Command Client Credentials . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 31

7.4 Invalid Client Credentials . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 32

7.5 Hostname or IP Does Not Match Trust Chain in Certificate . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 32

7.6 ArraySyntax Environment Variable Not Set . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 33

7.7 Dependency Missing . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 33

**A Driver Properties 35**

A.1 Driver Configuration . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 35

A.1.1 Driver Module . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 36

A.1.2 Driver Object Password (iManager Only) . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 36

A.1.3 Authentication . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 36

A.1.4 Startup Option . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 37

A.1.5 Driver Parameters . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 37

A.1.6 ECMAScript . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 38

A.1.7 Global Configuration . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 38

A.2 Global Configuration Values . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 38

**B Trace Levels 41**

**C RSA Object Schema 43**

C.1 User Object . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 43

C.2 Token Object . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 43

**About this Book and the Library**

The *Driver for RSA Implementation Guide* provides information about how to install, configure, and manage the Identity Manager Driver for RSA.

**Intended Audience**

The book provides information for individuals responsible for understanding how to install, configure, and manage the Identity Manager Driver for RSA.

**Other Information in the Library**

The library provides the following information resources:

**Installation Guide**

Provides detailed planning and installation information.

**Help**

Provides context‐sensitive information and step‐by‐step guidance for common tasks, as well as definitions for each field on each window.

**About NetIQ Corporation**

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

**Our Viewpoint**

**Adapting to change and managing complexity and risk are nothing new**

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

**Enabling critical business services, better and faster**

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

**Our Philosophy**

**Selling intelligent solutions, not just software**

In order to provide reliable control, we first make sure we understand the real‐world scenarios in which IT organizations like yours operate — day in and day out. Thatʹs the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And thatʹs so much more rewarding than simply selling software.

**Driving your success is our passion**

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post‐deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

**Our Solutions**

 Identity & Access Governance

 Access Management

 Security Management

 Systems & Application Management

 Workload Management

 Service Management

**Contacting Sales Support**

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

**Worldwide:** [www.netiq.com/about\_netiq/officelocations.asp](http://www.netiq.com/about_netiq/officelocations.asp)

**United States and Canada:** 1-888-323-6768

**Email:** [info@netiq.com](mailto:info@netiq.com)

**Web Site:** [www.netiq.com](http://www.netiq.com/)

**Contacting Technical Support**

For specific product issues, contact our Technical Support team.

**Worldwide:** [www.netiq.com/support/contactinfo.asp](http://www.netiq.com/support/contactinfo.asp)

**North and South America:** 1-713-418-5555

**Europe, Middle East, and Africa:** +353 (0) 91-782 677

**Email:** [support@netiq.com](mailto:support@netiq.com)

**Web Site:** [www.netiq.com/support](http://www.netiq.com/support)

**Contacting Documentation Support**

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at [www.netiq.com/documentation](http://www.netiq.com/documentation). You can also email [Documentation‐ Feedback@netiq.com](mailto:Documentation-Feedback@netiq.com). We value your input and look forward to hearing from you.

**Contacting the Online User Community**

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit [http:// community.netiq.com](http://community.netiq.com/).

1 1**Understanding the RSA Driver**

The Identity Manager Driver for RSA 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.

 Section 1.1, “Supported Software Versions,” on page 9

 Section 1.2, “RSA Driver Concepts,” on page 9

 Section 1.3, “Support for Standard Driver Features,” on page 11

**1.1 Supported Software Versions**

The following RSA Authentication Manager versions are supported:

 7.1

 8.1

The following Novell Identity Manager versions are supported:

 4.0.1

 4.0.2

 4.5

**1.2 RSA Driver Concepts**

 Section 1.2.1, “Synchronizing Data,” on page 9

 Section 1.2.2, “How the RSA Driver Works,” on page 10

**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” on page 10

 “Filters” on page 10

 “Policies” on page 10

**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 2 seconds, 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.

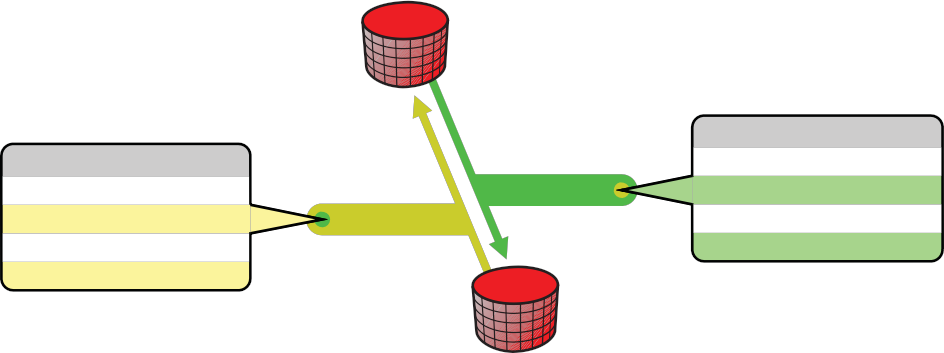
Due to a limitation in the RSA change notification subsystem, user object modifications in LDAP Identity Sources will not generate publisher add/modification events. Some operations in the RSA Security Console (e.g. token assignment) will still trigger publisher events for LDAP Identity Sources.The RSA Identity Source may be configured as described in Section A.1.5, “Driver Parameters,” on page 37.

**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*

RSA Authentication Manager



User

CN

Given Name Surname accessCardNumber

Subscriber

Publisher

User DefaultLogin FirstName LastName TokenSerialNumber

Identity Vault

**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.

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 11

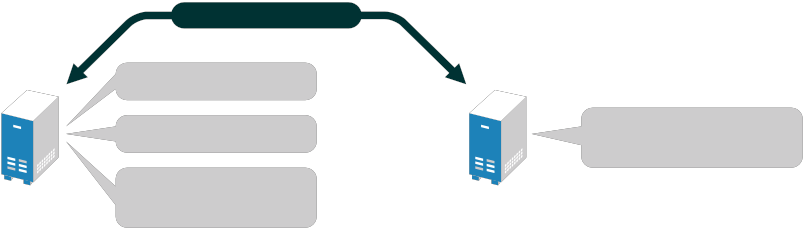
 Section 1.3.2, “Entitlements,” on page 11

**1.3.1 Local and Remote Platforms**

You can install the RSA driver locally or remotely.

A local configuration is when the RSA driver is installed on the same computer with an Identity Vault and the Metadirectory engine. A remote configuration is when the RSA driver is installed along with a remote loader on a computer without an Identity Vault and Metadirectory engine. The following figure illustrates a local configuration:

***Figure 1-2*** *A Local Configuration*



Synchronization

(any Identity

Identity Vault

Identity Manager

Identity Manager

Driver for RSA

(an RSA 7.1/8.1

RSA Authentication

Manager

Vault platform)

Authentication Manager server)

RSA Authentication Manager v7.1 supports both a local and remote configuration. The remote loader can be installed on the RSA Authentication Manager server.

RSA Authentication Manager v8.1 is provided as an appliance and does not support a remote configuration where the remote loader is installed on the Authentication Manager server. Consequently, the RSA driver may be installed with a local configuration or if a remote configuration is required, the remote loader must be installed on a computer other than the RSA Authentication Manager server.

See “[System Requirements](https://www.netiq.com/documentation/idm402/pdfdoc/idm_integrated_install/idm_integrated_install.pdf#bpo8wc2)” in the [*Identity Manager 4.0.2 Integrated Installation Guide*](https://www.netiq.com/documentation/idm402/pdfdoc/idm_integrated_install/idm_integrated_install.pdf#Front) 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 4.0.2 Entitlements Guide*](https://www.netiq.com/documentation/idm402/pdfdoc/idm_entitlements/idm_entitlements.pdf#bookinfo).

2 2**Installing the Driver Files**

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

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:

 Section 2.1, “Installing the Driver Files,” on page 13

 Section 2.2, “Copying Required Files and Information from RSA Authentication Manager,”

on page 13

**2.1 Installing the Driver Files**

The RSA driver files should be installed as follows, based on the chosen configuration:

Metadirectory Server

-Copy the jace.jar and ACEShim.jar to the following directory on your IDM server

--Windows: \Novell\NDS\lib

--Linux: /opt/novell/eDirectory/lib/dirxml/classes

---Set privileges on the jar files to 755

Remote Loader

-Copy the jace.jar and ACEShim.jar to the following directory on your Remote Loader server

--Windows: \novell\RemoteLoader\lib

--Linux: /opt/novell/eDirectory/lib/dirxml/classes

---Set privileges on the jar files to 755

**2.2 Copying Required Files and Information from RSA Authentication Manager**

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. The RSA Authentication Manager files must be copied to the appropriate Identity Manager driver library directory for your installation. The default locations are as follows:

Windows: \Novell\NDS\lib

Linux/Unix: /opt/novell/eDirectory/lib/dirxml/classes

**2.2.1.1 Copying RSA Authentication Manager 7.1 Files**

To copy the files:

**1** From a command prompt on your RSA Authentication Manager host, change directories to

RSA\_AM\_HOME/appserver/weblogic/server/lib/.

**2** Type:

../../../jdk/bin/java -jar ../../../modules/

com.bea.core.jarbuilder\_1.0.0.0.jar -profile wlfullclient

**3** Change directories to RSA\_AM\_HOME/

**4** Type:

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

**5** Type:

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

**2.2.1.2 Copying RSA Authentication Manager 8.1 Files**

Copy the following files from the sdk directory of the RSA Authentication Manager 8.1 installation media to the Identity Manager driver library.

am-client.jar

commons-beanutils.jar

commons-logging.jar

iScreen.jar

log4j.jar

ognl.jar

spring-asm.jar

spring-beans.jar

spring-context.jar

spring-core.jar

spring-expression.jar

wlfullclient.jar

Copy the following public files from the appropriate project:

gson-2.2.4.jar - Google Code google-gson project

hibernate-3.2.2.jar - SourceForge Hibernate project

hsqldb.jar - SourceForge HyperSQL Database Engine project

**2.2.2 Exporting Root Certificate**

When you install RSA Authentication Manager, the system creates a self‐signed root certificate. You must export this certificate from the server, and import it into a Java keystore file for Identity Manager.

RSA 7.1

To export the server root certificate:

**1** Change directories to RSA\_AM\_HOME/appserver/.

**2** Export the root certificate by typing:

jdk/jre/bin/keytool -export -keystore RSA\_AM\_HOME/server/security/

*server\_name*.jks -file am\_root.cer -alias rsa\_am\_ca

**3** When prompted for the keystore password, press Enter without typing a password.

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

The Java keytool utility writes the certificate file to the directory defined in Step 1.

**4** Copy the am\_root.cer to the Identity Manager server.

**5** Import the certificate into the Identity Manager Java keystore by running the following command on the Identity Manager server:

/opt/novell/eDirectory/lib64/nds-modules/jre1.6.0\_31/bin/keytool -v -import -file am\_root.cer -alias RSA7 -keystore cacerts

**NOTE:** 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 utility displays a confirmation that the certificate was added to the keystore.

RSA 8.1

To export the server root certificate:

**1** Change directories to /opt/rsa/am/appserver/.

**2** Export the root certificate by typing:

jdk/bin/keytool -export -keystore /opt/rsa/am/server/security/trust.jks -file am\_root.cer -alias rsa-am-ca

**3** When prompted for the keystore password, press Enter without typing a password.

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

The Java Keytool utility writes the certificate file to the directory defined in Step 1.

**4** Copy the am\_root.cer to the Identity Manager server.

**5** Import the certificate into the Identity Manager Java keystore by running the following command on the Identity Manager server:

/opt/novell/eDirectory/lib64/nds-modules/jre1.6.0\_31/bin/keytool -v -import -file am\_root.cer -alias RSA8 -keystore cacerts

**NOTE:** 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 utility displays a confirmation that the certificate was added to the keystore.

**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 user name values in the driver configuration for connection to the command server. Use the Manage Secrets utility to obtain these values from Authentication Manager.

To obtain the command client user name and password from RSA Authentication Manager:

**1** From a command prompt on your RSA Authentication Manager host, change directories to

RSA\_AM\_HOME/utils (7.1) or /opt/rsa/am/utils (8.1).

**2** Type:

rsautil manage-secrets --action list

**3** When prompted, type the master password chosen during RSA Authentication Manager installation.

The system displays the list of your internal system passwords.

**4** In the list that is displayed, locate the values for your command client user name 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 37.

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

**2.2.4 Setting IDM Java Startup Properties for RSA Authentication Manager**

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

**2.2.4.1 RSA Authentication Manager 7.1**

**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, click **Edit**, and skip to Step 7. If it does not exist, continue with 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** on each dialog until they are closed.

**On Linux**

Set or modify the DHOST\_JVM\_OPTIONS environment variable to the following:

-Dsun.lang.ClassLoader.allowArraySyntax=true

**2.2.4.2 RSA Authentication Manager 8.1**

**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, click **Edit**, and skip to Step 7. If it does not exist, continue with 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

-Djavax.xml.parsers.DocumentBuilderFactory=com.sun.org.apache.xerces.internal.jaxp.DocumentBuilderFactoryImpl -Djavax.xml.parsers.SAXParserFactory=com.sun.org.apache.xerces.internal.jaxp.SAXParserFactoryImpl

**8** Click **OK** on each dialog until they are closed.

**On Linux**

Update the /opt/novell/eDirectory/sbin/pre\_ndsd script with the following:

DHOST\_JVM\_OPTIONS=”-Dsun.lang.ClassLoader.allowArraySyntax=true -Djavax.xml.parsers.DocumentBuilderFactory=com.sun.org.apache.xerces.internal.jaxp.DocumentBuilderFactoryImpl -Djavax.xml.parsers.SAXParserFactory=com.sun.org.apache.xerces.internal.jaxp.SAXParserFactoryImpl”

3 3**Preparing RSA Authentication Manager**

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.

You will 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** Login to the RSA Security Console with an account that has SuperAdminRole rights.

**2** From the Identity menu, select **Users** > **Manage Existing**.

**3** Choose **Add New**.

**4** Fill out the user information.

**5** Confirm that **Require user to change password at next logon** is unchecked.

**6** Click **Save**

**7** From the Administration menu, select **Administrative Roles** > **Manage Existing**.

**8** Select the **SuperAdminRole**, then click **Assign More**.

**9** Search for the user you created for the service account.

**10** Select the user, then click **Assign to Role**.

4 4**Creating a New Driver**

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 13), 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.

 Section 4.1, “Creating the Driver in Designer,” on page 19

 Section 4.2, “Creating the Driver in iManager,” on page 23

 Section 4.3, “Activating the Driver,” on page 23

**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.

 Section 4.1.1, “Importing the Current Driver Packages,” on page 19

 Section 4.1.2, “Installing the Driver Packages,” on page 20

 Section 4.1.3, “Configuring the Driver,” on page 22

 Section 4.1.4, “Deploying the Driver,” on page 22

 Section 4.1.5, “Starting the Driver,” on page 23

**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.

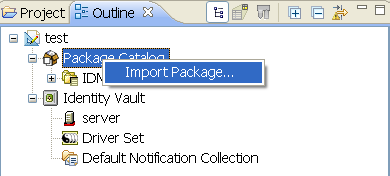
**2** In the toolbar, click **Help** > **Check for Package Updates**.

**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 package or

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

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**.

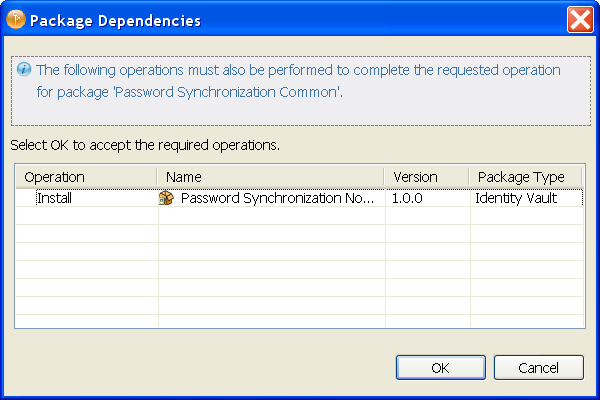
**3** Select **RSA Base**, then click **Next**.

**4** Select the default configuration for the RSA driver.

**NOTE:** 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.

**Connection Information:** Specify the connection information for the driver to connect to the RSA server. The connection information should be specified in the form t3s://*<ip or hostname>*:*<port>* (e.g. t3s://rsaserver.example.com:7002). The default port for an RSA Authentication Manager is 7002; for an RSA Authentication Manager Appliance, the default port is 7004.

**Password:** Specify the password for the RSA user created for the driver.

**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 4.0.2 Remote Loader Guide*](https://www.netiq.com/documentation/idm402/pdfdoc/idm_remoteloader/idm_remoteloader.pdf#bookinfo).

If you select **No**, continue with 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. 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 Section A.1.5, “Driver Parameters,” on page 37 located on the Driver Configuration page. The Driver Parameters let you configure the RSA API version and API version specific attributes. You may 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 10.

After completing the configuration tasks, continue with 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. If you do not activate the driver, at the end of the 90 day trial period, it will stop working.

For information on activation, refer to “[Activating Novell Identity Manager Products](https://www.netiq.com/documentation/idm402/pdfdoc/idm_integrated_install/idm_integrated_install.pdf#bpo948h)” in the [*Identity*](https://www.netiq.com/documentation/idm402/pdfdoc/idm_integrated_install/idm_integrated_install.pdf#Front)

[*Manager 4.0.2 Integrated Installation Guide*](https://www.netiq.com/documentation/idm402/pdfdoc/idm_integrated_install/idm_integrated_install.pdf#Front).

5 5**Managing the Driver**

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

These tasks as well as several others are common to all Identity Manager drivers, so they are all described in the [*Identity Manager 4.0.2 Common Driver Administration Guide*](https://www.netiq.com/documentation/idm402/pdfdoc/idm_common_driver/idm_common_driver.pdf#Front).

6 6**Synchronizing Data**

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).

 Section 6.1, “Determining Which Objects Are Synchronized,” on page 27

 Section 6.2, “Defining Schema Mapping,” on page 27

 Section 6.3, “Migrating and Resynchronizing Data,” on page 28

**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](https://www.netiq.com/documentation/idm402/pdfdoc/policy_designer/policy_designer.pdf#foverview)” in the [*Policies in Designer 4.0.2*](https://www.netiq.com/documentation/idm402/pdfdoc/policy_designer/policy_designer.pdf#bookinfo) 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.

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 doesnʹt 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](https://www.netiq.com/documentation/idm402/pdfdoc/policy_designer/policy_designer.pdf#smoverview)” in the [*Policies in Designer 4.0.2*](https://www.netiq.com/documentation/idm402/pdfdoc/policy_designer/policy_designer.pdf#bookinfo) 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.

7 7**Troubleshooting**

 Section 7.1, “Troubleshooting Driver Processes,” on page 31

 Section 7.2, “OutOfMemoryError,” on page 31

 Section 7.3, “Invalid Command Client Credentials,” on page 31

 Section 7.4, “Invalid Client Credentials,” on page 32

 Section 7.5, “Hostname or IP Does Not Match Trust Chain in Certificate,” on page 32

 Section 7.6, “ArraySyntax Environment Variable Not Set,” on page 33

 Section 7.7, “Dependency Missing,” on page 33

**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](https://www.netiq.com/documentation/idm402/pdfdoc/idm_common_driver/idm_common_driver.pdf#b1rc1vm)” in the [*Identity Manager 4.0.2 Common Driver Administration Guide*](https://www.netiq.com/documentation/idm402/pdfdoc/idm_common_driver/idm_common_driver.pdf#Front).

**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](https://www.netiq.com/documentation/idm402/pdfdoc/idm_common_driver/idm_common_driver.pdf#bg0n8f8)” in the [*Identity Manager 4.0.2*](https://www.netiq.com/documentation/idm402/pdfdoc/idm_common_driver/idm_common_driver.pdf#Front)

[*Common Driver Administration Guide*](https://www.netiq.com/documentation/idm402/pdfdoc/idm_common_driver/idm_common_driver.pdf#Front).

**7.3 Invalid Command Client Credentials**

The RSA driver may shut down during startup with the following error:

[04/23/13 14:16:27.990]:RSA ST: DirXML Log Event -------------------

Driver: \EXAMPLE\services\Driver Set\RSA Status: Fatal

Message: Code(-9005) The driver returned a "fatal" status indicating that the driver should be shut down. Detail from driver:

<description>com.trivir.ace.AceToolkitException: Instantiation of api class

failed.

java.lang.reflect.InvocationTargetException

com.rsa.common.SystemException: Failed to construct CommandTarget

javax.naming.AuthenticationException [Root exception is

java.lang.SecurityException: User: CmdClient\_dbfnwyrl, failed to be

authenticated.]

java.lang.SecurityException: User: CmdClient\_dbfnwyrl, failed to be authenticated.

If this occurs, confirm that the correct Command Client credentials have been entered as described in

Section 2.2.3, “Obtaining the Command Client Username and Password,” on page 15 and

Section A.1.5, “Driver Parameters,” on page 37.

**7.4 Invalid RSA Authentication Credentials**

The RSA driver may shut down during startup with the following error:

[04/23/13 15:23:45.326]:RSA ST: DirXML Log Event -------------------

Driver: \EXAMPLE\services\Driver Set\RSA Status: Fatal

Message: Code(-9005) The driver returned a "fatal" status indicating that the driver should be shut down. Detail from driver:

<description>com.trivir.ace.AceToolkitException: Instantiation of api class failed.

java.lang.reflect.InvocationTargetException

com.trivir.ace.AceToolkitException: Error creating connection factory. Access

Denied

com.rsa.authn.AuthenticationCommandException: Access Denied

If this occurs, confirm that the correct RSA credentials have been entered as described in Section 3.1, “Creating an RSA Authentication Manager 7.1 User Object with SuperAdminRole Rights,” on

page 17 and Section A.1.3, “Authentication,” on page 36.

**7.5 Hostname or IP Does Not Match Trust Chain in Certificate**

The RSA driver may shut down during startup with the following error:

[05/17/13 15:17:50.602]:RSA ST: DirXML Log Event -------------------

Driver: \RSA\services\Driver Set\RSA Status: Fatal

Message: Code(-9005) The driver returned a "fatal" status indicating that the driver should be shut down. Detail from driver:

<description>com.trivir.ace.AceToolkitException: Instantiation of api class

failed.

java.lang.reflect.InvocationTargetException

com.rsa.common.SystemException: Failed to construct CommandTarget

javax.naming.CommunicationException [Root exception is java.net.ConnectException:

t3s://172.17.2.101:7002: Destination unreachable; nested exception is:

javax.net.ssl.SSLKeyException: [Security:090504]Certificate chain received from

RSA-AM - 172.17.2.101 failed hostname verification check. Certificate contained

rsa-am.example.com but check expected RSA-AM; No available router to destination]

java.net.ConnectException: t3s://172.17.2.101:7002: Destination unreachable;

nested exception is:

javax.net.ssl.SSLKeyException: [Security:090504]Certificate chain received from

RSA-AM - 172.17.2.101 failed hostname verification check. Certificate contained

rsa-am.example.com but check expected RSA-AM; No available router to destination

java.rmi.ConnectException: Destination unreachable; nested exception is:

javax.net.ssl.SSLKeyException: [Security:090504]Certificate chain received from

RSA-AM - 172.17.2.101 failed hostname verification check. Certificate contained

rsa-am.example.com but check expected RSA-AM; No available router to destination

The hostname configured in Step 10 on page 21 does not match the certificate returned by Authentication Manager. The certificate contains the fully qualified domain name (for example, rsa- am.example.com), but the driver configuration contains just the hostname (for example, rsa-am). To correct this issue, configure the driver to use the fully qualified domain name (for example, t3s:// rsa-am.example.com:7002)

**7.6 ArraySyntax Environment Variable Not Set**

The RSA driver may shut down during startup with the following error:

[07/11/13 09:38:16.440]:RSA ST: DirXML Log Event -------------------

Driver: \EXAMPLE\services\Driver Set\RSA Status: Fatal

Message: Code(-9005) The driver returned a "fatal" status indicating that the

driver should be shut down. Detail from driver:

<description>com.trivir.ace.AceToolkitException: Instantiation of api class

failed.

java.lang.reflect.InvocationTargetException

com.trivir.ace.AceToolkitException: The 'sun.lang.ClassLoader.allowArraySyntax'

property is either false or not configured in your IDM installation. This value is

required for RSA driver functionality. Please refer to the RSA driver documentation

for configuration instructions.

</description>

If this occurs, confirm that the Java startup properties have been configured as described in

Section 2.2.4, “Setting IDM Java Startup Properties for RSA Authentication Manager 7.1,” on page 16.

**7.7 Dependency Missing**

The RSA Driver may shut down during startup with the following error:

[07/11/13 09:31:00.907]:RSA ST: DirXML Log Event -------------------

Driver: \EXAMPLE\services\Driver Set\RSA Status: Fatal

Message: Code(-9005) The driver returned a "fatal" status indicating that the driver should be shut down. Detail from driver:

<description>com.trivir.ace.AceToolkitException: Instantiation of api class

failed.

java.lang.reflect.InvocationTargetException

com.trivir.ace.AceToolkitException: The jar(s) wlfullclient.jar seem to be missing.

Please review the RSA driver installation instructions and confirm that the RSA jar

files are correctly installed.

If this occurs, confirm that the RSA files have been correctly copied as described in Section 2.2.1, “Copying RSA Files,” on page 14.

A A**Driver Properties**

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](https://www.netiq.com/documentation/idm402/pdfdoc/idm_common_driver/idm_common_driver.pdf#b94pq23)” in the [*Identity Manager 4.0.2 Common Driver Administration Guide*](https://www.netiq.com/documentation/idm402/pdfdoc/idm_common_driver/idm_common_driver.pdf#Front) 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.



 Section A.1, “Driver Configuration,” on page 35

 Section A.2, “Global Configuration Values,” on page 38

**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:

 Section A.1.1, “Driver Module,” on page 36

 Section A.1.2, “Driver Object Password (iManager Only),” on page 36

 Section A.1.3, “Authentication,” on page 36

 Section A.1.4, “Startup Option,” on page 37

 Section A.1.5, “Driver Parameters,” on page 37

 Section A.1.6, “ECMAScript,” on page 38

 Section A.1.7, “Global Configuration,” on page 38

**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 administrative user that the driver will use for authentication. For example: rsadriver. This is the user created in Section 3.0, “Preparing RSA Authentication Manager,” on page 17.

**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 host name 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 parameter 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 3.0, “Preparing RSA Authentication Manager,” on page 17.

**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 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 37

 “Subscriber Options” on page 38

 “Publisher Options” on page 38

**Driver Options**

**RSA Command Client User:** Specify the command client user for your RSA installation. This information was gathered in “Obtaining the Command Client Username and Password” on page 15.

**RSA Command Client Password:** Specify the command client password for your RSA installation. This information was gathered in “Obtaining the Command Client Username and Password” on page 15

**RSA Realm:** Specify the RSA realm containing the driver user specified in the Authentication

ID. Currently only the default SystemDomain realm is supported.

**Weblogic Library Directory:** Specify the location of the RSA/Weblogic jars that were copied during “Copying RSA Files” on page 14. The default locations are:

-Windows: C:\Novell\NDS\lib

-Linux/Unix: /opt/novell/eDirectory/lib/dirxml/classes

**RSA Identity Source:** Specify the case-sensitive name of the Identity Source with which to synchronize. If the field is empty, the first Identity Source in the Realm will be used. If in doubt, specify an Identity Source..

**Subscriber Options**

The RSA driver does not currently have any Subscriber Options.

**Publisher Options**

**Disable Publisher:** Specify whether the publisher will poll 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**

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**

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 ones 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‐click the driver set icon , then click **Properties** > **GCVs**.



B B**Trace Levels**

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](https://www.netiq.com/documentation/idm402/pdfdoc/idm_common_driver/idm_common_driver.pdf#b1rc1vm)” in the

[*Identity Manager 4.0.2 Common Driver Administration Guide*](https://www.netiq.com/documentation/idm402/pdfdoc/idm_common_driver/idm_common_driver.pdf#Front).

C C**RSA Object Schema**

The RSA driver supports the following objects and attributes:

 Section C.1, “User Object,” on page 43

 Section C.2, “Token Object,” on page 43

**NOTE:** All time values are expressed as a ctime value ‐ number of seconds elapsed since 00:00:00 on

January 1, 1970 UTC.

**C.1 User Object**

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 |
| Password | String | **NOTE:** The password attribute is only synchronized on the subscriber channel. The password must be populated when an LDAP Identity Source is specified in RSA Authentication Manager. The Password must meet the password complexity requirements of the specified Identity Source. |

**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) |
| 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) (read- only) |
| Assigned | Boolean | Whether the token is assigned (TRUE/FALSE) (read-only) |
| UserNum | String | Internal ID of the user to whom the token is assigned (read- only) |
| DefaultLogin | String | Login ID of the user to whom the token is assigned (read-only) |
| EmergencyAccess | String | Whether the token is enabled for emergency access (TRUE/ FALSE) (read-only) |
| 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 (read-only) |
| CountsLastModified | Numeric | Time the token counts were last modified (read-only) |
| Protected | Boolean | Whether the software token was copy-protected on last deployment (TRUE/FALSE) (read-only) |
| 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) |

|  |  |  |
| --- | --- | --- |
| **Attribute** | **Type** | **Description** |
| 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 tokencode |
|  |  | 1-PIN only |
| 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 (read-only) |
| EACPasscode | String | Assigned emergency token code (read-only) |