

Novell

Identity Manager Driver for Remedy Action Request System (ARS)

1.2

March 16, 2010

DRIVER GUIDE

www.novell.com



Novell.

Legal Notices

Novell, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose.

Further, Novell, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

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

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

Copyright © 2005 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at <http://www.novell.com/company/legal/patents/> and one or more additional patents or pending patent applications in the U.S. and in other countries.

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

| | |
|---|----|
| 1 Overview..... | 8 |
| 1.1 Supported ARS Remedy Versions..... | 8 |
| 1.2 ARS Driver Concepts..... | 8 |
| 1.2.1 Default Data Flow..... | 8 |
| 1.2.2 Policies..... | 9 |
| 1.2.3 Driver Components..... | 9 |
| 1.2.4 Limitations..... | 10 |
| 1.3 Support for Standard Driver Features..... | 10 |
| 1.3.1 Local Platforms..... | 10 |
| 1.3.2 Remote Platforms..... | 10 |
| 1.3.3 Entitlements..... | 10 |
| 2 Installing the Driver Files..... | 11 |
| 2.1 Where to Install the ARS Remedy Driver..... | 11 |
| 2.1.1 Local Installation..... | 11 |
| 2.1.2 Remote Installation..... | 11 |
| 2.2 Installing the Driver Files..... | 11 |
| 2.2.1 Local Installation..... | 11 |
| 2.2.2 Remote Installation on a ARS Remedy Server..... | 12 |
| 2.3 Copying files to Required Locations..... | 12 |
| 2.3.1 Windows ARS Remedy Server..... | 12 |
| 2.3.2 Linux ARS Remedy Server..... | 12 |
| 3 Creating a New Driver..... | 13 |
| 3.1 Creating an ARS Remedy Account..... | 13 |
| 3.2 Installing the IDM Notifier Filter..... | 13 |
| 3.3 Configuring the IDM Notifier Filter..... | 14 |
| 3.3.1 Editing the IDM Notifier Filter to match the ARS Remedy Account used by the driver | 14 |
| 3.3.2 Editing the IDM Notifier Filter to change the published ARS Remedy Forms..... | 14 |
| 3.4 Creating the Driver in Designer..... | 14 |
| 3.4.1 Importing the Driver Configuration File..... | 15 |
| 3.4.2 Configuring the Driver..... | 15 |
| 3.4.3 Deploying the Driver..... | 16 |
| 3.4.4 Starting the Driver..... | 17 |
| 3.5 Creating the Driver in iManager..... | 17 |
| 3.5.1 Importing the Driver Configuration File..... | 18 |
| 3.5.2 Configuring the Driver..... | 20 |
| 3.5.3 Starting the Driver..... | 21 |
| 4 Managing the Driver..... | 23 |
| 5 Troubleshooting the Driver..... | 24 |
| 6 Driver Properties..... | 26 |
| 6.1 Driver Configuration..... | 26 |
| 6.1.1 Driver Module..... | 26 |
| 6.1.2 Driver Object Password (iManager Only)..... | 27 |
| 6.1.3 Authentication..... | 27 |
| 6.1.4 Startup Option..... | 28 |
| 6.1.5 Driver Parameters..... | 29 |
| 7 Trace Levels..... | 30 |

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:

- [Chapter 1, “Overview” on page 7](#)
- [Chapter 2, “Installing the Driver Files” on page 10](#)
- [Chapter 3, “Creating a New Driver” on page 12](#)

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 3.6.1 Drivers documentation Web site (<http://www.novell.com/documentation/idm36drivers/index.html>).

Additional Documentation

For documentation on using Identity Manager and the other drivers, see the Identity Manager 3.6.1 Documentation Web site (<http://www.novell.com/documentation/idm36drivers/index.html>).

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 1.0 for Remedy ARS provides data integration between Novell® eDirectory™ and Remedy ARS.

The driver uses the Remedy Java* API to access 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 synchronise other Remedy data to the directory.

1.1 Supported ARS Remedy Versions

Since there is an API break between ARS 7.0 and ARS 7.1, there is two different shim for this driver.

You can use the ARS Remedy driver 7.0 with ARS Server 5.x, 6.x and 7.0.

You can use the ARS Remedy driver 7.1 with ARS Server 7.1 and up.

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 7](#)
- [Section 1.2.2 “Policies” on page 8](#)
- [Section 1.2.3 “Driver Components” on page 8](#)

1.2.1 Default Data Flow

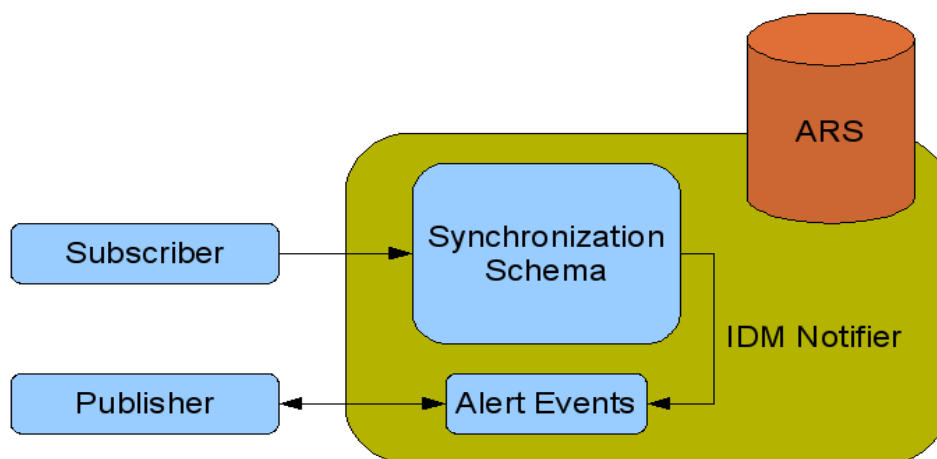
A channel is a combination of rules, policies, and filters that is used to synchronize data between two systems. The Subscriber and Publisher channels describe the direction in which the data flows. The Subscriber and Publisher channels act independently; actions in one channel are not affected by what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

- **Default Driver Configuration File:** A file you can import to set up default rules, style sheets, and driver parameters. The driver configuration files included with this driver are `RemedyARS71-IDM3_5_0-V1.xml` and `RemedyARS-IDM3_5_0-V1.xml`, with their accompanying `.xlf` files (for any language other than English).
- **Driver Files:** `ARSDriver71.jar` and `ARSDriver.jar` are the Java files that direct synchronization between ARS Remedy and the Identity Vault.
- **Publisher Notification Filters:** `IDM_Notifier.xml` is the Remedy ARS Filter that is required for publisher operations. 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. Referential attribute (Views, Tables...) synchronization isn't supported.
- Password Synchronization is only supported on Subscriber channel. The driver can send 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:

- [Section 1.3.1 “Local Platforms” on page 9](#)
- [Section 1.3.2 “Remote Platforms” on page 9](#)
- [Section 1.3.3 “Entitlements” on page 9](#)

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 3.6.1 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 3.6.1 Installation Guide*.

1.3.3 Entitlements

The ARS Remedy driver can be configured to use entitlements to manage user accounts and group membership in the ARS Remedy. When using entitlements, this driver works in conjunction with external services, such as the User Application with workflow or role-based provisioning or the Entitlements Service driver, to manage entitlement functionality.

The ARS Remedy driver also supports customized entitlements, if there are policies created for the driver to consume.

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.

- [Section 2.1, “Where to Install the ARS Remedy Driver” on page 10](#)
- [Section 2.2, “Installing the Driver Files” on page 10](#)
- [Section 2.3, “Copying files to Required Location” on page 11](#)

2.1 Where to Install the ARS Remedy Driver

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

- [Section 2.1.1, “Local Installation” on page 10](#)
- [Section 2.1.2, “Remote Installation” on page 10](#)

2.1.1 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.

You should always use the Remote Loader with the ARS Remedy driver, even in a local installation like this one. Using the Remote Loader has the following advantages:

- An exception in the driver caused by the ARS Remedy APIs doesn't cause the Identity Vault (eDirectory™) to shut down.
- The driver has its own Java memory space, which helps avoid heap issues.

2.1.2 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.

2.2 Installing the Driver Files

The following sections correspond to the scenarios in [Section 2.1, “Where to Install the ARS Remedy Driver”, on page 10](#). Complete the steps for the scenario you've chosen:

- [Section 2.2.1, “Local Installation” on page 10](#)
- [Section 2.2.2, “Remote Installation on a ARS Remedy Server” on page 11](#)

2.2.1 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*

3.6.1 Installation Guide.

2. If you want to use the Remote Loader with the driver, install the Remote Loader on the ARS Remedy server. For instructions, see “[Installing the Remote Loader](#)” in the *Identity Manager 3.6.1 Installation Guide*.
3. Continue with [Section 2.3, “Copying files to the Required Locations,” on page 11](#) to complete installation of the files.

2.2.2 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 3.6.1 Installation Guide*.
2. Install the Remote Loader on the ARS Server server. For instructions, see “[Installing the Remote Loader](#)” in the *Identity Manager 3.6.1 Installation Guide*.

You install the ARS Remedy driver as part of the Remote Loader installation.

3. Continue with [Section 2.3, “Copying files to the Required Locations,” on page 11](#) to complete installation of the files.

2.3 Copying files to Required Locations

After the ARS Remedy driver files are installed, you need to copy the Remedy ARS JAR API files to the driver directory.

- [Section 2.3.1, “Windows ARS Remedy Server” on page 11](#)
- [Section 2.3.2, “Linux ARS Remedy Server” on page 11](#)

2.3.1 Windows ARS Remedy Server

1. Copy all the jar files (*.jar) from \Program Files\BMC Software\ARSystem\Arserver\api\lib to \Novell\RemoteLoader\lib or \Novell\NDS\lib (without a Remote Loader).
2. Make sure that the ARS Remedy shared libraries directory (for example, C:\Program Files\BMC Software\ARSystem) is in the Windows system path, and reboot the computer to make sure this step becomes effective.

Without this directory in the Windows system path, the JVM* might have difficulty locating the ARS Remedy shared libraries required by arapiXX.jar, such as arjniXX.dll (with XX being the ARS Remedy server version).

2.3.2 Linux ARS Remedy Server

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 10](#)), 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:

- [Section 3.1, “Creating an ARS Remedy Account” on page 12](#)
- [Section 3.2, “Installing the IDM Notifier Filter” on page 12](#)
- [Section 3.3, “Configuring the IDM Notifier Filter” on page 13](#)
- [Section 3.4, “Creating the Driver in Designer” on page 13](#)
- [Section 3.5, “Creating the Driver in iManager” on page 16](#)

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*, *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 13”](#)).

3.2 Installing the IDM Notifier Filter

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 `IDM_Notifier.xml` or `IDM_Notifier71.xml` located in `<idminstall lcoation>\drivers\remedy\tools`.
6. Click *Next*.
7. Select the *DirXML Notifier* Filter.
8. Click *Finish*.

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 used by the driver

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 12](#).
5. Deploy the *If Actions* sub-panel.
6. Change *dirxml* in the *User* field with the *Login Name* created in [Section 3.1, “Creating an ARS Remedy Account” on page 12](#).
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 Creating the Driver in Designer

You create the ARS Remedy driver by importing the driver’s basic configuration file and then modifying the configuration to suit your environment. After you’ve created and configured the driver, you need to deploy it to the Identity Vault and start it.

- [Section 3.4.1, “Importing the Driver Configuration File” on page 14](#)
- [Section 3.4.2, “Configuring the Driver” on page 14](#)
- [Section 3.4.3, “Deploying the Driver” on page 15](#)
- [Section 3.4.4, “Starting the Driver” on page 16](#)

3.4.1 Importing the Driver Configuration File

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 Driver Configuration list, select *Remedy*, then click *Run*.
4. On the Import Information Requested page, fill in the following fields:

Driver Name: Specify a name that is unique within the driver set.

Driver is Local/Remote: Select *Local* if this driver will run on the Metadirectory server without using the Remote Loader service. Select *Remote* if you want the driver to use the Remote Loader service, either locally on the Metadirectory server or remotely on another server.

5. (Conditional) If you chose to run the driver remotely, click *Next*, then fill in the fields listed below. Otherwise, skip to [Step 6](#).

Remote Host Name and Port: Specify the host name or IP address of the server where the driver's Remote Loader service is running.

Driver Password: Specify the driver object password that is defined in the Remote Loader service. The Remote Loader requires this password to authenticate to the Metadirectory server.

Remote Password: Specify the Remote Loader's password (as defined on the Remote Loader service). The Metadirectory engine (or Remote Loader shim) requires this password to authenticate to the Remote Loader

6. Click *Next* to import the driver configuration.

At this point, the driver is created from the basic configuration file. 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.

7. To review or modify the default configuration settings, click *Configure*, then continue with the next section, [Configuring the Driver](#).

or

To skip the configuration settings at this time, click *Close*. When you are ready to configure the settings, continue with [Configuring the Driver](#).

3.4.2 Configuring the Driver

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

- Ensure that the driver can authenticate to ARS Remedy: Make sure that you've established a Remedy user account for the driver (see [Section 3.1, "Creating an ARS Remedy Account," on page 12](#)) and the correct authentication information is defined for the driver parameters (see [Section 6.1.3, "Authentication," on page 27](#)).
- Configure the driver parameters: There are many settings that can help you customize and optimize the driver. The settings are divided into categories such as Driver Configuration, Engine Control Values, and Global Configuration Values (GCVs). Although it is important for you to understand all of the settings, your first priority should be to configure the driver

parameters located on the Driver Configuration page. The driver parameters control general settings such as the synchronized Forms accessed by the driver, Subscriber channel settings, and Publisher channel settings. For information about the driver parameters, see [Section A.1.5, “Driver Parameters,” on page 29](#).

- Configure the driver filter: Modify the driver filter to include the object classes and attributes you want synchronized between the Identity Vault and ARS Remedy.
- Configure policies: Modify the policies as needed. For information about the default configuration policies, see [“Policies” on page 8](#).
- Configure password synchronization: The basic driver configuration is set up to support password synchronization through Universal Password. If you don’t want this setup, see [“Configuring Password Flow”](#) in the *Identity Manager 3.6.1 Password Management Guide*.

After completing the configuration tasks, continue with the next section, [Deploying the Driver](#).

3.4.3 Deploying the Driver

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

1. In Designer, open your project.
2. In the Modeler, right-click the driver icon or the driver line, then select *Live > Deploy*.
3. If you are authenticated to the Identity Vault, skip to [Step 5](#); otherwise, specify the following information:
 - **Host:** Specify the IP address or DNS name of the server hosting the Identity Vault.
 - **Username:** Specify the DN of the user object used to authenticate to the Identity Vault.
 - **Password:** Specify the user’s password.
4. Click *OK*.
5. Read 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*.

3.4.4 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:
 - **Windows:** Open the Remote Loader console on the driver's server, select the driver in the list, then click *Start*.
 - **Linux, AIX, or Solaris:** At the server command line, add the driver object password and remote loader password to the Remedy ARS driver startup script. For example:

```
cd driver_script_directory
./rdxml.startremedy -sp driver_password
remote_loader_password
```

These passwords must be the same as the **Driver Object Password** and **Remote Loader Password** you specified when configuring the driver. The `driver_script_directory` should be the directory where you placed the files (see [Section 2.3.3, "Linux, AIX, or Solaris," on page 19](#)).

Use `rdxml.startremedy` to start the Remote Loader for the driver.

For example,

```
cd driver_script_directory
./rdxml.startremedy
```

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

3.5 Creating the Driver in iManager

You create the ARS Remedy driver by importing the driver's basic configuration file and then modifying the configuration to suit your environment. After you've created and configured the driver, you need to start it.

- [Section 3.5.1, "Importing the Driver Configuration File" on page 17](#)
- [Section 3.5.2, "Configuring the Driver" on page 21](#)
- [Section 3.5.3, "Starting the Driver" on page 22](#)

3.5.1 Importing the Driver Configuration File

1. In iManager, click  to display the Identity Manager Administration page.
2. In the Administration list, click *Import Configuration* to launch the Import Configuration wizard.
3. Follow the wizard prompts, filling in the requested information (described below) until you reach the Summary page.

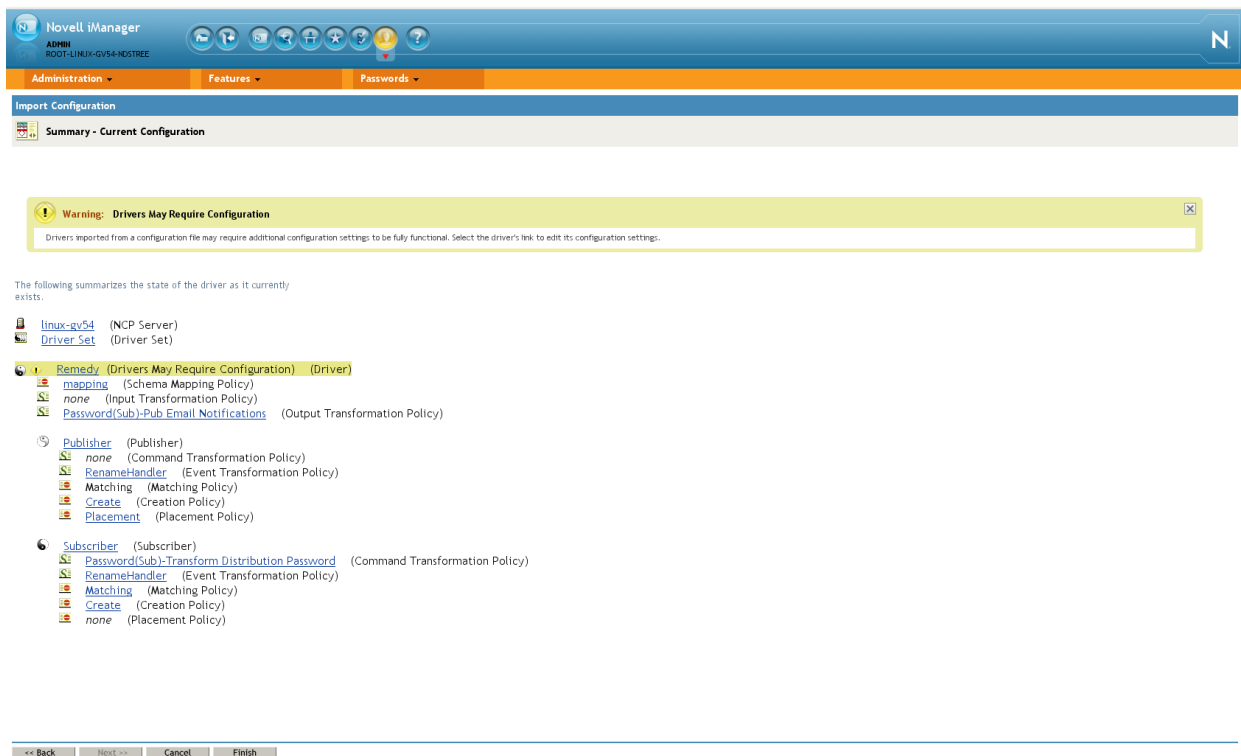
| Prompt | Description |
|---|--|
| Where do you want to place the new driver? | You can add the driver to an existing driver set, or you can create a new driver set and add the driver to the new set. If you choose to create a new driver set, you are prompted to specify the name, context, and server for the driver set. |
| Import a configuration into this driver set | Use the default option, Import a configuration from the server (.XML file). In the Show field, select Identity Manager 3.5 configurations. In the Configurations field, select the Remedy file. |
| Driver name | Type a name for the driver. The name must be unique within the driver set. |
| Driver is Local/Remote | Select <i>Local</i> if this driver will run on the Metadirectory server without using the Remote Loader service. Select <i>Remote</i> if you want the driver to use the Remote Loader service, either locally on the Metadirectory server or remotely on another server. |
| Remote Host Name and Port | This applies only if the driver is running remotely. Specify the host name or IP address of the server where the driver's Remote Loader service is running. |
| Driver Password | This applies only if the driver is running remotely. Specify the driver object password that is defined in the Remote Loader service. The Remote Loader requires this password to authenticate to the Metadirectory server. |
| Remote Password | This applies only if the driver is running remotely. Specify the Remote Loader's password (as |

| Prompt | Description |
|---------------|---|
| | defined on the Remote Loader service). The Metadirectory engine (or Remote Loader shim) requires this password to authenticate to the Remote Loader |

| Prompt | Description |
|------------------------------|---|
| Define Security Equivalences | 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. |

| Prompt | Description |
|------------------------------|--|
| Exclude Administrative Roles | You should exclude any administrative User objects (for example, Admin and DriversUser) from synchronization. |
| Authentication id | Enter the Remedy User ID used to authenticate to ARS Remedy server. |
| Authentication Password | Enter the password for the Remedy user ID that this driver uses when authenticating to ARS Remedy (for the above user ID file). |
| Authentication Server | Specify the name (or IP) of the ARS Remedy Server. If the ARS Remedy server is not configured to use RPC port-mapping, you need to specify the TCP port (ie: remedy:1234) |
| Polling Interval (secondes) | Specify the polling interval used by the Publisher to check for changes in ARS Remedy. |
| Polling Precision | If the driver is running in a Virtual environment (like Vmware), there can be an issue with the polling interval because time is drifting. This value allows you to correct it. |
| Synchronized Schema | Specify the Remedy ARS Remedy Froms you want to synchronize with the driver separated by a semi-colon (ie: User;Group). |
| Base container in eDirectory | Specify the eDirectory container where Users and G |

When you finish providing the information required by the wizard, a Summary page similar to the following is displayed.



4. To modify the default configuration settings, click the linked driver name, then continue with the next section, [Configuring the Driver](#).

or

To skip the configuration settings at this time, click Finish. When you are ready to configure the settings, continue with [Configuring the Driver](#).

3.5.2 Configuring the Driver

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

- Ensure that the driver can authenticate to ARS Remedy: Make sure that you've established a Remedy user account for the driver (see [Section 3.1, "Creating an ARS Remedy Account," on page 12](#)) and the correct authentication information is defined for the driver parameters (see [Section 6.1.3, "Authentication," on page 27](#)).
- Configure the driver parameters: There are many settings that can help you customize and optimize the driver. The settings are divided into categories such as Driver Configuration, Engine Control Values, and Global Configuration Values (GCVs). Although it is important for you to understand all of the settings, your first priority should be to configure the driver parameters located on the Driver Configuration page. The driver parameters control general settings such as the synchronized Forms accessed by the driver, Subscriber channel settings, and Publisher channel settings. For information about the driver parameters, see [Section 6.1.5, "Driver Parameters," on page 29](#).
- Configure the driver filter: Modify the driver filter to include the object classes and attributes you want synchronized between the Identity Vault and ARS Remedy.
- Configure policies: Modify the policies as needed. For information about the default

configuration policies, see [“Policies” on page 8](#).

- Configure password synchronization: The basic driver configuration is set up to support password synchronization through Universal Password. If you don't want this setup, see [“Configuring Password Flow”](#) in the *Identity Manager 3.6.1 Password Management Guide*.

After completing the configuration tasks, continue with the next section, [Starting the Driver](#).

3.5.3 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:
 - **Windows:** Open the Remote Loader console on the driver's server, select the driver in the list, then click *Start*.
 - **Linux, AIX, or Solaris:** At the server command line, add the driver object password and remote loader password to the Remedy ARS driver startup script. For example:


```
cd driver_script_directory
./rdxml.startremedy -sp driver_password
remote_loader_password
```

These passwords must be the same as the **Driver Object Password** and **Remote Loader Password** you specified when configuring the driver. The `driver_script_directory` should be the directory where you placed the files (see [Section 2.3.3, “Linux, AIX, or Solaris,” on page 19](#)).

Use `rdxml.startremedy` to start the Remote Loader for the driver.

For example,

```
cd driver_script_directory
./rdxml.startremedy
```

2. In iManager, click  to display the Identity Manager Administration page.
3. Click *Identity Manager Overview*.
4. Browse to and select the driver set object that contains the driver you want to start.
5. Click the driver set name to access the Driver Set Overview page.
6. Click the upper right corner of the driver, then click *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

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 3.6.1 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.

- **No authentication information:** No login/password/server were supplied to the driver. Check the driver configuration in iManager. Fatal error so the driver will shutdown.
- **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.
- **Unable to connect to ARS server:** The driver didn't successfully log in. Check the driver authentication configuration (login name, password and context)
- **Error trying to build Entry DN:** An error occurred when the driver tried to build the DN for the Entry. Since the driver installs the required Fields to handle the DN, this error should happen only if the 'eDir Container DN' Field is undefined for an Entry.
- **No SchemaDef was found for xxxx:** The driver tried to get information for an unknown Schema. Check that all Classes in Pub/Sub Filter are mapped and check the driver parameter '*Schemas to synchronize*' in the Driver Configuration.
- **Problem with natives libraries:** The driver can't access the Remedy libraries. Check that the Remedy .dll files are in the system path (usually /WINNT/System32 for Windows and /usr/lib for Linux)
- **No events published:** Check that the IDM notifier is installed correctly on the ARS server.
- **Issues when synchronising national characters:**

Install the driver in a remote loader and add the following lines in the beginning of the dirxml_jremote script.

```
LANG=en.US.ISO-8859-1 (or any other character encoding)
```

```
export LANG
```

- **Issues with polling interval cycle in VM environment:**

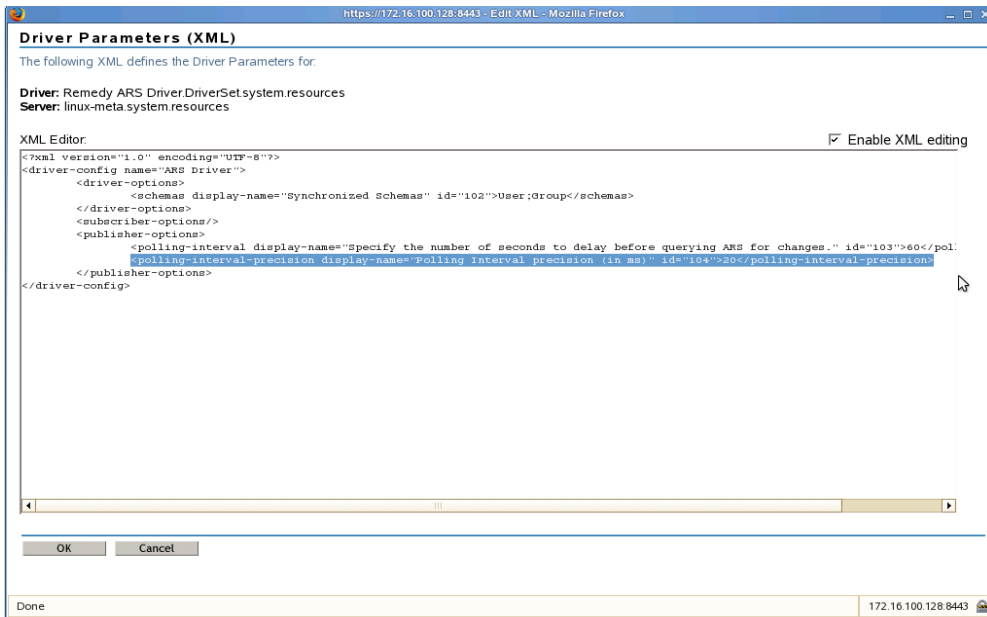
VM time precision can interfere with the polling process (ie: the polling is done only the other cycle), to correct this behaviour, a special publisher option is available.

Add the following tag to the publisher-options.

```
<polling-interval-precision display-name="Polling Interval Precision (in ms)">20</polling-interval-precision>
```

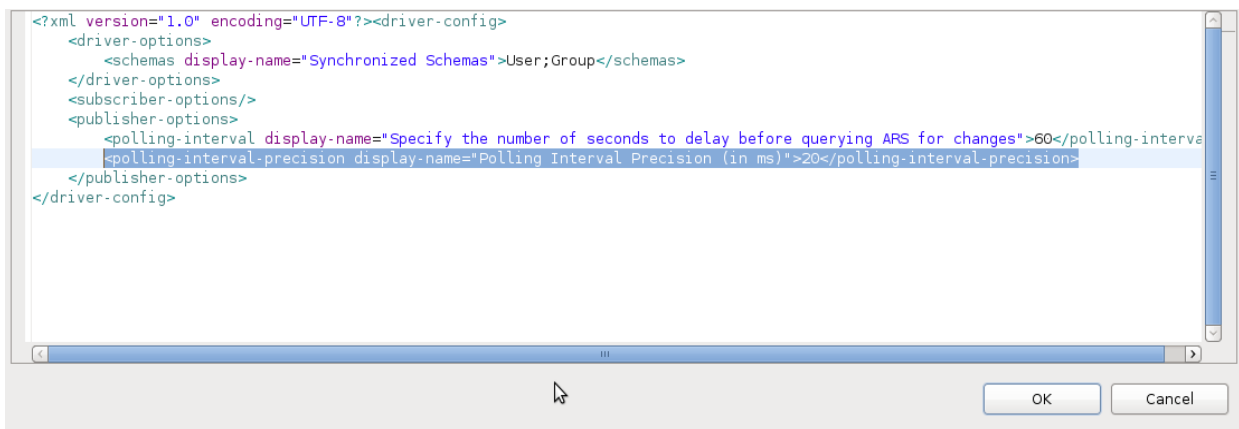
This will adapt the precision of the polling cycle to allow a differences of 20 milliseconds.

Edit the XML driver parameters in iManager.




Edit the driver option in Designer.

1. Edit the driver properties
2. Select the Driver Configuration in list on the left
3. Select the Driver Parameters tab
4. Click on Edit XML and the tab



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 3.6.1 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 6.1, “Driver Configuration,” on page 26](#)

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:

- [Section 6.1.1, “Driver Module,” on page 26](#)
- [Section 6.1.2, “Driver Object Password \(iManager Only\),” on page 27](#)
- [Section 6.1.3, “Authentication,” on page 27](#)
- [Section 6.1.4, “Startup Option,” on page 28](#)
- [Section 6.1.5, “Driver Parameters,” on page 29](#)

6.1.1 Driver Module

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

| 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 |

| Options | Description |
|---------------------------------|--|
| | <p>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.</p> <p>The java class name is: <code>be.opns.dirxml.driver.xds.arsdriver.ARSDriverShim</code> for Remedy 7.1 and up. <code>be.opns.dirxml.driver.ars.arsremedydrivershim.ARSDriverShim</code> for Remedy 7.0 and lower.</p> |
| <i>Native</i> | This option is not used with the Remedy driver. |
| <i>Connect to Remote Loader</i> | <p>Used when the driver is connecting remotely to the connected system.</p> <p>Designer includes two suboptions:</p> <ul style="list-style-type: none"> 🔑 <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 does not run. The Remote Loader uses this password to authenticate itself to the remote driver shim. 🔑 <i>Remote Loader Client Configuration for Documentation</i>: Includes information on the Remote Loader client configuration when Designer generates documentation for the driver. |









6.1.2 Driver Object Password (iManager Only)

| 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 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 |
|--|--|
| <i>Authentication ID</i> or 🔑 <i>User ID</i> | Specify a user application ID. This ID is used to pass Identity Vault subscription information to the application. Example: <code>dirxml</code> |
| <i>Authentication Context</i> or 🔑 <i>Connection Information</i> | Specify the IP address or name of the server the application shim should communicate with. The connection string uses the following format: <code>remedy</code> or <code>remedy:port</code> if not user RPC port mapping |

| Option | Description |
|--|---|
| <p><i>Remote Loader Connection Parameters</i></p> <p>ok</p> <ul style="list-style-type: none">  <i>Host name</i>  <i>Port</i>  <i>KMO</i>  <i>Other parameters</i> | <p>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 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</p> |
| <p>Driver Cache Limit (kilobytes)</p> <p>or</p> <ul style="list-style-type: none">  Cache limit (KB) | <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">  Click <i>Unlimited</i> to set the file size to unlimited in Designer. |
| <p>Application Password</p> <p>or</p> <ul style="list-style-type: none">  Set Password | <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">  Set Password | <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> |

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 |
|--|---|
| <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 synchronize the driver</i> | This option only applies if the driver is deployed and was previously |

| Option | Description |
|--------|--|
| | 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 behavior to align with your network environment.

Driver Settings

- ***Synchronized Schemas***: Specify the synchronized Remedy Forms the driver will use to synchronize. If empty, the driver will assume that you want to synchronize with the complete ARS Remedy Schema.

Publisher Settings

- ***Polling Interval***: Specify the number of seconds the publisher channel will sleep between polling cycles.
- ***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 extent. See [Chapter 5 Troubleshooting the Driver on page 24](#).

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 |

For information about setting driver trace levels, see to “[Viewing Identity Manager Processes](#)” in the *Identity Manager 3.6.1 Common Driver Administration Guide*.