Novell

Identity Manager Driver for Remedy Action Request System (ARS)

1.3.2

August 22, 2014

www.novell.com

DRIVER GUIDE

Novell.

Legal Notices

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com
Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

ConsoleOne is a registered trademark of Novell, Inc., in the United States and other countries.
DirXML is a registered trademark of Novell, Inc., in the United States and other countries.
eDirectory is a trademark of Novell, Inc.,
NCP and NetWare Core Protocol are registered trademarks of Novell, Inc.,
NDS and Novell Directory Services are registered trademarks of Novell, Inc., in the United States and other countries.
NetWare is a registered trademark of Novell, Inc., in the United States and other countries.
Novell is a registered trademark of Novell, Inc., in the United States and other countries.
Novell Certificate Server is a trademark of Novell, Inc.,
Novell Client is a registered trademark of Novell, Inc.,

Third-Party Materials

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

Contents

About this Guide

The Identity Manager Driver for ARS Remedy is designed to synchronize data in an eDirectory™ tree with data stored in a ARS Remedy server. This configurable solution allows you to increase productivity and streamline business processes by integrating ARS Remedy and eDirectory.
The guide contains the following sections:

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.

Feedback

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

Documentation Updates

For the most recent version of this document, see the Identity Manager 4.0.2 Drivers documentation Web site (https://www.netiq.com/documentation/idm402/).

Additional Documentation

For documentation on using Identity Manager and the other drivers, see the Identity Manager 4.0.2 Documentation Web site (https://www.netiq.com/documentation/idm402drivers/).

Documentation Conventions

In Novell® documentation, a greater-than symbol (>) is used to separate actions within a step and items within a cross-reference path.
A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.
When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux* or UNIX*, should use forward slashes as required by your software.

1 Overview

The Remedy Action Request System (ARS) is a platform and development environment for automating Service Management business processes.
Identity Manager Driver for Remedy ARS provides data integration between Novell® 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 and then send the information to Remedy ARS, where an account and password are created automatically.
The driver can also synchronize other Remedy data to the directory.

1.1 Supported ARS Remedy Versions

The ARS Driver use the web-service provided by ARS Remedy and you can use it with ARS Server 7.1 and up. This driver for requires the Remedy Mid-tier sever for the web-services.

1.2 ARS Driver Concepts

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

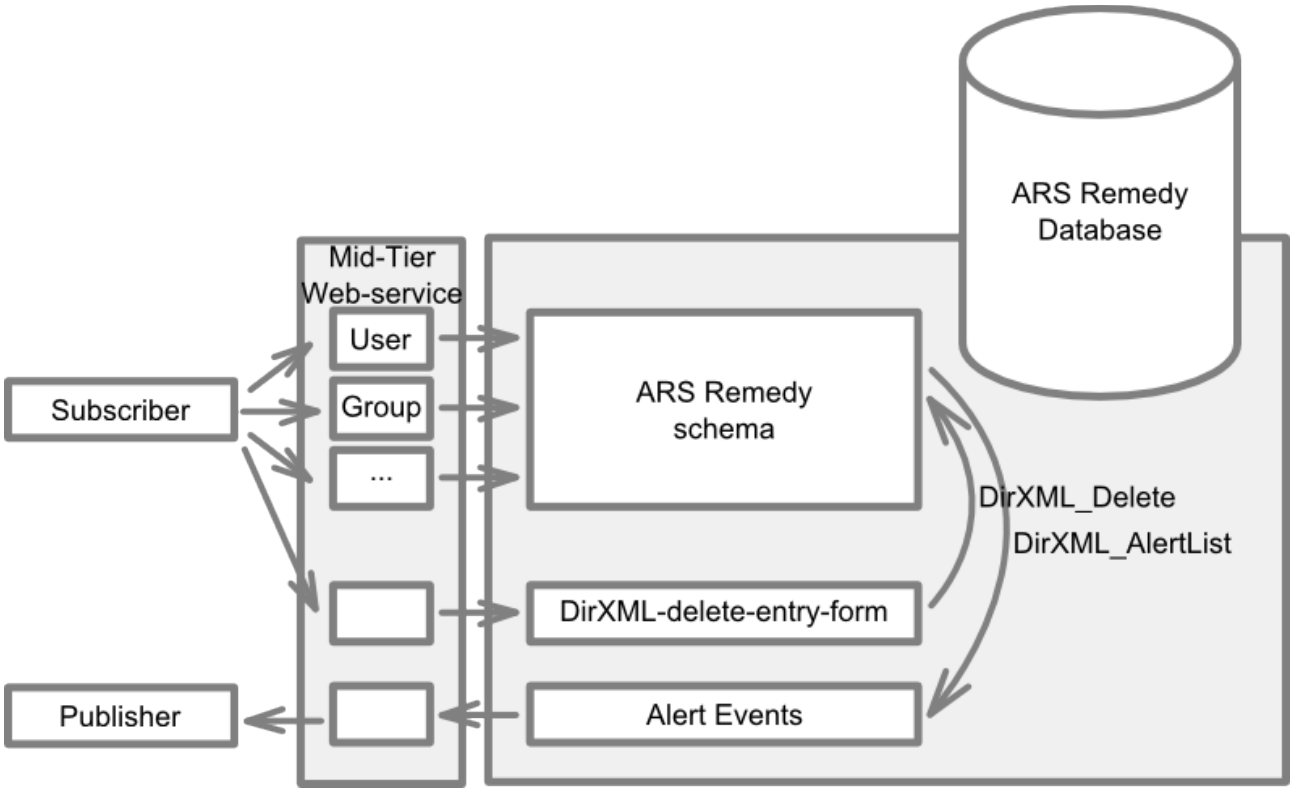
- Section 1.2.1 “Default Data Flow” on page 8
- Section 1.2.2 “Policies” on page 9
- Section 1.2.3 “Driver Components” on page 9

1.2.1 Default Data Flow

A channel is a combination of rules, policies, and filters that is 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 takes events generated in the Identity Vault and sends them to the ARS system.

Publisher Channel
The Publisher channel represents the channel of communication from ARS Remedy to the Identity Vault. The channel takes event generated in ARS Remedy and sends them 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**: Subscriber Creation policy make checks on mandatory attributes and ensure that the object does have a Creator, a License Type and a Full Text License Type. Publisher Creation policy build the Surname for Users base on the Remedy Full Name.
- **Matching**: The default Matching policy logic for the Publisher channel and the Subscriber channel is 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 policies.
- **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 OU name 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 3.5.1 Packages.
- **Driver Files**: `ARSDriver75.jar` is the Java files that direct synchronization between ARS Remedy and the Identity Vault.

- **Web service definitions**: `DirXML-WS.def` is the Remedy ARS web-service definition for the web-services:
  - DirXML_AlertList: Provides an interface to the action performed in ARS Remedy on User and Group objects (like the changelog present in JDBC drivers).
  - DirXML_Delete: Provides an interface to delete objects in ARS Remedy. Default, ARS Remedy does not provide a web-service interface to delete objects. This one allows to delete objects with the help of the DirXML-delete-entry-form and the DirXML-delete-entry-filter (described below).
- **Form definitions**: `DirXML-delete-entry-form.def` is the Remedy ARS form definition for the delete object requests. These objects are technical objects created and cleaned-up by the diver used for the deletion of objects in ARS Remedy. It is a place-holder for a the object form name and the object request ID.
- **Publisher/Subscriber Filters**: `DirXML_Filters.def` is the Remedy ARS Filter that is required for publisher and subscriber operations. It contains three filters:
  - 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 occurs in Remedy ARS and save data in the Alert Form for the publisher. The publisher channel then reads that form to determines the event type and filter the updates based on objects and attributes specified in the Publisher filter in the driver configuration in the Identity Vault.

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 attribute (Views, Tables…) within is WSDL, synchronization for those attributes is by default mapped to string attributes and no reference is made. But, the drivers allow to override this behaviour through a configuration file (see Appendix II. Driver type mapping) so that those attributes can be mapped to a dn.
- Password Synchronization is only supported on Subscriber channel. The driver can sent passwords to Remedy but cannot get passwords back out because Remedy does not support capturing passwords.
- <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:

1.3.1 Local Platforms

A local installation is an installation of the driver on the Metadirectory server. The ARS Remedy driver can be installed on the operating systems supported for the Metadirectory server.
For information about the operating systems supported for the Metadirectory server, see "Metadirectory Server" in "System Requirements" in the *Identity Manager 4.0.2 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 Metadirectory server. For example, you might not want to install the Metadirectory server (Metadirectory engine and Identity Vault) on the same server as ARS Remedy. In this case, you install the Remote Loader and driver on the ARS Remedy server and 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 4.0.2 Installation Guide*.

1.3.3 Entitlements

The ARS Remedy driver does provide entitlement within the Entitlement package. For more information, see Section 3.5.1.3 Entitlements package.
The ARS Remedy driver also supports customized entitlements, you can implement policies for the driver to consume them.

2 Installing the Driver Files

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've chosen.

2.1 Prerequisites

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

2.2 Where to Install the ARS Remedy Driver

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

2.2.1 Local Installation

In a local installation, the ARS Remedy driver is on the same server as the Metadirectory engine, Identity Vault, and ARS Remedy server. When using a local installation you should (highly recommended) configure the Mid-Tier to user SSL for the web services. If SSL is not enabled, passwords will flow in clear text on the network.

2.2.2 Remote Installation

In a remote installation, the ARS Remedy driver is on the ARS Remedy server and the Metadirectory engine and Identity Vault are on a separate Metadirectory server. The driver uses the Remote Loader, also installed on the ARS Remedy server, to communicate with the Metadirectory engine. You should set-up an SSL communication between the Remote-Loader and the Metadirectory.

2.3 Installing the Driver Files

The following sections correspond to the scenarios in Section 2.1, "Where to Install the ARS Remedy Driver", on page 12. Complete the steps for the scenario you've chosen:

2.3.1 Local Installation

Complete the following steps for a local installation. In this scenario, the Metadirectory engine, Identity Vault, ARS Remedy driver, and ARS Remedy are all on the same server.

1. Install the Metadirectory server (Metadirectory engine and drivers) on the ARS Remedy server. For instructions, see "Installing the Metadirectory Server" in the *Identity Manager 4.0.2 Installation Guide*.
2. Deploy and configure the driver (see Section 3, Creating a New Driver)

2.3.2 Remote Installation on a ARS Remedy Server

Complete the following steps for a remote installation on a ARS Remedy server. In this scenario, the Metadirectory engine and Identity Vault are on one server and the Remote Loader and ARS Remedy driver are on a separate ARS Remedy server.

1. If you have not already done so, install a Metadirectory server. For instructions, see "Installing the Metadirectory Server" in the *Identity Manager 4.0.2 Installation Guide*.
2. Install the Remote Loader on the ARS Server server. For instructions, see "Installing the Remote Loader" in the *Identity Manager 4.0.2 Installation Guide*.
   You install the ARS Remedy driver as part of the Remote Loader installation.
3. Deploy and configure the driver (see Section 3, Creating a New Driver)

3 Creating a New Driver

After the ARS Remedy driver files are installed on the server where you want to run the driver (see Chapter 2, “Installing the Driver Files,” on page 12), you can create the driver in the Identity Vault. You do so by importing the basic driver configuration file and then modifying the driver configuration to suit your environment. The following sections provide instructions:

3.1 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 3.3, “Configuring the IDM Notifier Filter on page 14”).

3.2 Installing the IDM Filters, Form, Web-service in Remedy

The publisher channel of the ARS Remedy driver requires a Remedy Filter to be installed on the ARS Remedy server.

1. Login with 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 `DirXML-delete-entry-form.def` located in <idminstall lcoation>\drivers\remedy\tools.
6. Click *Next*.
7. Select the all presented objects.
8. Click *Finish*.
9. Repeat steps 2-8 with the filters (`DirXML_Filters.def`) and the web-service (`DirXML-WS.def`).
10. Check that the User and the group web-service are already 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 you don't find one of them, import it (repeat steps 2-8) with the `User-Group-WS.def`

3.3 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 Notify 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.
If you want to publish other ARS Remedy Forms to the Identity Vault, you need to change the IDM Notifier Filter.

3.3.1 Editing the IDM Notifier Filter to match the ARS Remedy Account

1. Login with BMC Remedy Developer Studio.
2. Browse and double-click on the DirXML Notifier Filter in the left panel.
3. Deploy the *Run If Qualification* sub-panel.
4. Change *“dirxml”* with the *Login Name* created in Section 3.1, “Creating an ARS Remedy Account” on page 14.
5. Deploy the *If Actions* sub-panel.
6. Change *dirxml* in the *User* filed with the *Login Name* created in Section 3.1, “Creating an ARS Remedy Account” on page 14.
7. Click on *File* > *Save*.

3.3.2 Editing the IDM Notifier Filter to change the published ARS Remedy Forms

1. Login with BMC Remedy Developer Studio.
2. Browse and double-click on the DirXML Notifier Filter in the left panel.
3. Deploy the Associated Forms sub-panel.
4. Right-click to remove or add Associated Form.
5. Click on *File* > *Save*.

3.4 Configuring the Web service

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

1. Login with 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. Deploy 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).

3.5 Creating the Driver in Designer

You create the ARS Remedy driver by importing the driver's package. After you've created and configured the driver, you need to deploy it to the Identity Vault and start it.

3.5.1 Packages

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

3.5.1.1 Base package

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

3.5.1.2 Password package

This package adds the password synchronization for the users, from the Identity Vault to ARS Remedy only.

3.5.1.3 Entitlements package

This package adds two entitlements to the driver:

- User Account: granting or revoking this entitlement creates or delete (or disable) 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.

3.5.1.4 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.

3.5.1.5 Managed System Information package

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

3.5.2 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 the wanted optional packages (see 3.5.1 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, select here the container for the users, otherwise, select the base container for the users. In case of a non flat placement, you will 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 users, select here the container for the users, otherwise, select the base container for the users. 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 login of the user for the driver. This is the user you created in Section 3.1. 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 (only recommended), 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 of the web-service. This name can thus 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. Can be empty.
                3. *ARS Locale information*: Fill in the locale that will be used to communicate with the web-service. Can be empty.
                4. *ARS Timezone information*: Fill in the timezone that will be used to communicate with the web-service. 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 whose name begins with "ars" (case-insensitive) and 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 III. 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 objects in ARS. If *no* is selected, the DirXML_AlertList web-service must be available (see Section 3.2. Installing the IDM Filters, Form, 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 like VMWare etc... In virtual environment there can be issues with time tracking, this parameter allows you to correct this to some extends. See Chapter 5 Troubleshooting the Driver on page 24. In milliseconds.
   4. *Heartbeat interval*: The heartbeat interval (in minutes) of the subscriber.
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 3.2. Installing the IDM Filters, Form, 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. It can be the driver user.
   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 4.0.2 Remote Loader Guide*). If you select yes, please fill-in the required informations:

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 there is an SSL connection 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*: When creating a user in the target system, when the distribution password is not available, the driver can choose to **Force presence** (this veto the event, the User creation is so delayed until the distribution password is present) or to **Use default password** (a default value used 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 showed and can be edited.
                    1. *Identifiers*: List of account identifiers. This list is in the application namespace.
                    2. *Object class*: List of object class 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 his 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 you turn on role mapping here, this driver is be visible to the role mapping administrator.
            1. *Enable Role Mapping for User Account*: **Yes**/**No** this allows to enable/disable role mapping for the User Account entitlement.
            2. *Enable Role Mapping for Group Membership*: **Yes**/**No** this allows to enable/disable role mapping for the Group Membership entitlement.
        2. **No**: Role mapping is disabled for all entitlements
    2. *Enable Resource Mapping*:
        1. **Yes**: If you turn on resource mapping here, this driver is available for resource mapping in the roles-based provisioning module.
            1. *Enable Resource Entitlement for User Account*: **Yes**/**No** this allows to enable/disable resource mapping for the User Account entitlement.
            2. *Enable Resource Entitlement for Group Membership*: **Yes**/**No** this allows to enable/disable 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. Select a user object (not a role, group, or container).
        2. *Application owner*: Specify the application owner of the managed system. Select 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 end 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 must review and modify (if necessary) the driver's default configuration settings, its policies, the schema mapping and the filter. After completing the configuration tasks, continue with the next section, Deploying the Driver.

3.5.3 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 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.
    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, Admin and DriversUser) 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*.

3.5.4 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 4.0.2 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 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 4.0.2 Common Driver Administration Guide*.

5 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. Fatal error so the driver will shutdown.
- **XML parsing error :: Can't parse XML for class … from …** : The specified web service is either unavailable or misspelled.
- **No schemas to sync**: No schema names were supplied to the driver. Check the driver configuration in 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 national 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 done only the other 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.
- **Issue with HTTP Error 500: Internal Server Error**: When using ARS-Remedy with Mid-tier on an 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 can not 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 Mid-tier lies on.
  - Double-click on "*Error Pages*"
  - Click on "*Edit Features Settings...*" on the right pannel.
  - Select "*Detailed errors*" and click on OK.

  The other 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.

6 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 4.0.2 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.

6.1 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 on 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:

6.1.1 Driver Module

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

Options	Description
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 java class name is: `be.opns.nds.dirxml.driver.ars.ARSDriverShim`.
Native	This option is not used with the Remedy driver.
Connect to Remote Loader	Used when the driver is connecting remotely to the connected system.

Options	Description
	Designer includes two suboptions: • *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. • *Remote Loader Client Configuration for Documentation*: Includes information on the Remote Loader client configuration when Designer generates documentation for the driver.

6.1.2 Driver Object Password

Option	Description
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 or the remote driver does not run. This password is used by the Remote Loader to authenticate itself to the remote driver shim.

6.1.3 Authentication

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

Option	Description
Authentication ID or *User ID*	Specify a user application ID. This ID is used to pass Identity Vault subscription information to the application. Example: `dirxml`
Authentication Context or *Connection Information*	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 <Connection Information>/<Object class> 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: https://<server-mid-tier>/arsys/WSDL/public/<server-ars>
Remote Loader Connection Parameters ok *Host name*	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`, where the hostname is

Option	Description
Port *KMO* *Other parameters*	the IP address of the application server running the Remote Loader server and the port is the port the Remote Loader is listening on. The default port for the Remote Loader is 8090. The `kmo` entry is optional. It is only used when there is an SSL connection between the Remote Loader and the Metadirectory engine. Example: `hostname=10.0.0.1 port=8090 kmo=IDMCertificate`
Driver Cache Limit (kilobytes) or 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.
Application Password or Set Password	Specify the password for the user object listed in the Authentication ID field.
Remote Loader Password or Set 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.

6.1.4 Startup Option

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

Option	Description
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 only applies if the driver is deployed and was previously disabled. If this is not selected, the driver re-synchronizes the next time it is started.

6.1.5 Driver Parameters

The Driver Parameters section lets you configure the driver-specific parameters. When you change

driver parameters, you tune driver behaviour 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 can not be empty.
    2. *ARS Authentication information*: Specify the ARS Authentication information for the web service authentication. Can be empty.
    3. *ARS Locale information*: Specify the ARS Locale information for the web service authentication. Can be empty.
    4. *ARS Timezone information*: Specify the ARS Timezone information for the web service authentication. 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 whose name begins with "ars" (case-insensitive) and 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. 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. In virtual environment there can be issues with time tracking, this parameter allows you to correct this to some extends. See Chapter 5 Troubleshooting the Driver on page 24.
    4. *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.
3. 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.

6.2 Driver Global Configuration Values (GCV)

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

6.2.1 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

6.2.2 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 presence on subscriber channel? If the selected option is f**orce presence** and not distribution password is set for the user, the operation will be vetoed. Otherwise, if the **use default password** option is selected, when the distribution password is not available on user creation, the surname is used as password in the target system.

6.2.3 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 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 you turn on role mapping here, this driver is be 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 you turn on resource mapping here, this driver is 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 are being added below the User Account entitlement element in the EntitlementConfiguration resource object.
2. *Group extensions*: Children of the <entitlement-extensions> node are being added below the Group entitlement element in the EntitlementConfiguration resource object.

6.2.4 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. Select a user object (not a role, group, or container).
   2. *Application Owner*: Specify the application owner of the managed system. Select 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 (auto-generated, do not change!): these information are generated by the driver itself and are overwritten on driver reboot, do not change them.

6.2.5 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 acount 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.

7 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 leaks password in the logs

For information about setting driver trace levels, see to "Viewing Identity Manager Processes" in the *Identity Manager 4.0.2 Common Driver Administration Guide*.

Appendix

I Upgrade procedure from previous version

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.

1 Configuring ARS Remedy web services

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

- 2.1 Prerequisites,
- 3.2 Installing the IDM Filters, Form, Web-service in Remedy,
  - While importing the objects in BMC Remedy Developer Studio, make sure to select "Replace Objects on the Destination Server".
- 3.3 Configuring the IDM Notifier Filter and
- 3.4 Configuring the Web service.

2 Installation of the new shim

If the new driver shim is not already installed, copy into 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*:
      ```
      # 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.

3 Update of the driver object

In Designer:

1. Rename or save the current driver. Rename is prefered 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 3.6 Creating the Driver in Designer.
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 new driver:
   1. On the driver, click on "Live" > "Restart Driver"

II Uninstalling the driver

1 Deleting Identity Manager Driver Objects

When you are deleting Novell 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:

6. In Novell iManager, click *Identity Manager* > *Identity Manager Overview*.
7. Select a driver set.
8. On the Identity Manager Overview page, click *Delete Driver*.
9. Select the driver that you want to delete, then click OK.

2 Deleting the User, Filters, Form, Web-service from ARS Remedy

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

1. Delete the filters created by the `DirXML_Filters.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 3.1.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*.

III Driver type mapping

Because 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 mutivalued attribute to the format handled by the web-service,
- do the resolution of "foreign key" (i.e. resolve the association).

1 Class-mapping XML file format

This mapping is configured through an XML file put in a jar in the classpath of eDirectory. A default mapping for the User and the Group is bundled with the driver. Only one configuration is allowed by the driver. So, 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 Appendix II Section 3 Class-mapping sample file).

The XML file is a list of class/web-service, for each classes, there are two type 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`: the service to query for the content of one form (must be a *Get Operation* in Developer Studio),
    - `set`: the service to set the content of one form (must be a *Set Operation* in Developer Studio),
    - `get-list`: the service to query on one form (must be a *Get List Operation* in Developer Studio),
    - `create`: 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 an 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`: to map the attribute to a dn. The value is a reference to another object.
    - `string`: no mapping is done
    - `int`: to map the attribute to an integer
    - `time`: to map the attribute to a time
  - **multivalue**: indicates if the attribute is multivalued (for the web-service). The default value is `false`.
    - `true`
    - `false`
  - **separator**: specify it 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 the object is referring to. 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, not the form name in ARS Remedy, nor the class name in the Metadirectory.
  - **dn-map-to-attribute**: specify the attribute the object is referring to. 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 of 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 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 and the attribute is an enumeration. This attribute is optional.

2 Class-mapping installation procedure

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

3. Create the XML file according to your needs.
4. Create a jar file (the filename must start with "ars") with the XML configuration file in META-INF\<xml-file-name>.
   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`
5. 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 driverset
         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*.
6. 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.
7. Restart the eDirectory service:
   1. For Linux*:
      ```
      # 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.

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>
```