

# **Driver for Remedy Action Request System (ARS) Implementation Guide**

**Identity Manager 4.5**

July 2014



## Legal Notices

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 "AS IS" 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 ("Module") 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.

© 2014 NetIQ Corporation. All Rights Reserved.

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

<b>About this Guide</b>	<b>5</b>
<b>About NetIQ Corporation</b>	<b>7</b>
<b>1 Understanding the Remedy Driver</b>	<b>9</b>
1.1 Supported ARS Remedy Versions.....	9
1.2 Driver Concepts.....	9
1.2.1 Default Data Flow.....	9
1.2.2 Policies.....	10
1.2.3 Driver Components.....	10
1.2.4 Limitations.....	11
1.3 Support for Standard Driver Features.....	12
1.3.1 Local Platforms.....	12
1.3.2 Remote Platforms.....	12
1.3.3 Entitlements.....	12
<b>2 Driver preparation</b>	<b>13</b>
2.1 Prerequisites.....	13
2.2 Where to Install the ARS Remedy Driver.....	13
2.2.1 Local installation.....	13
2.2.2 Remote Loader installed on the Mid-Tier server.....	13
2.2.3 Remote Loader installed on another server.....	14
2.3 Creating an ARS Remedy Account.....	14
<b>3 Installing ARS Objects Driver</b>	<b>15</b>
3.1 Installing the IDM Filters, Form and Web-service in Remedy.....	15
3.2 Configuring the IDM Notifier Filter.....	15
3.2.1 Editing the IDM Notifier Filter to match the ARS Remedy Account.....	15
3.2.2 Editing the IDM Notifier Filter to change the published ARS Remedy Forms.....	16
3.3 Configuring the Web service.....	16
<b>4 Creating a New Driver</b>	<b>19</b>
4.1 Packages.....	19
4.1.1 Base package.....	19
4.1.2 User Passwords package.....	19
4.1.3 Entitlements package.....	19
4.1.4 Account tracking package.....	19
4.1.5 Managed System Information package.....	19
4.2 Importing the Driver Package.....	19
4.3 Importing SSL certificate.....	24
4.4 Deploying the Driver.....	25
4.5 Starting the Driver.....	25
4.6 Activating the Driver.....	25
<b>5 Managing the Driver</b>	<b>27</b>
<b>6 Troubleshooting the Driver</b>	<b>29</b>
<b>A Driver Properties</b>	<b>31</b>
A.1 Driver Configuration.....	31
A.1.1 Driver Module.....	31
A.1.2 Driver Object Password.....	32
A.1.3 Authentication.....	32
A.1.4 Startup Option.....	33
A.1.5 Driver Parameters.....	34

A.2 Driver Global Configuration Values (GCV).....	34
A.2.1 Base package.....	35
A.2.2 Password synchronization package.....	35
A.2.3 Entitlements package.....	35
A.2.4 Managed System Information package and data collection.....	36
A.2.5 Account tracking package.....	36
<b>B Upgrade procedure from ARS Remedy driver 7.1</b>	<b>39</b>
B.1 Configuring ARS Remedy web services.....	39
B.2 Installation of the new shim.....	39
B.3 Update of the driver object.....	39
<b>C Uninstalling the driver</b>	<b>41</b>
C.1 Deleting Identity Manager Driver Objects.....	41
C.2 Deleting the User, Filters, Form and Web-service from ARS Remedy.....	41
<b>D Synchronize a custom object class</b>	<b>43</b>
<b>E Driver type mapping</b>	<b>45</b>
E.1 Class-mapping XML file format.....	45
E.2 Class-mapping installation procedure.....	46
E.3 Class-mapping sample file.....	47
<b>F Trace Levels</b>	<b>49</b>

---

# About this Guide

The Identity Manager Driver for ARS Remedy is designed to synchronize data between the IDM Metadirectory and data stored in an ARS Remedy server. This configurable solution allows you to increase productivity and streamline business processes by integrating ARS Remedy and eDirectory. The Remedy Action Request System (ARS) Implementation Guide explains how to install, configure, and manage the Identity Manager Driver for Remedy.

## Intended Audience

This guide is intended for consultants, administrators, and IS personnel who need to install, configure, and maintain the Identity Manager driver for ARS Remedy.

## Other Information in the Library

The library provides the following information resources:

### Identity Manager Framework Installation Guide

Provides detailed planning and installation information for Identity Manager components.

### Identity Manager Integrated Installation Guide

Provides integrated installation information for installing Identity Manager components.

### Identity Manager Overview Guide

Provides conceptual information about Identity Manager. This book also provides an overview of the various components and many administration tasks.

### Identity Manager Driver Guides

Provides implementation information about Identity Manager drivers.



---

# 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. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's 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.

<b>Worldwide:</b>	<a href="http://www.netiq.com/about_netiq/officelocations.asp">www.netiq.com/about_netiq/officelocations.asp</a>
<b>United States and Canada:</b>	1-888-323-6768
<b>Email:</b>	<a href="mailto:info@netiq.com">info@netiq.com</a>
<b>Web Site:</b>	<a href="http://www.netiq.com">www.netiq.com</a>

## Contacting Technical Support

For specific product issues, contact our Technical Support team.

<b>Worldwide:</b>	<a href="http://www.netiq.com/support/contactinfo.asp">www.netiq.com/support/contactinfo.asp</a>
<b>North and South America:</b>	1-713-418-5555
<b>Europe, Middle East, and Africa:</b>	+353 (0) 91-782 677
<b>Email:</b>	<a href="mailto:support@netiq.com">support@netiq.com</a>
<b>Web Site:</b>	<a href="http://www.netiq.com/support">www.netiq.com/support</a>

## Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click Add Comment at the bottom of any page in the HTML version 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

NetIQ Communities, 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, NetIQ Communities 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 [community.netiq.com](http://community.netiq.com).



---

# 1 Understanding the Remedy Driver

The Remedy Action Request System (ARS) is a platform and development environment for automating Service Management business processes.

The Identity Manager Driver for Remedy ARS provides data integration between NetIQ® eDirectory™ and Remedy ARS.

The ARS Remedy driver uses the web-service to access ARS Remedy objects and data. Preconfigured driver policies allow synchronization, creation, and management between eDirectory and Remedy ARS for both users and groups.

For example, the driver can synchronize new employee data from eDirectory by sending the information to Remedy ARS, where an account and password are created automatically.

The driver can also synchronize other Remedy data between the two systems.

- ◆ [Section 1.1, “Supported ARS Remedy Versions” on page 9](#)
- ◆ [Section 1.2, “Driver Concepts” on page 9](#)
- ◆ [Section 1.3, “Support for Standard Driver Features” on page 12](#)

## 1.1 Supported ARS Remedy Versions

The ARS Remedy Driver uses the web-service provided by ARS Remedy and can be used with ARS Server 7.1 and later. This driver requires the Remedy Mid-tier sever for the web-services.

## 1.2 Driver Concepts

The following sections explain concepts you should understand before implementing the ARS driver.

- ◆ [Section 1.2.1, “Default Data Flow” on page 9](#)
- ◆ [Section 1.2.2, “Policies” on page 10](#)
- ◆ [Section 1.2.3, “Driver Components” on page 10](#)
- ◆ [Section 1.2.4, “Limitations” on page 11](#)

### 1.2.1 Default Data Flow

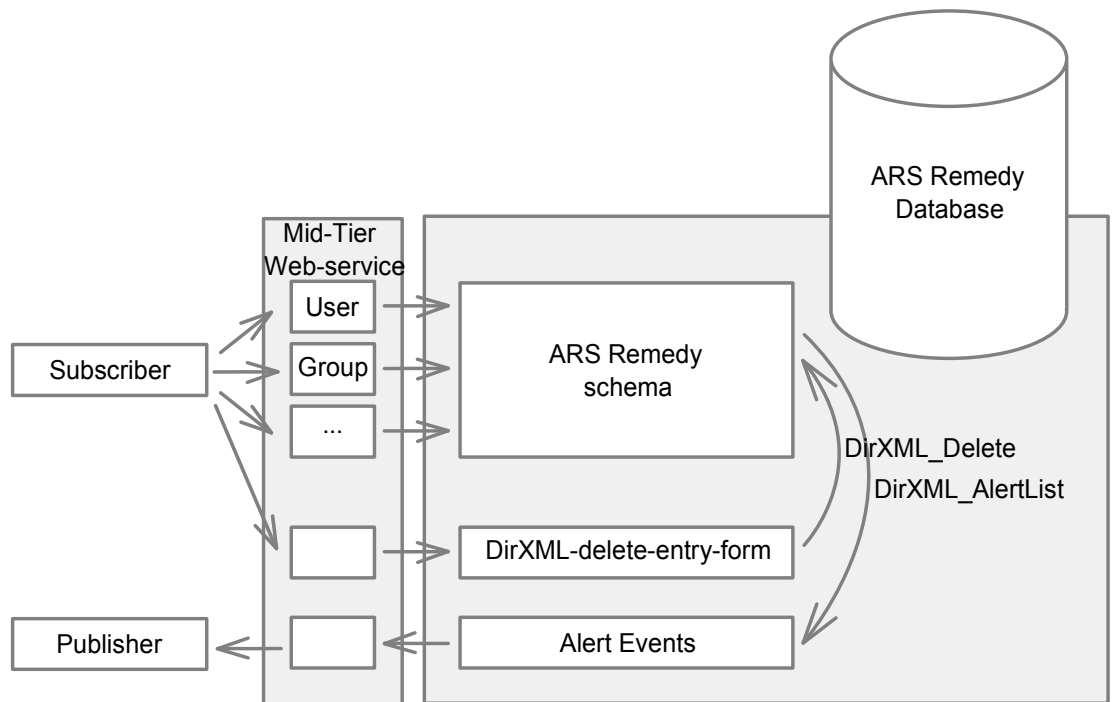
A driver channel is a combination of rules, policies, and filters that are used to synchronize data between two systems. The Subscriber and Publisher channels describe the direction in which the data flows. The Subscriber and Publisher channels act independently; actions in one channel are not affected by what happens in the other.

#### **Subscriber Channel**

The Subscriber channel is the channel of communication from the Identity Vault to ARS Remedy. The channel sends events generated in the Identity Vault to ARS.

#### **Publisher Channel**

The Publisher channel represents the channel of communication from ARS Remedy to the Identity Vault. The channel sends events generated in ARS Remedy to the Identity Vault.



## 1.2.2 Policies

Policies are used to control the synchronization of data between the Identity Vault and ARS Remedy. Policies transform an event on a channel input into a set of commands on the channel output. The ARS Remedy driver includes the following set of preconfigured policies:

- ◆ **Schema Mapping:** Mappings have been defined for the User and Group Remedy forms.
- ◆ **Creation:** The Subscriber Creation policies check mandatory attributes and ensure that the object has a Full Name. The Publisher Creation policy builds the Surname for Users based on the Remedy Full Name.
- ◆ **Matching:** The default Matching policy logic for the Publisher and Subscriber channels are the same. An Identity Vault User object is considered to be the same object in ARS when CN and Object Name match in both directories. You should modify these policies to meet your business requirements.
- ◆ **Placement:** Since ARS Remedy Object placement is flat, there is no Placement Policy for the subscriber. The Publisher Placement policy is flat by default, the container name and context for the default Publisher Placement policy is collected from the user when importing the default driver configuration. You should modify or add additional Placement policies and policy rules to meet your business needs.

## 1.2.3 Driver Components

The driver contains the following components:

- ◆ **Driver Packages:** The packages for Designer are delivered through the Designer package update system. If they are not available in your setup, check for package updates: in designer, click on Help > Check for Package Updates. The available packages are described in [Section 4.1 Packages on page 19](#).
- ◆ **Driver shim:** `ARSDriver75.jar` is the Java file that directs synchronization between ARS Remedy and the Identity Vault.
- ◆ **Remedy object definitions:** `ARSDriver75-Objects.def` contains a set of object definitions to be imported with the BMC Remedy Developer Studio:

- **Web service definitions:**
  - *DirXML\_AlertList*: Provides an interface to the action performed in ARS Remedy on User and Group objects (similar to the changelog present in JDBC drivers).
  - *DirXML\_Delete*: Provides an interface to delete objects in ARS Remedy. By, default, ARS Remedy does not provide a web-service interface to delete objects. This one allows deleting objects with the help of the DirXML-delete-entry-form and the DirXML-delete-entry-filter (described below).
  - *User*: Provides an interface to create, read and modify users. This is a standard Remedy object and should be already present. If not, see section 3.1 Installing the IDM Filters, Form and Web-service in Remedy step 9.
  - *Group*: Provides an interface to create, read and modify groups. This object is a standard Remedy object and should be already present. If not, see section 3.1 Installing the IDM Filters, Form and Web-service in Remedy step 9.
- **Form definitions**
  - *DirXML-delete-entry-form* is the Remedy ARS form definition for the delete object requests (which are technical objects created and cleaned-up by the driver and are used for the deletion of objects in ARS Remedy). This form is a place-holder for the object form name and the object request ID.
- **Filter definitions:** Remedy ARS Filters are required for the publisher channel to work and for the subscriber delete operations.
  - *DirXML-Delete-entry-filter*: The filter is triggered when a new DirXML-delete-entry-form is created. The DirXML-delete-entry-form object contains the reference to the object that must be deleted (form name and request ID). The filter deletes the referenced object.
  - *DirXML-Delete-entry-filter-cleanup*: The filter is triggered on modification of a DirXML-delete-entry-form and is used to clean (delete) the DirXML-delete-entry-form object. This filter is automatically triggered by the shim through the DirXML\_Delete web-service.
  - *DirXML Notifier*: The Filter is triggered when events occur in Remedy ARS and saves data in the Alert Form for the publisher channel. The publisher channel then reads that form to determine the event type and filters the updates based on objects and attributes specified in the Publisher filter in the Identity Vault driver configuration.

The driver can be configured without publisher channel : no events will be received from ARS Remedy. In this case, the objects *DirXML Notifier* and *DirXML-AlertList* should not be installed. The driver can be configured to not delete objects in ARS Remedy. In which case, the object *DirXML\_Delete*, *DirXML-delete-entry-form*, *DirXML-Delete-entry-filter* and *DirXML-Delete-entry-filter-cleanup* should not be installed. You should only disable the delete operations if you do not use the publisher channel. Otherwise, alert events objects (created by the *DirXML Notifier*) will not be deleted by the shim and will accumulate. A better option is to add a custom policy that veto the delete operations.

## 1.2.4 Limitations

- ◆ The driver supports only the Character, Date/Time, Integer, Drop-Down List and Radio Button Fields. Because the web-service does not provide information about referential attributes (Views, Tables...) within the WSDL, these are mapped to string attributes by default and no reference is made. But, the driver allows for the overriding of this behavior through a configuration file (see [Appendix E](#). Driver type mapping) so that these attributes can be mapped to a dn.
- ◆ Password Synchronization is only supported on the Subscriber channel. The driver can send

passwords to Remedy but cannot get passwords since Remedy does not support password capture.

- ◆ <move> commands are not supported by this driver since the ARS is a flat name-space. There is no way to move objects in Remedy.

## 1.3 Support for Standard Driver Features

The following sections provide information about how the ARS Remedy driver supports these standard driver features:

- ◆ [Section 1.3.1, “Local Platforms” on page 12](#)
- ◆ [Section 1.3.2, “Remote Platforms” on page 12](#)
- ◆ [Section 1.3.3, “Entitlements” on page 12](#)

### 1.3.1 Local Platforms

A local installation is an installation of the driver that runs on the Metadirectory server. The ARS Remedy driver can be installed on any Metadirectory-supported operating system.

For information about the operating systems supported for the Metadirectory server, see [“Metadirectory Server”](#) in [“System Requirements”](#) in the *Identity Manager 4.5 Installation Guide*.

### 1.3.2 Remote Platforms

The ARS Remedy driver can use the Remote Loader service to run on a server other than the IDM server. You may want to spread the load onto different servers. In this case, you can install the Remote Loader and driver on the Mid-tier server or on a server running the IDM Remote Loader. The Remote Loader enables the driver to communicate with the Metadirectory server.

For information about the operating systems supported for the Remote Loader, see [“Remote Loader”](#) in [“System Requirements”](#) in the *Identity Manager 4.5 Installation Guide*.

### 1.3.3 Entitlements

The ARS Remedy driver does provide entitlements within the Entitlement package. For more information, see [Section 4.1.3 Entitlements package](#).

As for other drivers, you can also setup customized entitlements and implement policies allowing the driver to use them.

---

# 2 Driver preparation

There are several installation scenarios you can use to best meet the needs of your environment. The following sections explain the scenarios and provide instructions for installing the files based upon the scenario you have chosen.

- ◆ Section 2.1, “Prerequisites” on page 13
- ◆ Section 2.2, “Where to Install the ARS Remedy Driver” on page 13
- ◆ Section 2.3, “Creating an ARS Remedy Account” on page 14

## 2.1 Prerequisites

The ARS Remedy driver requires at least patch “IDM Roles Based Provisioning Module 402 Field Patch A” to be installed. You also have to apply the “Special Instructions #9 WSSDK” from the readme.html.

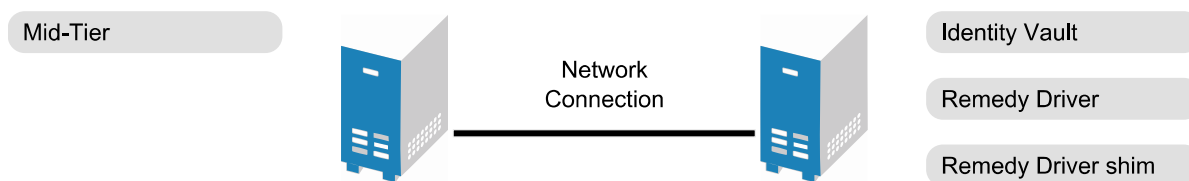
## 2.2 Where to Install the ARS Remedy Driver

You must decide whether to install the ARS Driver locally or remotely.

- ◆ Section 2.2.1, “Local installation” on page 13
- ◆ Section 2.2.2, “Remote Loader installed on the Mid-Tier server” on page 13
- ◆ Section 2.2.3, “Remote Loader installed on another server” on page 14

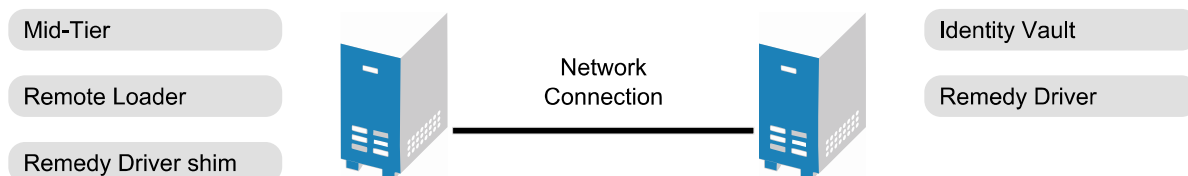
### 2.2.1 Local installation

In a local installation, the ARS Remedy driver is on the same server as the Metadirectory engine. The Mid-Tier server can either run on the same or on another server. If the driver does not run on the Mid-Tier server, it is highly recommended that you configure the Mid-Tier to use SSL for the web services. If SSL is not enabled, clear text passwords will be sent over the network.



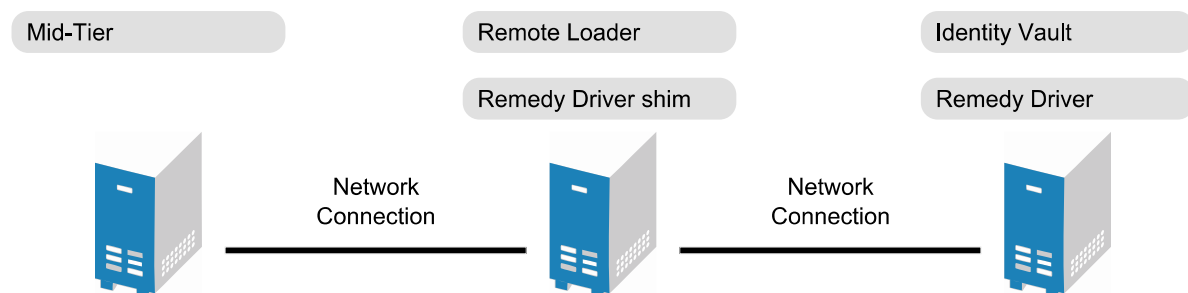
### 2.2.2 Remote Loader installed on the Mid-Tier server

One remote installation is for the ARS Remedy driver to run on the Mid-Tier server. This means that the Metadirectory engine and the driver shim run on different servers. The driver shim uses the Remote Loader to communicate with the Metadirectory engine. SSL communication between the Remote-Loader and the Metadirectory is highly recommended. For more information on how to install and configure the Remote loader, see the *Identity Manager 4.5 Remote Loader Guide*.



### 2.2.3 Remote Loader installed on another server

Another remote installation option is for the ARS Remedy driver to run on a third server – an IDM Remote Loader. The Mid-Tier server, the Metadirectory engine and the driver shim run on three different servers. The driver shim uses the Remote Loader to communicate with the Metadirectory engine and the shim communicates to the Mid-Tier server. SSL communication between the Remote Loader and the Metadirectory is highly recommended. You should also set-up the Mid-Tier service to use SSL. For more information on how to install and configure the Remote loader, see the [Identity Manager 4.5 Remote Loader Guide](#).



## 2.3 Creating an ARS Remedy Account

The driver requires an ARS Remedy account with Administrator rights and a fixed license to access the ARS Remedy system.

1. Login with the BMC Remedy User application.
2. Open the Object List, select the User form and click on *New*.
3. Fill in the *Login Name* (e.g.: dirxml), *Full Name* and *Password*.
4. Click on the *Fixed License Type* option.
5. Add the *Administrator Group* to the *Group List*.
6. Click on *Save*.

The Login Name must match with the *Run If Qualification* of the IDM Notifier Filter and the User Name for the *Notify Action* (see [Section 3.2, "Configuring the IDM Notifier Filter"](#) on page 15).

---

# 3 Installing ARS Objects Driver

Before creating the driver in the Identity Vault, you will need to import some objects into Remedy and possibly adapt them. The following sections provide instructions:

- ◆ Section 3.1, “Installing the IDM Filters, Form and Web-service in Remedy” on page 15
- ◆ Section 3.2, “Configuring the IDM Notifier Filter” on page 15
- ◆ Section 3.3, “Configuring the Web service” on page 16

## 3.1 Installing the IDM Filters, Form and Web-service in Remedy

You will need to import some objects in ARS Remedy server using the BMC Remedy Developer Studio. For more information on the imported objects, see section 1.2.3 [Driver Components](#) on page 10.

1. Log into the BMC Remedy Developer Studio.
2. Click on *File > Import...*
3. Select *Object Definitions* then click on *Next*.
4. Select the ARS Remedy server then click on *Next*.
5. Browse and choose the `ARSDriver75-Objects.def` located in `<idm install location>\drivers\remedy\tools`.
6. Click *Next*.
7. Select the all needed objects.
8. Click *Finish*.
9. Check that the User and the group web-service are configured
  1. Within BMC Remedy Developer Studio.
  2. In the panel *AR System Navigator*, select *All Objects > Web Services*
  3. Search for the User and the Group web-service
  4. If any of the above are missing, import the `User-Group-WS.def` by repeating steps 2-8

## 3.2 Configuring the IDM Notifier Filter

The IDM Notifier Filter acts like a trigger on the ARS Remedy Forms you want to publish to the Identity Vault. By default the filter is triggered on User and Group forms and notifies the user “dirxml”.

If the ARS Remedy Account used by the driver is not “dirxml” and you need the publisher channel, you must change the IDM Notifier Filter.

This is also true if you want to publish other ARS Remedy Forms to the Identity Vault.

- Section 3.2.1, “Editing the IDM Notifier Filter to match the ARS Remedy Account” on page 15
- Section 3.2.2, “Editing the IDM Notifier Filter to change the published ARS Remedy Forms” on page 16

### 3.2.1 Editing the IDM Notifier Filter to match the ARS Remedy Account

1. Log into the BMC Remedy Developer Studio.
2. In the left-hand panel, select *All Objects* and double-click on *Filters*.

3. In the resultant *Filters* tab that opens to the right, scroll down to and double-click *DirXML Notifier*.
4. Expand the *Run If Qualification* sub-panel below.
5. Change “*dirxml*” with the *Login Name* created in [Section 2.3, “Creating an ARS Remedy Account”](#) on page 14.
6. Expand the *If Actions* → *Notify* just below.
7. Change the *User* listed from “*dirxml*” to the same *Login Name* as step 4.
8. Click on *File > Save*.

### 3.2.2 Editing the IDM Notifier Filter to change the published ARS Remedy Forms

1. Log into the BMC Remedy Developer Studio.
2. Browse to and double-click on the DirXML Notifier Filter as above in steps 2-3.
3. Expand the Associated Forms sub-panel.
4. Right-click to remove or add Associated Form.
5. Click on *File > Save*.

### 3.3 Configuring the Web service

Follow this procedure to add a new web-service for a form present in ARS Remedy.

1. Log into the BMC Remedy Developer Studio.
2. Click on *File > New > Web Service*
3. Select your server and click on *Finish*
4. Select the form (e.g.: MyClass) you want to synchronize with IDM
5. Enter a label and a description
6. Expand the *WSDL-Ports* and the first *Port*
7. Change the name of the Port (e.g.: MyClass). The name you choose here will be the class name of the object advertised by the ARS Remedy Driver
8. Add the create operation:
  1. Right-click on *WSDL-Operations > Add Operation > Add Create Operation*
  2. Set the *name* of the operation to OpCreate
  3. You can remove attributes that you do not want to be synchronized by the driver with IDM
9. Add the set operation:
  1. Right-click on *WSDL-Operations > Add Operation > Add Set Operation*
  2. Set the *name* of the operation to OpSet
  3. You can remove attributes that you do not want to be synchronized by the driver with IDM
10. Add the get operation:
  1. Right-click on *WSDL-Operations > Add Operation > Add Get Operation*
  2. Set the *name* of the operation to OpGet
  3. You can remove attributes that you do not want to be synchronized by the driver with IDM
11. Add the get list operation:
  1. Right-click on *WSDL-Operations > Add Operation > Add Get List Operation*
  2. Set the *name* of the operation to OpGetList
  3. You can remove attributes that you do not want to be synchronized by the driver with IDM
12. Add permissions to the web-service:



1. In the *Properties* panel, change the *permissions*
2. Add the *Public* permission
3. Click *OK*
13. Click on *File > Save*.
14. Give a name to the web-service (e.g.: DirXML\_MyClass).



---

# 4 Creating a New Driver

Now you need to create and configure the ARS Remedy driver in Designer, after which you need to deploy it to the Identity Vault and start it.

- ◆ Section 4.1, “Packages” on page 19
- ◆ Section 4.2, “Importing the Driver Package” on page 19
- ◆ Section 4.3, “Importing SSL certificate” on page 24
- ◆ Section 4.4, “Deploying the Driver” on page 25
- ◆ Section 4.5, “Starting the Driver” on page 25

## 4.1 Packages

The driver is distributed as packages within Designer 4.0. If you do not find them, please check for packages updates (Help > Check for Packages Updates).

### 4.1.1 Base package

The base package contains the rules and configurations for the bi-directional synchronization of users and groups.

### 4.1.2 User Passwords package

This package adds user password synchronization from the Identity Vault to ARS Remedy only. Password synchronization on the publisher channel is not supported by the driver.

### 4.1.3 Entitlements package

This package adds two entitlements to the driver:

- ◆ User Account: granting or revoking this entitlement creates or deletes (or disables) the account in ARS Remedy.
- ◆ Group: this entitlement allows you to add / remove users to / from group through entitlements and, by extension, resources and roles.

### 4.1.4 Account tracking package

This package adds account tracking to users. This allows you to track the accounts and its status in ARS Remedy. The account and state information is stored in the DirXML-Accounts attribute of the user.

### 4.1.5 Managed System Information package

The Managed System Information package provides the required informations for the Data Collection and Managed System Gateway Drivers. This allows the Reporting Module to include information from your Remedy system.

## 4.2 Importing the Driver Package

1. In Designer, open your project.

2. In the Modeler, right-click the driver set where you want to create the driver, then select *New > Driver* to display the Driver Configuration Wizard.
3. In the *Available Packages* list, select *ARS Remedy Base*, then click *Next*.
4. Select any optional packages such as (see [4.1 Packages](#) for a description of the packages):
  1. ARS Remedy User Passwords
  2. ARS Remedy Entitlements
  3. ARS Remedy Managed System Info
  4. ARS Remedy Account Tracking
5. [Optional] Confirm the import of the driver dependencies by clicking *Ok*.
6. Follow the package configuration wizard by filling in the following fields:
  1. Common settings (configuration of the driver dependencies, may not appear if it is already configured):
    1. *User Container*: In case of a flat placement for the users in the ID Vault, select the container for the users, otherwise, select the base container of all the users. In case of a non flat placement, you will also have to update the placement policy of the publisher channel to fill your needs.
    2. *Group Container*: In case of a flat placement for the groups in the ID Vault, select the container for the groups, otherwise, select the base container for the groups. In case of a non flat placement, you will have to update the placement policy of the publisher channel to fill your needs.
    3. Click on *Next*
  2. Give the driver a name:
    1. *Driver Name*: Specify a name for the driver
    2. Click on *Next*
  3. Fill in the driver configuration informations:
    1. *Authentication ID*: Provide the user login information for the driver. This is the user you created in [Section 2.3 Creating an ARS Remedy Account](#).
    2. *Connection Information*: This is the base URL for the web-service's WSDL, without the "class part". It should be of the form `https://<mid-tier server name>/arsys/WSDL/public/<server name>`.  
Note that this URL does not point to any valid content. The URL composed by `<Connection Information>/<Object class>` must point to a valid WSDL (e.g.: `https://<mid-tier server name>/arsys/WSDL/public/<server name>/User`).  
Also note that HTTPS is not mandatory but it is recommended so you can use HTTP.
    3. *Set Password*: Set the password used by the user provided in the *Authentication ID*.
    4. *Driver Parameters*:
      1. *Driver Options (show/hide)*: Select show to (re)view the driver options.
        1. *Synchronized classes*: Fill in the synchronized classes, separated by a semicolon (;). The specified classes are the name(s) of the web-service(s). This name can, therefore, be different to the ARS Remedy form synchronized behind.
        2. *ARS Authentication information*: Fill in the ARS authentication information for the driver, see ARS Remedy documentation. This can be empty.
        3. *ARS Locale information*: Fill in the locale that will be used to communicate with the web-service. This can be empty.
        4. *ARS Timezone information*: Fill in the timezone that will be used to communicate with the web-service. This can be empty.
        5. *ARS Advanced options (show/hide)*: Select show to see the ARS driver advanced options.
          1. *ARS mapping filename*: Filename for the class mapping configuration. The

filename must have the extension .xml and be located in a jar file with a name beginning with "ars" (case-insensitive) and is in the runtime classpath. The file must be in the META-INF folder within this jar file. Leave the field empty to use the default mapping for the User and Group classes. For more information see [Appendix E Driver type mapping](#).

2. *Publisher Options (show/hide)*: Select show to (re)view the driver publisher options.
  1. *Disable publisher?*: Select *yes* if you do not want the driver to process events from ARS. If *no* is selected, the DirXML\_AlertList web-service must be available (see [Section 3.1 Installing the IDM Filters, Form and Web-service in Remedy](#)).
  2. *Polling interval*: Specify the number of seconds the publisher channel will sleep between polling cycles.
  3. *Polling interval precision*: Only for use when the driver is running in a virtual environment. In virtual environments there can be issues with time tracking and this parameter allows you, to some extent, to correct this. See [Chapter 6 Troubleshooting the Driver on page 29](#). In milliseconds.
  4. *Heartbeat interval*: The Subscriber heartbeat interval (in minutes).
3. *Subscriber Options (show/hide)*: Select show to (re)view the driver subscriber options.
  1. *Disable delete?*: Select *yes* if you do not want the driver to delete objects in ARS. If *no* is selected, the DirXML\_Delete web-service must be available (see [Section 3.1 Installing the IDM Filters, Form and Web-service in Remedy](#)).
5. Click on *next* to validate your choices and continue the driver configuration.
4. Continue the driver configuration:
  1. *Default Creator of objects*: Select the default creator for the object created by the driver in ARS Remedy. This is usually the user configured in section 2.3 Creating an ARS Remedy Account.
  2. *User default values*: Select some values that will be used during User create events.
    1. **Default User Licences Type**: Select the default User License Type for user creation. See ARS Remedy documentation for more information.
    2. **Default Full Text License Type**: Select the default Full Text License Type for user creation. See ARS Remedy documentation for more information.
    3. **Default User Default Notify Mechanism**: Select the default value for the Default Notify Mechanism for user creation. See ARS Remedy documentation for more information.
    4. **Default User Status**: Select the default User Status for user creation. See ARS Remedy documentation for more information.
  3. *Group default values*: Select some values that will be used during Group create events.
    1. **Default Group Category**: Select the default Group Category for group creation. See ARS Remedy documentation for more information.
    2. **Default Group Type**: Select the default Group Type for group creation. See ARS Remedy documentation for more information.
    3. **Default Group Status**: Select the default Group Status for group creation. See ARS Remedy documentation for more information.
  4. Click on *next* to validate your choices and continue the driver configuration.
5. Remote-loader configuration:
  1. *Connect to Remote Loader*: Select "yes" if you want to use a Remote Loader (for more

information, look at *Identity Manager 4.5 Remote Loader Guide*). If you select yes, please fill-in the required information:

1. *Host name*: Specify the host name or IP address of the server where the driver's Remote Loader service is running.
  2. *Port*: Specify the port number where the driver's Remote Loader service is listening.
  3. *KMO*: The kmo entry is optional. It is only used when SSL is configured between the Remote Loader and the Metadirectory engine. The KMO is the name of the certificate used for the SSL channel.
  4. *Other parameters*: Is used to add other parameters to the remote-loader.
  5. *Remote Password*: Specify the Remote Loader's password (as defined on the Remote Loader service). The Metadirectory engine requires this password to authenticate to the Remote Loader
  6. *Driver Password*: Specify the driver's password (as defined on the Remote Loader service).
6. Configure the selected packages:
1. ARS Remedy User Password:
    1. *Connected System or Driver Name*: Fill in the name of the system/driver that will be used in the email template for password synchronization.
    2. *On User creation, force distribution password presence on subscriber channel*: If the distribution password is not available when creating a user in the target system, the driver can choose to **Force presence** (this vetoes the User creation event which is delayed until the distribution password is present) or to **Use default password** (which is the surname of the user).
  2. ARS Remedy Account Tracking
    1. *Enable Account Tracking*: Select true to enable account tracking.
      1. *Realm*: Name of Realm, Security Domain or Namespace in which the account name is unique
    2. *Advanced Settings*:
      1. **Show**: the advanced settings are shown and can be edited.
        1. *Identifiers*: List of account identifiers. This list is in the application namespace.
        2. *Object class*: List of object classes being tracked. This list is in the application namespace.
        3. *Status Attribute*: The attribute indicating the account status. The value is in the application namespace.
        4. *Status active value*: The value of the Status Attribute indicating an active status.
        5. *Status inactive value*: The value of the Status Attribute indicating an inactive status.
        6. *Subscription default status*: Default status the policies will assume when an object is subscribed to the application and the status attribute is not set in the identity vault.
        7. *Publication default status*: Default status the policies will assume when an object is published to the identity vault and the status attribute is not set in the application.
      2. **Hide**: the advanced settings are not shown.
  3. ARS Remedy Entitlements
    1. *Use User Account Entitlement*:
      1. **true**: if this GCV is set to true, user accounts are only created for users with

the User Account entitlement granted. User objects without the entitlement are not created in ARS Remedy.

1. When using user account entitlements, you can specify the applied action when the entitlement is revoked.
  1. **Set Status:** when the entitlement is revoked, the Status is set to Disabled in ARS Remedy.
  2. **Delete Account:** when the entitlement is revoked, the Account is removed from ARS Remedy.
  3. **Do nothing:** when the entitlement is revoked, the Account is not removed from ARS Remedy and the status is not changed.
2. **false:** this value indicates that the User Account will not be used: all users are synchronized.
2. *Show Advanced Options:*
  1. *Enable Role Mapping:*
    1. **Yes:** If role mapping is enabled, this driver becomes visible to the role mapping administrator.
      1. *Enable Role Mapping for User Account:* **Yes/No** allows for enabling/disabling role mapping for the User Account entitlement.
      2. *Enable Role Mapping for Group Membership:* **Yes/No** allows for enabling/disabling role mapping for the Group Membership entitlement.
    2. **No:** Role mapping is disabled for all entitlements
  2. *Enable Resource Mapping:*
    1. **Yes:** If resource mapping is enabled, this driver becomes available for resource mapping in the roles-based provisioning module.
      1. *Enable Resource Entitlement for User Account:* **Yes/No** allows for enabling/disabling resource mapping for the User Account entitlement.
      2. *Enable Resource Entitlement for Group Membership:* **Yes/No** allows for enabling/disabling resource mapping for the Group Membership entitlement.
    2. **No:** Resource mapping is disabled for all entitlements
  3. *User Account extension:* The content of this field is added below the entitlement elements in the EntitlementConfiguration resource object.
  4. *Group Extension:* The content of this field is added below the entitlement elements in the EntitlementConfiguration resource object.
4. ARS Remedy Managed System Info
  1. General information
    1. *Name:* Specify a descriptive name for the managed system.
    2. *Description:* Specify a brief description of the managed system
    3. *Location:* Specify the location of the managed system.
    4. *Vendor:* Specify the vendor of the managed system.
    5. *Version:* Specify the version of the managed system.
  2. System Ownership
    1. *Business owner:* Specify the business owner of the managed system. This must be a user object (not a role, group, or container).
    2. *Application owner:* Specify the application owner of the managed system. This must be a user object (not a role, group, or container).
  3. System Classification
    1. *Classification:* Specify the classification of the managed system. Possible

values are:

1. **Mission-critical**
  2. **Vital**
  3. **Non-critical**
  4. **Other:** when selecting other, a prompt for a custom classification shows.
    1. *Custom classification:* Custom value for the classification.
  2. *Environment:* Specify the type of environment the managed system provides.
    1. **Development**
    2. **Test**
    3. **Staging**
    4. **Production**
    5. **Other:** when selecting other, a prompt for a custom environment name shows.
      1. *Custom Type Of Environment:* Specify a custom type of environment the managed system provides.
7. Click on finish to conclude the packages driver configuration.

At this point, the driver is created and configured from the packages. To ensure that the driver works the way you want it to for your environment, you should review and modify (if necessary) the driver's default configuration settings, policies, schema mapping and filter. After completing the configuration tasks, if the mid-tier uses SSL, continue with the next section 4.3, Importing SSL certificate, otherwise jump to section 4.4, Deploying the Driver.

## 4.3 Importing SSL certificate

To configure Mid-Tier to use SSL, please see the application server documentation. If the Mid-Tier server uses SSL, you will need to import the certificate in the java keystore where the driver runs.

1. Export the certificate, e.g. using the browser of your choice to navigate to the mid-tier and export the certificate of the service.
2. Install the certificate:

Java path		Linux	Windows
Remote loader	32bit	See the Identity Manager 4.5 Remote Loader Guide sections "Configuring the Java Remote Loader" and "Creating a Secure Connection"	[remote loader install folder]\jre
	64bit		[remote loader install folder]\64bit\jre
Local installation	32bit	[eDirectory install folder]/lib/nds-modules/jre[version]	[eDirectory install folder]\jre
	64bit	[eDirectory install folder]/lib64/nds-modules/jre[version]	[eDirectory install folder]\jre

### 2.1. run keytool

```
[java path]/bin/keytool -importcert -trustcacerts -alias
[certificate alias] -file [path to the certificate] -keystore
[java path]/lib/security/cacerts
```

### 2.2. restart eDirectory or the remote loader



## 4.4 Deploying the Driver

After the 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 the deployment summary, then click *Deploy*.
6. Read the 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 may be used to supply these rights. However, you might want to create a user for the driver and assign security rights to that user so that the driver will be able to act on the Identity Vault.

  - a) Click *Add*, then browse to and select the object with the correct rights.
  - b) 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, the admin and driver's user) from synchronization.
  - a) Click *Add*, then browse to and select the user object you want to exclude.
  - b) Click *OK*.
  - c) Repeat **Step 8a** and **Step 8b** for each object you want to exclude.
  - d) Click *OK*.
9. Click *OK*.

## 4.5 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. If you are using the Remote Loader with the driver, make sure the Remote Loader driver instance is running (see *Identity Manager 4.5 Remote Loader Guide*).
2. In Designer, open your project.
3. In the Modeler, right-click the driver icon or the driver line, then select *Live > Start Driver*.

When the driver starts for the first time, it does the following:

- Searches for the ARS Remedy Server (specified in the **driver parameters**).
- Retrieve the ARS Remedy Schema for the selected Object classes.

## 4.6 Activating the Driver

If you created the driver in a driver set where you have already activated the Identity Manager server and service drivers, the driver inherits the activation. If you created the driver in a driver set that has not been activated, you must activate the driver within 90 days. Otherwise, the driver stops working. For information on activation, refer to "*Activating NetIQ Identity Manager Products*" in the *Identity Manager 4.5 Integrated Installation Guide*.



---

# 5 Managing the Driver

As you work with the ARS Remedy 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 4.5 Common Driver Administration Guide*.



---

# 6 Troubleshooting the Driver

This section contains potential problems and error codes you might encounter while configuring or using the driver.

- ◆ **Authentication failed:** The login or the password is invalid in the driver's configuration, correct it and start the driver again. This is a fatal error so the driver will shutdown.
- ◆ **Missing authentication information:** No login/password/server were supplied to the driver. Check the driver configuration in iManager. This is a fatal error and the driver will stop.
- ◆ **XML parsing error :: Can't parse XML for class ... from ... :** The specified web service is either unavailable or misspelled, please review the driver configuration and check if the web service is present.
- ◆ **No schemas to sync:** No schema names were supplied to the driver. Check the driver configuration with Designer or iManager. This is a fatal error and the driver will shutdown.
- ◆ **Malformed URL:** The driver didn't successfully log in. Check the driver authentication context. This is a fatal error so the driver will shutdown.
- ◆ **No events published:** Check that the IDM notifier is installed correctly on the ARS server.
- ◆ **Issues when synchronizing international characters:** Configure the locale in the *driver configuration/driver parameters* with iManager or Designer.  
ARS Local information=en.US.ISO-8859-1 (or any other character set)
- ◆ **Issues with polling interval cycle in VM environment:** VM time precision can interfere with the polling process (ie: the polling is not every cycle). To correct this behavior, a special publisher option is available. Set the *Polling interval precision (ms)* in the *driver configuration/driver parameters* with iManager or Designer.
- ◆ **Namespace issue:** you will see an error message similar to:  

```
com.sun.xml.internal.ws.streaming.XMLStreamReaderException:  
unexpected XML tag. expected:  
{urn:DirXML_AlertList}OpGetListResponse but found:  
{DirXML_AlertList}OpGetListResponse
```

This is due to a known bug in Developer Studio (solved in version 7.6.04 sp1). The description of the issue can be found in [Knowledge Article KA350259](#). If you use both Delete and AlertList services, you will have to apply the following procedure twice:

  1. Open the Web Service which has the operation with the corrupted targetNamespace.
  2. Go to its Input and Output Mapping sections and hover the mouse over the Root element.
  3. Check the value of targetNamespace property.
  4. If targetNamespace property shows a namespace with "urn:" prefix, then mapping is either correct or Developer Studio is showing targetNamespace after fixing it.
  5. To confirm that Web Service indeed has correct targetNamespace go to WSDL Publish Location section and load the WSDL.
    1. Check the namespace set for the operation response element.
    2. If the namespace has \*urn:\* prefixed, then targetNamespace if properly saved in Web Service.
    3. However if namespace of the element does not has \*urn:\* prefix then targetNamespace was not properly saved in Web Service.
  6. If targetNamespace is not properly saved then you must make some dummy changes in

the operation, so that editor gets "dirty", and then save the Web Service.

7. Then clear Mid-Tier cache and then check the WSDL again, this time namespace of the response element should be correctly generated.


- ◆ **Issue with HTTP Error 500: Internal Server Error.** When using ARS-Remedy with Mid-tier on IIS, you should configure IIS7+ to allow detailed error not only for local requests. The driver shim makes use of the detailed error messages and cannot take any action from the generic error 500. To solve this problem, follow the steps on the Mid-Tier server:
  - Open Internet Information Services (IIS) Manager
  - Select the Site and the Web site where the Mid-tier is.
  - Double-click on "Error Pages"
  - Click on "Edit Features Settings..." on the right pannel.
  - Select "Detailed errors" and click on OK.

Another option is to select "*Detailed errors for local requests and custom error pages for remote requests*" with a remote loader installed on the Mid-Tier server.

---

# A Driver Properties


This section provides information about the Driver Configuration and Global Configuration Values properties for the Remedy 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 4.5 Common Driver Administration Guide* for information about the common properties.

The information is presented from the viewpoint of iManager. If a field is different in Designer, it is marked with an  icon.

- ◆ [Section A.1, “Driver Configuration” on page 31](#)
- ◆ [Section A.2, “Driver Global Configuration Values \(GCV\)” on page 34](#)

## 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:
  1. In the *Administration* list, click *Identity Manager Overview*.
  2. If the driver set is not listed in the *Driver Sets* tab, use the *Search In* field to search for and display the driver set.
  3. 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 31](#)
- ◆ [Section A.1.2, “Driver Object Password” on page 32](#)
- ◆ [Section A.1.3, “Authentication” on page 32](#)
- ◆ [Section A.1.4, “Startup Option” on page 33](#)
- ◆ [Section A.1.5, “Driver Parameters” on page 34](#)

### A.1.1 Driver Module

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

Options	Description
<i>Java</i>	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 java class name is:



Options	Description
	be.opns.nds.dirxml.driver.ars.ARSDriverShim.
<i>Native</i>	This option is not used with the Remedy driver.
<i>Connect to Remote Loader</i>	Used when the driver is connecting remotely to the connected system. Designer includes two sub-options: <ul style="list-style-type: none"> <li>◆  <i>Driver Object Password</i>: 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 will not run. The Remote Loader uses this password to authenticate itself to the remote driver shim.</li> <li>◆  <i>Remote Loader Client Configuration for Documentation</i>: Includes information on the Remote Loader client configuration when Designer generates documentation for the driver.</li> </ul>

## A.1.2 Driver Object Password









Option	Description
<i>Driver Object Password</i>	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 or the remote driver will not run. This password is used by the Remote Loader 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.


Option	Description
<i>Authentication ID</i> or  <i>User ID</i>	Specify a user ID for the application. This ID is used to pass Identity Vault subscription information to the application.  Example: dirxml
<i>Authentication Context</i> or  <i>Connection Information</i>	Specify the base URL for the web-service's WSDL, without the "class part". Note that this URL does not point to any valid content. The URL composed by <code>&lt;Connection Information&gt;/&lt;Object class&gt;</code> must point to a valid WSDL. Also note that HTTPS is not mandatory, only recommended. You can use HTTP.  The connection string uses the following format: <code>https://&lt;server-mid-tier&gt;/arsys/WSDL/public/&lt;server-ars&gt;</code>



Option	Description
<p><i>Remote Loader Connection Parameters</i></p> <p>ok</p> <ul style="list-style-type: none"> <li> <i>Host name</i></li> <li> <i>Port</i></li> <li> <i>KMO</i></li> <li> <i>Other parameters</i></li> </ul>	<p>Used only if the driver is connecting to the application through the remote loader. The parameter to enter is <code>hostname=xxx.xxx.xxx.xxx port=xxxx kmo=certificatename</code>, where the hostname is the IP address or DNS name 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 only used when there is an SSL connection between the Remote Loader and the Metadirectory engine. Example: <code>hostname=10.0.0.1 port=8090 kmo=IDMCertificate</code></p>
<p>Driver Cache Limit (kilobytes)</p> <p>or</p> <ul style="list-style-type: none"> <li> Cache limit (KB)</li> </ul>	<p>Specify the maximum event cache file size (in KB). If it is set to zero, the file size is unlimited.</p> <ul style="list-style-type: none"> <li> Click <i>Unlimited</i> to set the file size to unlimited in Designer.</li> </ul>
<p>Application Password</p> <p>or</p> <ul style="list-style-type: none"> <li> Set Password</li> </ul>	<p>Specify the password for the user object listed in the Authentication ID field.</p>
<p>Remote Loader Password</p> <p>or</p> <ul style="list-style-type: none"> <li> Set Password</li> </ul>	<p>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.</p>

## A.1.4 Startup Option

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

Option	Description
<i>Auto Start</i>	The driver starts every time the Identity Manager server is started.
<i>Manual</i>	The driver does not start when the Identity Manager server is started. The driver must be started through Designer or iManager.
<i>Disabled</i>	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.
 <i>Do not automatically</i>	This option only applies if the driver is deployed and was

Option	Description
<i>synchronize the driver</i>	previously disabled. If this is not selected, the driver re-synchronizes all associated objects 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.

1. Driver Settings:
  1. *Synchronized Schemas*: Specify the synchronized Remedy Forms the driver will use to synchronize. This is the list of the web-service names, separated by a semicolon (;). This must not be empty.
  2. *ARS Authentication information*: Specify the ARS Authentication information for the web service authentication. This can be empty.
  3. *ARS Locale information*: Specify the ARS Locale information for the web service authentication. This can be empty.
  4. *ARS Timezone information*: Specify the ARS Timezone information for the web service authentication. This can be empty.
  5. *ARS mapping filename*: Specify the filename for the class mapping configuration. The filename must have the extension .xml and be located in a jar file with a name beginning with "ars" (case-insensitive) and is in the runtime classpath. The file must be in the META-INF folder within this jar file. Leave the field empty to use the default mapping for the classes User and Group.
2. Subscriber Settings:
  1. *Disable delete*: Select whether you want the shim to ignore delete events flowing from Identity Manager to ARS. Select yes if the DirXML\_Delete web-service is not implemented.
3. Publisher Settings:
  1. *Disable Publisher*: Select whether you want to ignore events flowing from ARS to Identity Manager. Select yes if the DirXML\_AlertList web-service is not implemented.
  2. *Polling Interval*: Specify the number of seconds the publisher channel will sleep between polling cycles.
  3. *Polling Interval Precision*: Only for use when the driver is running in a virtual environment.
  4. In virtual environment there can be issues with time tracking and this parameter allows you, to some extent, to correct this. See [Chapter 6 Troubleshooting the Driver on page 29](#).
  5. *Heartbeat interval*: Select the driver heartbeat in seconds. The driver heartbeat is a feature of the Identity Manager drivers. Using it is optional. The driver heartbeat is configured by using a driver parameter with a time interval specified. If a heartbeat parameter exists and has an interval value other than 0, the driver sends a heartbeat document to the Metadirectory engine if no communication occurs on the Publisher channel for the specified interval of time.

## A.2 Driver Global Configuration Values (GCV)

Here is the list of the driver configuration values, grouped by package.

- ◆ Section A.2.1, "Base package" on page 35
- ◆ Section A.2.2, "Password synchronization package" on page 35

- ◆ Section A.2.3, “Entitlements package” on page 35
- ◆ Section A.2.4, “Managed System Information package and data collection” on page 36
- ◆ Section A.2.5, “Account tracking package” on page 36

## A.2.1 Base package

1. **Default Creator of objects:** Select the default value for the Creator on object creation
2. **User default values:**
  1. *Default User License Type:* Select the default value for ARS License Type on User creation
  2. *Default User Full Text License Type:* Select the default User Full Text License Type
  3. *Default User Default Notify Mechanism:* Select the default value for the Default Notify Mechanism
  4. *Default User Status:* Select the default value for ARS Status on User creation
3. **Group default values:**
  1. *Default Group Category:* Select the default value for ARS Category on "Default Group Type" creation
  2. *Default Group Type:* Select the default value for ARS Group Type on "Default Group Type" creation
  3. *Default Group Status:* Select the default value for ARS Status on Group creation

## A.2.2 Password synchronization package

1. *Connected System or Driver Name:* The name of the connected system, application or Identity Manager driver. This value is used by the e-mail notification templates.
2. *On User creation, force distribution password presence on subscriber channel:* On User creation, should the distribution password be present on subscriber channel? If the selected option is **force presence** and no distribution password is set for the user, the operation will be vetoed. Otherwise, if the **use default password** option is selected, and the distribution password is not available on user creation, the surname is used as password in the target system.

## A.2.3 Entitlements package

1. *Use User Account Entitlement:* Entitlements act like an ON/OFF switch to control account access. When the driver is enabled for entitlements, accounts are only created and removed/disabled when the account entitlement is granted to or revoked from users. Entitlements are granted and revoked only by entitlement agents. If you select True, one of these entitlement agents must be installed and configured for your driver to create and delete/disable accounts.
  1. *When Account Entitlement revoked:* Choose what action is taken in Remedy when a User Account Entitlement is revoked. Allowed values are:
    1. **Do nothing:** no action is taken when the entitlement is revoked.
    2. **Set Status:** the Status of the user is set to Disabled when the entitlement is revoked.
    3. **Delete Account:** the account is deleted from ARS Remedy when the entitlement is revoked.
2. *Use Group Entitlement:* If set to true, the driver manages group memberships based on the Group Entitlement.
3. *Show Advanced Options:*
  1. **Role Mapping Configuration**
    1. *Enable Role Mapping:* If role mapping is enabled, this driver becomes visible to the role mapping administrator.
      1. *Enable Role Mapping for User Account:* Enable Role Entitlement for User Account

2. *Enable Role Mapping for Group Membership*: Enable Role Entitlement for Group Membership
2. **Resource mapping Configuration**
  1. *Enable Resource Mapping*: If resource mapping is enabled, this driver becomes available for resource mapping in the roles-based provisioning module.
    1. *Enable Resource Mapping for User Account*: Enable Resources Mapping for User Account
    2. *Enable Resource Mapping for Group Membership*: Enable Resources Mapping for Group Membership.
3. **Entitlement Extensions**
  1. *User account extensions*: Children of the <entitlement-extensions> node will be added below the User Account entitlement element in the EntitlementConfiguration resource object.
  2. *Group extensions*: Children of the <entitlement-extensions> node will be added below the Group entitlement element in the EntitlementConfiguration resource object.

## A.2.4 Managed System Information package and data collection

1. General Information
  1. *Name*: Specify a descriptive name for the managed system.
  2. *Description*: Specify a brief description of the managed system
  3. *Location*: Specify the location of the managed system.
  4. *Vendor*: Specify the vendor of the managed system.
  5. *Version*: Specify the version of the managed system.
2. System Ownership
  1. *Business Owner*: Specify the business owner of the managed system. This must be a user object (not a role, group, or container).
  2. *Application Owner*: Specify the application owner of the managed system. This must be a user object (not a role, group, or container).
3. System classification
  1. *Classification*: Specify the classification of the managed system.
  2. *Environment*: Specify the type of environment the managed system provides.
4. Connection And Miscellaneous Information: this information is automatically generated by the driver itself and is overwritten on driver reboot. **Do not touch this information!**

## A.2.5 Account tracking package

1. *Enable account tracking*: If true, account tracking policies are enabled. If false, account tracking policies are not executed.
  1. *Realm*: Name of Realm, Security Domain or Namespace in which the account name is unique
  2. *Advanced settings*: Changing these settings may result in malfunction of the Account Tracking feature. Only change these settings if you know exactly what you are doing!
    1. *Identifiers*: Add the account identifier attributes
    2. *Object class*: Add the object classes to track. Class names must be in the application namespace.
    3. *Status attribute*: Name of the attribute in the application namespace to represent the account status.
    4. *Status active value*: Value of the status attribute that represents an active state.
    5. *Status inactive value*: Value of the status attribute that represents an inactive state.

6. *Subscription default status*: Default status the policies will assume when an object is subscribed to the application and the status attribute is not set in the identity vault.
7. *Publication default status*: Default status the policies will assume when an object is published to the identity vault and the status attribute is not set in the application.



---

# B Upgrade procedure from ARS Remedy

## driver 7.1

This appendix describes the procedure to migrate from the old ARS Remedy driver 7.1 to this new driver. This upgrade procedure starts by adding the required new objects in the ARS Remedy system. When those objects are deployed, the new shim must be installed (if not already done). Using Designer, the new driver object must be configured, customized and deployed.

- ◆ Section B.1, “Configuring ARS Remedy web services” on page 39
- ◆ Section B.2, “Installation of the new shim” on page 39
- ◆ Section B.3, “Update of the driver object” on page 39

### B.1 Configuring ARS Remedy web services

To import and configure the required filters in ARS Remedy, follow the procedures:

- ◆ [2.1 Prerequisites](#),
- ◆ [3.1 Installing the IDM Filters, Form and Web-service in Remedy](#),
  - While importing the objects in BMC Remedy Developer Studio, make sure to select “Replace Objects on the Destination Server”.
- ◆ [3.2 Configuring the IDM Notifier Filter](#)
- ◆ [3.3 Configuring the Web service](#).

### B.2 Installation of the new shim

If the new driver shim is not already installed, copy it into the eDirectory classpath and restart eDirectory.

1. Copy the jar file (ARSDriver75.jar) in the eDirectory classpath:
  1. on Linux\*, it can be copied in the folder <eDirectory install folder>/lib/dirxml/classes.
  2. on Windows\*, it can be copied in the folder <eDirectory install folder>\lib.
2. Restart the eDirectory service:
  1. For Linux\*:

```
> sudo service ndsd restart
```
  2. For Windows\*:
    1. Start > Run
    2. Type “services.msc”, click on OK
    3. Find the eDirectory service (NDS Server), right-click on it and select restart.

### B.3 Update of the driver object

In Designer:

1. Rename or save the current driver. Rename is preferred if you have customized policies.
  - To save: right-click on the driver and select “Export to configuration file”
  - To rename: right-click on the driver and select “Properties”, change the name and click OK.

2. Import the new driver. Make sure the new driver has the same name as the previous one. Follow the procedure [section 4.2 Importing the Driver Package](#).
3. Copy, adapt and review the customized rules of the old driver, if any.
4. Deploy the new updated driver:
  1. On the driver, click on "Live" > "Deploy"
  2. Review the changes and click on "Deploy"
5. Restart the newly deployed driver:
  1. On the driver, click on "Live" > "Restart Driver"



---

# C Uninstalling the driver

- ◆ Section C.1, “Deleting Identity Manager Driver Objects” on page 41
- ◆ Section C.2, “Deleting the User, Filters, Form and Web-service from ARS Remedy” on page 41

## C.1 Deleting Identity Manager Driver Objects

When you are deleting NetIQ Identity Vault objects, you must delete all child objects before you can delete a parent object. For example, you must delete all rules and style sheets on the Publisher channel before you can delete the Publisher object. Similarly, you must delete both the Publisher and Subscriber objects before you can delete the Driver object. To remove a driver object from an Identity Vault:

1. In iManager, click *Identity Manager > Identity Manager Overview*.
2. Select a driver set.
3. On the Identity Manager Overview page, click *Delete Driver*.
4. Select the driver that you want to delete, then click OK.

## C.2 Deleting the User, Filters, Form and Web-service from ARS Remedy

Some objects will have been created during the driver installation procedure, follow these steps to remove them.

1. Delete the filters created by the `ARSDriver75-Objects.def`:
  1. Open BMC Remedy Developer Studio.
  2. In the AR System Navigator, open the Filters.
  3. Find the *DirXML-delete-entry-filter*.
  4. Right click and select Delete.
  5. Confirm the deletion of the filter by clicking OK.
  6. Repeat steps 3-5 for the *DirXML-delete-entry-filter-cleanup* and the *DirXML Notifier* filters.
2. Delete the *DirXML-delete-entry-form* form:
  1. Open BMC Remedy Developer Studio.
  2. In the AR System Navigator, open the Forms.
  3. Find the *DirXML-delete-entry-form*.
  4. Right click and select Delete.
  5. Confirm the deletion of the filter by clicking OK.
3. Delete the web-services:
  1. Open BMC Remedy Developer Studio.
  2. In the AR System Navigator, open the Forms.
  3. Find the *DirXML\_AlertList*.
  4. Right click and select Delete.
  5. Confirm the deletion of the filter by clicking OK.
  6. Repeat steps 3-5 for the *DirXML\_Delete* web-service.
4. Delete the user that you created in [section 2.3.Creating an ARS Remedy Account](#):
  1. Open BMC Remedy User.

2. Open the Object List, select the User form.
3. Search for the user with *Login Name* (e.g.: dirxml).
4. Select *Actions > Delete*.
5. Confirm the User deletion by clicking OK.

---

# D Synchronize a custom object class

Both ARS Remedy and the Metadirectory allows the creation and management of custom object classes. This section explains how to synchronize another object class (other than user and group).

To support another class, you have to:

1. Create a web service for that class with Remedy Developer Studio (use the user & group class as example), see Section 3.3 [“Configuring the Web service” on page 16](#)
2. [Optional] If you want to receive events from Remedy for that class, in Remedy Developer Studio, update the DirXML Notifier filter and add your class to the Associated Forms list:
  1. In the AR System Navigator, select All Objects and double click on Filters,
  2. Double click on the DirXML Notifier
  3. Expand the Associated Forms and add the new class you want to synchronize
3. [Optional] follow the procedure [section E Driver type mapping](#) to change the type of some attributes,
4. In Designer:
  1. Open the driver properties, select the driver configuration,, driver parameters, driver options.
  2. Update the list of Synchronized Classes : add the new class you want to synchronize.
  3. Deploy the driver changes and restart the driver (see [section 4.4, “Deploying the Driver”](#)).
  4. You can now, refresh the application schema and, as with any other driver, start writing custom rules for the new class.
5. Repeat the steps 1 to 4 for each new class you want to synchronize,



---

# E Driver type mapping

Sometimes the type of the attributes differ between the ARS Remedy web-service and the attributes known in the Metadirectory. This mapping is different from the Schema mapping policies (which mostly map two attributes of the same type with different names). This mapping is done by the shim and has two main usages:

- ◆ transform a multi-valued attribute to the format handled by the web-service,
- ◆ the resolution of “foreign key” (i.e. resolve the association).
  
- ◆ Section E.1, “Class-mapping XML file format” on page 45
- ◆ Section E.2, “Class-mapping installation procedure” on page 46
- ◆ Section E.3, “Class-mapping sample file” on page 47

## E.1 Class-mapping XML file format

This mapping is configured through an XML file inside a jar in the eDirectory classpath. A default mapping for the User and the Group is bundled with the driver. Only one configuration is allowed by the driver. This means that if you set a new configuration file, you will lose the default configuration for the Users and the Groups unless you start your work from the default configuration (see [Section E.3 Class-mapping sample file](#)).

The XML file is a list of class/web-service pairings and each class has two types of mapping:

- ◆ *operation-map*: used to map an operation type to the name of the operation in the web-service.
  - **type**: the type of the operation. Mandatory attribute in the XML.
    - `get`: is the service to query the content of one form (must be a *Get Operation* in Developer Studio),
    - `set`: is the service to set the content of one form (must be a *Set Operation* in Developer Studio),
    - `get-list`: is the service to query one form (must be a *Get List Operation* in Developer Studio),
    - `create`: is the service to create a new object (must be a *Create Operation* in Developer Studio).

The operation-map is optional, the default mapping is:


- `get` → `OpGet`,
  - `set` → `OpSet`,
  - `get-list` → `OpGetList`,
  - `create` → `OpCreate`.
- ◆ *attribute-map*: used to map the type of attribute.
    - **name**: the name of the attribute. Mandatory attribute in the XML.
    - **type**: the type the attribute will be mapped to. Mandatory attribute in the XML.
      - `dn`: maps the attribute to a dn. The value is a reference to another object.
      - `string`: no mapping is performed
      - `int`: maps the attribute to an integer
      - `time`: maps the attribute to a time
    - **multivalued**: indicates whether the attribute is multivalued (for the web-service). The

default value is `false`.

- `true`
- `false`
- **separator:** specify this to set the character separator used to separate the values on this multivalued attribute. Only needed when **multivalue** is set to true. Default value is the semicolon (;).
- **dn-map-to-class:** specify the class to which the object is referring. Must only be set when type is dn. Note that the class must be in the driver's configuration synchronized classes. Also note that the class name is the name of the web-service, and not the ARS Remedy form name or the Metdirectory class name.
- **dn-map-to-attribute:** specify the attribute to which the object is referring. Must only be set when type is dn. Note that the attribute name is the name provided by the web-service, not the name present on the ARS Remedy form (usually the difference between the two is that the spaces are replaced by underscores). See sample file.
- **validate-enum-value:** used to disable the validation of an enumeration value based on the WSDL coming from ARS Remedy. May be required when a value is missing within the WSDL (May be required if you see a message like "Invalid enumeration value: <value> for <attribute\_name>" in the log file of the driver). Only available if type is string and the attribute is an enumeration. This attribute is optional.

## E.2 Class-mapping installation procedure

Here is the procedure to update the class-mapping file for the driver:

1. Create the XML file according to your needs.
  2. Create a jar file (the filename must start with "ars") with the XML configuration file in the META-INF directory, e.g. META-INF\<xml-file-name>.ol style="list-style-type: none;">  - 1. Create a new folder named META-INF
  - 2. Copy the XML configuration file to the META-INF folder
  - 3. Create the jar file (e.g.: *arsMapping.jar*):
    - `jar -cf arsMapping.jar META-INF`
3. Set the configuration of the driver, this can be done either with Designer or with iManager:
  1. In Designer:
    1. Right-click on the driver, select *Properties*.
    2. Click on *Driver-configuration > Driver-parameters*.
    3. Select show for the *ARS Advanced Options*.
    4. Type the XML filename in the *ARS mapping filename*.
    5. Validate the operation by clicking *OK*.
    6. Deploy the change:
      1. Right-click on the driver, select *Live>Deploy*.
      2. Click on *Deploy*.
      3. Review the deployment status and click *OK*.
  2. In iManager:
    1. Click on  *Identity Manager Administration*
    2. Select *Identity Manager Overview*
    3. Find the driver set
      1. 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.
      2. Click the driver set to open the *Driver Set Overview* page.
    4. Locate the driver icon, then click the upper right corner of the driver icon to display the *Actions* menu. Select *Edit properties*.

5. Select show for the *ARS Advanced Options*.
  6. Type the XML filename in the *ARS mapping filename*.
  7. Validate the operation by clicking *OK*.
  8. Accept to restart the driver by clicking *OK*.
4. Copy the jar file in the eDirectory classpath
    1. On Linux\*, it can be copied in the folder <eDirectory install folder>/lib/dirxml/classes.
    2. On Windows\*, it can be copied in the folder <eDirectory install folder>\lib.
  5. Restart the eDirectory service:
    1. For Linux\*:
      - > sudo service ndsd restart
    2. For Windows\*:
      1. Start > Run
      2. Type "services.msc", click on *OK*
      3. Find the eDirectory service (NDS Server), right-click, select restart.

## E.3 Class-mapping sample file

Here follows the default configuration for the Users and Groups.

```
<?xml version="1.0"?>
<classes xmlns="http://schemas.opns.be/IDM/Driver/Remedy/ClassMapping">
  <class name="User">
    <operation-map type="get">OpGet</operation-map>
    <operation-map type="set">OpSet</operation-map>
    <operation-map type="get-list">OpGetList</operation-map>
    <operation-map type="create">OpCreate</operation-map>
    <!-- possible values for the type : get, set, get-list, create
    default mapping:
      get : OpGet
      set : OpSet
      get-list : OpGetList
      create : OpCreate
    ignores all other operations on the web service -->
  <attribute-map name="Group_List" type="dn"
    multivalue="true" separator=";" dn-map-to-class="Group"
    dn-map-to-attribute="Group_ID"/>
    <!-- type, possible values : string, dn, int, time -->
    <!-- default multivalue : false, possible values : true, false-->
    <!-- default separator : ; -->
    <!-- dn-map-to-class : used to the association/DN resolution.
    Required if type="dn" -->
    <!-- dn-map-to-attribute : used to the association/DN resolution.
    Required if type="dn" -->
```

```

<attribute-map name="Assigned_To" type="dn"
  dn-map-to-class="User" dn-map-to-attribute="Login_Name"/>
<attribute-map name="Creator" type="dn"
  dn-map-to-class="User" dn-map-to-attribute="Login_Name"/>
  <!-- validate-enum-value : used to disable the validation of an enum
value based on the WSDL coming from ARS Remedy. May be required when a
value is missing within the WSDL (May be required is you see a message
like 'Invalid enumeration value : <value> for <attribute_name>' in the log
file of the driver). Only available if type is string, optional -->
  <attribute-map name="Status" type="string" validate-enum-
value="false"/>
</class>
<class name="Group">
  <operation-map type="get">OpGet</operation-map>
  <operation-map type="set">OpSet</operation-map>
  <operation-map type="get-list">OpGetList</operation-map>
  <operation-map type="create">OpCreate</operation-map>
  <attribute-map name="Group_List" type="dn"
    multivalue="true" separator=";" dn-map-to-class="Group"
    dn-map-to-attribute="Group_ID"/>
  <attribute-map name="Assigned_To" type="dn"
    dn-map-to-class="User" dn-map-to-attribute="Login_Name"/>
  <attribute-map name="lastModifiedBy" type="dn"
    dn-map-to-class="User" dn-map-to-attribute="Login_Name"/>
</class>
</classes>

```



---

# F Trace Levels

The driver supports the following trace levels:

Level	Description
0	Status messages (success/failure/warning)
1	Informational messages about what Identity Manager is doing
2	Adds dumps of the XML that is passed to/from the driver
3	Adds XML dumps after a policy is applied and more verbose output during policy evaluation
4	Informational messages about the application
6	Driver shim debug level, only use it if you want to troubleshoot the shim, this level will display password information in the logs

For information about setting driver trace levels, see to [“Viewing Identity Manager Processes”](#) in the *Identity Manager 4.5 Common Driver Administration Guide*.