

Driver for eDirectory™ Implementation Guide

Novell® Identity Manager

3.6

July 23, 2008

www.novell.com



Legal Notices

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

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

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

Copyright © 2007-2008 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 [Novell Legal Patents \(http://www.novell.com/company/legal/patents/\)](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 [Novell Documentation \(http://www.novell.com/documentation/\)](http://www.novell.com/documentation/).

Novell Trademarks

For a list of Novell trademarks, see [Trademarks \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

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

Contents

About This Guide	7
1 Overview	9
1.1 Driver Concepts	9
1.1.1 Key Terms	9
1.1.2 How the eDirectory Driver Works	10
1.2 Driver Features	10
1.2.1 Local Platforms	10
1.2.2 Remote Platforms	10
1.2.3 Entitlements	10
1.2.4 Password Synchronization	11
1.2.5 Synchronizing Data	11
2 Installing the Driver Files	13
3 Creating a New Driver	15
3.1 Creating the Driver in Designer	15
3.1.1 Importing the Driver Configuration File	15
3.1.2 Configuring the Driver	16
3.1.3 Deploying the Driver	16
3.1.4 Starting the Driver	17
3.2 Creating the Driver in iManager	17
3.2.1 Importing the Driver Configuration File	18
3.2.2 Configuring the Driver	19
3.2.3 Starting the Driver	20
3.3 Activating the Driver	20
4 Upgrading an Existing Driver	21
4.1 Supported Upgrade Paths	21
4.2 What's New in Version 3.6	21
4.3 Upgrade Procedure	21
5 Securing Driver Communication	23
5.1 Configuring Secure Data Transfers	23
5.1.1 Understanding Secure Connections via the eDirectory Driver	23
5.1.2 Setting Up a KMO	24
5.2 Configuring Authentication Between Drivers	25

6	Synchronizing Passwords	27
7	Managing the Driver	29
8	Troubleshooting	31
8.1	Troubleshooting Driver Processes	31
8.2	Adding Driver Configuration Parameters	31
A	Driver Properties	33
A.1	Driver Configuration	33
A.1.1	Driver Module	33
A.1.2	Driver Object Password (iManager Only)	34
A.1.3	Authentication	35
A.1.4	Startup Option	36
A.1.5	Driver Parameters	36
A.1.6	ECMAScript	38
A.2	Global Configuration Values	38
B	Synchronized Attributes	41

About This Guide

This guide explains how to install and configure the Identity Manager Driver for eDirectory™.

- ♦ Chapter 1, “Overview,” on page 9
- ♦ Chapter 2, “Installing the Driver Files,” on page 13
- ♦ Chapter 3, “Creating a New Driver,” on page 15
- ♦ Chapter 4, “Upgrading an Existing Driver,” on page 21
- ♦ Chapter 5, “Securing Driver Communication,” on page 23
- ♦ Chapter 6, “Synchronizing Passwords,” on page 27
- ♦ Chapter 7, “Managing the Driver,” on page 29
- ♦ Chapter 8, “Troubleshooting,” on page 31
- ♦ Appendix A, “Driver Properties,” on page 33
- ♦ Appendix B, “Synchronized Attributes,” on page 41

Audience

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

Feedback

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

Documentation Updates

For the most recent version of this document, see the [Identity Manager 3.6 Drivers Documentation Web site \(http://www.novell.com/documentation/idm36drivers/index.html\)](http://www.novell.com/documentation/idm36drivers/index.html).

Additional Documentation

For information on Identity Manager 3.6 and other Identity Manager 3.6 drivers, see the [Identity Manager 3.6 Documentation Web site \(http://www.novell.com/documentation/idm36\)](http://www.novell.com/documentation/idm36).

Documentation Conventions

In this 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.

The Identity Manager Driver for eDirectory™ (eDirectory driver) synchronizes objects and attributes between different eDirectory trees.

This driver is unique among all other Identity Manager drivers. Because you are synchronizing data between eDirectory trees, you will always have two drivers installed, each in its own tree. The driver in one tree communicates with the driver in the other tree.

- [Section 1.1, “Driver Concepts,” on page 9](#)
- [Section 1.2, “Driver Features,” on page 10](#)

1.1 Driver Concepts

- [Section 1.1.1, “Key Terms,” on page 9](#)
- [Section 1.1.2, “How the eDirectory Driver Works,” on page 10](#)

1.1.1 Key Terms

Driver shim: A Java file (`NdsToNds.jar`) loaded directly by Identity Manager. Communicates event changes to be sent from the Identity Manager Driver for eDirectory to an Identity Vault, communicates changes from the Identity Vault to the Identity Manager Driver for eDirectory, and operates as the link that connects the Identity Vault and the Identity Vault Driver object.

Driver: A set of policies, filters, and objects that act as the connector between an Identity Vault and the driver shim.

This software enables an application to publish events from an application to the directory, enables an application to subscribe to events from the directory, and synchronizes data between the directory and applications.

To establish a connection between the Metadirectory engine and an Identity Vault, you specify the driver’s configuration and connection parameters, policies, and filter values.

Driver object: A collection of channels, policies, rules, and filters that connect an application to an Identity Vault that is running Identity Manager.

Each driver performs different tasks. Policies, rules, and filters tell the driver how to manipulate the data to perform those tasks.

The Driver object displays information about the driver’s configuration, policies, and filters. This object enables you to manage the driver and provide eDirectory management of the driver shim parameters.

Identity Vault. A hub, with applications and directories publishing their changes to it. The Identity Vault then sends changes to the applications and directories that have subscribed for them. This results in two main flows of data: the Publisher channel and the Subscriber channel.

1.1.2 How the eDirectory Driver Works

Channels, filters, and policies control data flow.

Publisher and Subscriber Channels

The eDirectory driver is installed and configured in two trees. The driver's Publisher channel in TreeA communicates with the driver's Subscriber channel in TreeB. Conversely, the driver's Publisher channel in TreeB communicates with the driver's Subscriber channel in TreeA.

Filters

Identity Manager uses filters to control which objects and attributes are shared. The default filter configurations for the eDirectory driver allow objects and attributes to be shared. For a list of synchronized attributes, see [Appendix B, "Synchronized Attributes," on page 41](#).

Policies

Identity Manager uses policies to control data synchronization between the eDirectory driver and the Identity Vaults. The eDirectory driver comes with an example configuration file to set up policies.

1.2 Driver Features

- ♦ [Section 1.2.1, "Local Platforms," on page 10](#)
- ♦ [Section 1.2.2, "Remote Platforms," on page 10](#)
- ♦ [Section 1.2.3, "Entitlements," on page 10](#)
- ♦ [Section 1.2.4, "Password Synchronization," on page 11](#)
- ♦ [Section 1.2.5, "Synchronizing Data," on page 11](#)

1.2.1 Local Platforms

The eDirectory driver runs in any Identity Manager 3.6 installation. See "[System Requirements](#)" in the *Identity Manager 3.6 Installation Guide*.

1.2.2 Remote Platforms

The eDirectory driver supports remote connections without the Remote Loader. The driver does not use the Remote Loader because the driver in one tree communicates directly with the driver in the other tree.

1.2.3 Entitlements

The eDirectory driver example configuration does not implement any entitlements. However, the driver does support entitlements you create. For more information about entitlements, see the *Identity Manager 3.6 Entitlements Guide*.

1.2.4 Password Synchronization

The eDirectory driver supports password synchronization via Universal Password. If desired, you can also use the older form of password synchronization (Public/Private key pair or NDS[®] password). For more information, see [Chapter 6, “Synchronizing Passwords,” on page 27](#).

1.2.5 Synchronizing Data

The eDirectory driver synchronizes data between two Identity Vaults or trees. The driver can run anywhere that a Metadirectory server is running.

Installing the Driver Files

2

If you are synchronizing information between TreeA and TreeB, you must install the Metadirectory engine and eDirectory driver on eDirectory servers in both trees. Therefore, the installation must be completed twice—once for the Metadirectory engine and eDirectory driver in TreeA and once in TreeB. Use the instructions in “[Installing the Metadirectory Server](#)” in the *Identity Manager 3.6 Installation Guide*.

The eDirectory servers where you install the driver must hold master or read/write replicas of the objects you want synchronized between the two trees.

The installation program extends the Identity Vault (eDirectory) schema and installs the driver shim and driver configuration file. It does not create the driver in the Identity Vault (see [Chapter 3, “Creating a New Driver,”](#) on page 15) or upgrade an existing driver’s configuration (see [Chapter 4, “Upgrading an Existing Driver,”](#) on page 21).

The eDirectory driver does not use the Remote Loader because the driver in one tree communicates directly with the driver in the other tree.

The eDirectory driver requires the following:

- Novell® Certificate Server™ running on each server that hosts the driver.
- A Certificate Authority (CA) to support SSL encryption between drivers.

Novell Certificate Server and the Certificate Authority are discussed more in [Chapter 5, “Securing Driver Communication,”](#) on page 23.

Creating a New Driver

3

After the eDirectory™ driver files are installed on the server where you want to run the driver (see [Chapter 2, “Installing the Driver Files,” on page 13](#)), you can create the driver in the Identity Vault. You do so by importing the basic driver configuration file and then modifying the driver configuration to suit your environment. You can do this in either Designer or iManager.

- ♦ [Section 3.1, “Creating the Driver in Designer,” on page 15](#)
- ♦ [Section 3.2, “Creating the Driver in iManager,” on page 17](#)
- ♦ [Section 3.3, “Activating the Driver,” on page 20](#)

3.1 Creating the Driver in Designer

You create the eDirectory 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. To connect two trees, you need to do this for the driver installed in each tree.

- ♦ [Section 3.1.1, “Importing the Driver Configuration File,” on page 15](#)
- ♦ [Section 3.1.2, “Configuring the Driver,” on page 16](#)
- ♦ [Section 3.1.3, “Deploying the Driver,” on page 16](#)
- ♦ [Section 3.1.4, “Starting the Driver,” on page 17](#)

3.1.1 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 *eDirectory*, 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.

Remote Tree Base Container: Specify the source container for the eDirectory objects.

User Container: Select the Identity Vault container where any new users created from eDirectory file information will be placed. This value becomes the default for all drivers in the driver set. If you don’t want to change this value for all drivers, leave this field alone and change the value on the driver’s Global Configuration Values page after you’ve finished importing the driver.

Group Container: Select the Identity Vault container where any new groups created from eDirectory file information will be placed. This value becomes the default for all drivers in the driver set. If you don’t want to change this value for all drivers, leave this field alone and change the value on the driver’s Global Configuration Values page after you’ve finished importing the driver.

Remote Tree Address and Port: Specify the host name or IP address, and communication port of the Identity Manager server in the remote tree.

- 5 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 the driver's default configuration settings.

- 6 To review or modify the default configuration settings, click *Configure*, then continue with [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](#).

3.1.2 Configuring the Driver

After importing the driver configuration file, the eDirectory driver will run. However, the basic configuration might not meet the requirements for your environment. You should complete the following tasks to configure the driver:

- ♦ **Secure the driver connection:** eDirectory drivers communicate via SSL using digital certificates for authentication. You need to set up this secure connection. See [Chapter 5, "Securing Driver Communication,"](#) on page 23.
- ♦ **Configure the driver filter:** Modify the driver filter to include the object classes and attributes you want synchronized between the two eDirectory trees. For information about the classes and attributes include in the filter for the basic configuration, see [Appendix B, "Synchronized Attributes,"](#) on page 41.
- ♦ **Configure policies:** Modify the policies as needed. Policies should generally be placed only on the Publisher channel, not on the Subscriber channel. The Matching and Placement policies cannot operate correctly on the Subscriber channel because the Subscriber channel is acting primarily as a source of events for the Publisher channel of the other tree.


You might consider placing an Event Transform or Create Policy on the Subscriber channel to prevent sending unnecessary data across the channel. See ["Using Scope Filtering to Manage Users on Different Servers"](#) in the *Identity Manager 3.6 Installation Guide*.

- ♦ **Configure password synchronization:** The basic driver configuration is set up to support bidirectional password synchronization through Universal Password. If you don't want this setup, see [Chapter 6, "Synchronizing Passwords,"](#) on page 27.

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

3.1.3 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 through the deployment summary, then click *Deploy*.
- 6 Read the successful message, then click *OK*.
- 7 Click *Define Security Equivalence* to assign rights to the driver.

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

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

7b Click *OK* twice.

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

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

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

8b Click *OK*.

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


8d Click *OK*.

- 9 Click *OK*.

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


For information about management tasks with the driver, see [Chapter 7, “Managing the Driver,” on page 29](#).

3.2 Creating the Driver in iManager

You create the eDirectory 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. To connect two trees, you need to do this for the driver installed in each tree.

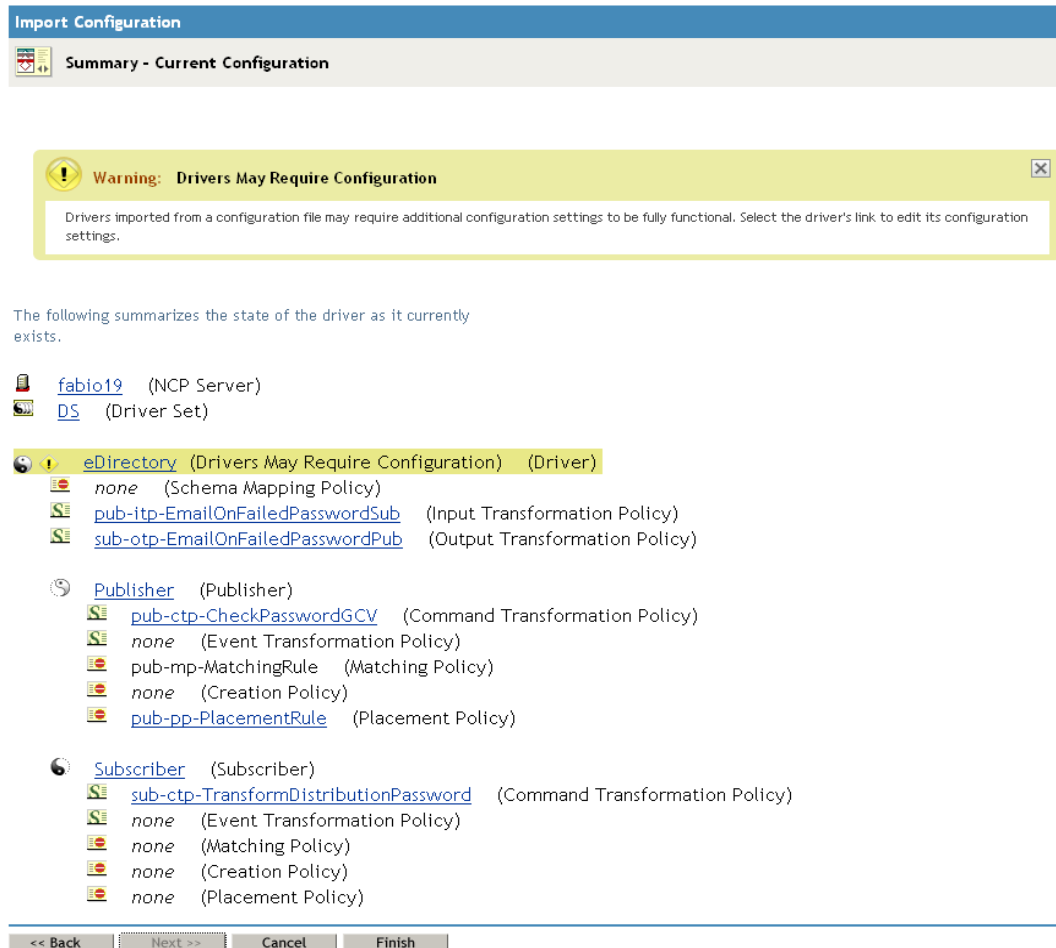
- ♦ [Section 3.2.1, “Importing the Driver Configuration File,” on page 18](#)
- ♦ [Section 3.2.2, “Configuring the Driver,” on page 19](#)
- ♦ [Section 3.2.3, “Starting the Driver,” on page 20](#)

3.2.1 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, <i>Import a configuration from the server (.XML file)</i> . In the <i>Show</i> field, select <i>Identity Manager 3.6 configurations</i> . In the <i>Configurations</i> field, select the eDirectory file.
Driver name	Type a name for the driver. The name must be unique within the driver set.
Remote Tree Base Container	Specify the source container for the eDirectory objects.
User Container	Select the Identity Vault container where any new users created from eDirectory file information will be placed. This value becomes the default for all drivers in the driver set. If you don't want to change this value for all drivers, leave this field alone and change the value on the driver's Global Configuration Values page after you've finished importing the driver.
Group Container	Select the Identity Vault container where any new groups created from eDirectory file information will be placed. This value becomes the default for all drivers in the driver set. If you don't want to change this value for all drivers, leave this field alone and change the value on the driver's Global Configuration Values page after you've finished importing the driver.
Remote Tree Address and Port	Specify the hostname or IP address, and the communication port of the Identity Manager server in the remote tree.
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.
Exclude Administrative Roles	You should exclude any administrative User objects (for example, Admin and DriversUser) from synchronization.

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



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.

- To modify the default configuration settings, click the linked driver name, then continue with **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**.

3.2.2 Configuring the Driver

After importing the driver configuration file, the eDirectory driver will run. However, the basic configuration might not meet the requirements for your environment. You should complete the following tasks to configure the driver:

- ♦ **Secure the driver connection:** eDirectory drivers communicate via SSL using digital certificates for authentication. You need to set up this secure connection. See **Chapter 5, "Securing Driver Communication,"** on page 23.


- ♦ **Configure the driver filter:** Modify the driver filter to include the object classes and attributes you want synchronized between the two eDirectory trees. For information about the classes and attributes include in the filter for the basic configuration, see [Appendix B, “Synchronized Attributes,” on page 41.](#)
- ♦ **Configure policies:** Modify the policies as needed. Policies should generally be placed only on the Publisher channel, not on the Subscriber channel. The Matching and Placement policies cannot operate correctly on the Subscriber channel because the Subscriber channel is acting primarily as a source of events for the Publisher channel of the other tree.
You might consider placing an Event Transform or Create Policy on the Subscriber channel to prevent sending unnecessary data across the channel. See [“Using Scope Filtering to Manage Users on Different Servers”](#) in the *Identity Manager 3.6 Installation Guide*.
- ♦ **Configure password synchronization:** The basic driver configuration is set up to support bidirectional password synchronization through Universal Password. If you don’t want this setup, see [Chapter 6, “Synchronizing Passwords,” on page 27.](#)

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

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

For information about management tasks with the driver, see [Chapter 7, “Managing the Driver,” on page 29.](#)

3.3 Activating the Driver

If you created the driver in a driver set where you’ve already activated the Metadirectory engine and service drivers, the driver inherits the activation. If you created the driver in a driver set that has not been activated, you must activate the driver within 90 days. Otherwise, the driver stops working.

For information on activation, refer to [“Activating Novell Identity Manager Products”](#) in the *Identity Manager 3.6 Installation Guide*.

Upgrading an Existing Driver

4

The following sections provide information to help you upgrade an existing driver to version 3.6:

- [Section 4.1, “Supported Upgrade Paths,” on page 21](#)
- [Section 4.2, “What’s New in Version 3.6,” on page 21](#)
- [Section 4.3, “Upgrade Procedure,” on page 21](#)

4.1 Supported Upgrade Paths

You can upgrade from any 3.x version of the eDirectory™ driver. Upgrading a pre-3.x version of the driver directly to version 3.6 is not supported.

4.2 What’s New in Version 3.6

Version 3.6 of the driver does not include any new features that are not already in the 3.6 version. However, the process for creating a new driver has changed. For detailed information, see [Chapter 3, “Creating a New Driver,” on page 15](#).

4.3 Upgrade Procedure

The process for upgrading the eDirectory driver is the same as for other Identity Manager drivers. For detailed instructions, see “[Upgrading](#)” in the *Identity Manager 3.6 Installation Guide*.

Securing Driver Communication

5

To provide security while transmitting information between two Identity Vaults, you must configure the eDirectory™ driver to communicate with the destination eDirectory driver through an SSL connection.

In addition, you can provide additional security by requiring the two eDirectory drivers to authenticate to one another. Although this is optional, it is strongly recommended.

The following sections explain how to set up SSL and configure driver authentication:

- ♦ [Section 5.1, “Configuring Secure Data Transfers,” on page 23](#)
- ♦ [Section 5.2, “Configuring Authentication Between Drivers,” on page 25](#)

5.1 Configuring Secure Data Transfers

All eDirectory driver communication is secured through SSL. To configure your eDirectory drivers to handle secure data transfers, run the NDS-to-NDS Driver Certificate Wizard in iManager.

- ♦ [Section 5.1.1, “Understanding Secure Connections via the eDirectory Driver,” on page 23](#)
- ♦ [Section 5.1.2, “Setting Up a KMO,” on page 24](#)

5.1.1 Understanding Secure Connections via the eDirectory Driver

The following items can help you understand how secure connections are established when using the eDirectory driver:


- ♦ The driver uses SSL sockets to provide authentication and a secure connection. SSL uses digital certificates to allow the parties to an SSL connection to authenticate one another. Identity Manager in turn uses Novell Certificate Server certificates for secure management of sensitive data.
- ♦ To use the driver, you must have the Novell® Certificate Server™ running in each tree. We recommend that you use the Certificate Authority from one of the trees containing the driver to issue the certificates used for SSL. If your tree does not have a Certificate Authority, you need to create one. You can use an external Certificate Authority. For information about Novell Certificate Server, see the [Novell Certificate Server 3.3 Documentation Web site \(http://www.novell.com/documentation/crtsrv33/index.html\)](http://www.novell.com/documentation/crtsrv33/index.html).
- ♦ The Novell implementation of SSL that the driver uses is based on Novell Secure Authentication Services (SAS) and NTLS for eDirectory. These must be installed and configured on the server where the driver runs. eDirectory usually does this automatically.
- ♦ To configure driver security, it is necessary to create and reference certificates in the eDirectory trees that will be connected using the driver. Certificate objects in eDirectory are called Key Material Objects (KMOs) because they securely contain both the certificate data (including the public key) and the private key associated with the certificate.

A minimum of two KMOs (one KMO per tree) must be created for use with the eDirectory drivers. This section explains using a single KMO per tree.

The NDS-to-NDS Driver Certificate Wizard sets up the KMOs.

5.1.2 Setting Up a KMO

To configure your Identity Vault system to handle secure Identity Manager data transfers:

- 1 Find out the tree name or IP address of the destination server.
- 2 Launch iManager and authenticate to your first tree.
- 3 Click  to display the Identity Manager Administration page.
- 4 In the *Administration* list, click *NDS-to-NDS Driver Certificates* to launch the wizard.
- 5 At the Welcome page, enter the requested information for the first tree.

Default values are provided by using objects in the tree that you authenticated to when you launched iManager. You must enter or confirm the following information:

- ♦ **Driver DN:** Specify the distinguished name of the eDirectory driver (for example, eDirectoryDriver.DriverSet1.Services.Novell).
 - ♦ **Tree:** Verify the name of the current tree; if it is not correct, enter the correct name.
 - ♦ **Username:** Specify the username for an account with Admin privileges in the current tree (for example, Admin).
 - ♦ **Password:** Specify the password for the user.
 - ♦ **Context:** Specify the user's context (for example Services.Novell).
- 6 Click *Next*.

The wizard uses the information you entered to authenticate to the first tree, verify the driver DN, and verify that the driver is associated with a server.

- 7 Specify the requested information for the second tree.
 - ♦ **Driver DN:** Specify the distinguished name of the eDirectory driver (for example, eDirectoryDriver.DriverSet2.Novell).
 - ♦ **Tree:** Specify the name of the second tree.
 - ♦ **Username:** Specify the username for an account with Admin privileges in the second tree (for example, Admin).
 - ♦ **Password:** Specify the password for the user.
 - ♦ **Context:** Specify the user's context (for example Users.Novell).

- 8 Click *Next*.

The wizard uses the information you entered to authenticate to the second tree, verify the driver DN, and verify that the driver is associated with a server.

- 9 Review the information on the Summary Page, then click *Finish*.

If KMOs already existed for these trees, the wizard deletes them and then does the following:

- ♦ Exports the trusted root of the CA in the first tree.
- ♦ Creates KMO objects.
- ♦ Issues a certificate signing request.
- ♦ Places certificate key pair names in the drivers' Authentication IDs (see [Section A.1.3, "Authentication," on page 35](#)).

5.2 Configuring Authentication Between Drivers

In addition to providing the mandatory certificates needed to use SSL, you can set up additional security by configuring the Subscriber channel on one eDirectory driver to authenticate to the Publisher channel on the other driver.

Set a driver object password and application password on each driver. Make sure the driver object password of the first driver matches the application password of the second driver, and that the driver object password of the second driver matches the application password of the first driver. For example:

Table 5-1 *Driver Object and Application Passwords*

	Driver Object Password	Application Password
Driver 1	Provo	Cambridge
Driver 2	Cambridge	Provo

For information about setting the passwords, see [Section A.1.2, “Driver Object Password \(iManager Only\),” on page 34](#) and [Section A.1.3, “Authentication,” on page 35](#).

Synchronizing Passwords

6

To use the eDirectory™ driver to set up password synchronization between the two Identity Vaults, follow the instructions in the *Identity Manager 3.6 Password Management Guide*.

The following list contains information that is specific to setting up password synchronization with the eDirectory driver. Use it to supplement the information in the *Password Management Guide*.

- ♦ Universal Password is the standard method to synchronize passwords with Identity Manager. The eDirectory driver's policies and filters (in the basic configuration file) are set up to support this method. However, you can use the older method of synchronizing passwords through the NDS® password. This method is also known as synchronizing the Public Key and Private Key. If you choose to use the NDS password method, make sure you follow the instructions in “*Scenario 1: Using NDS Password to Synchronize between Two Identity Vaults*” in the *Identity Manager 3.6 Password Management Guide*.

- ♦ If you decide to enforce password policies in multiple trees, make sure that the Advanced Password Rules in the password policies are compatible in each tree, so that password synchronization can be successful.

If you enforce incompatible password policies in multiple eDirectory trees, and choose to reset a password back to the distribution password if it does not comply (with the option *If password does not comply, enforce Password Policy on the connected system by resetting user's password to the Distribution Password*), you could encounter a loop in which each Identity Vault server tries to change a noncompliant password.

Information about password policies is in “Managing Passwords by Using Password Policies” in the *Password Management Administration Guide* (http://www.novell.com/documentation/password_management32/pwm_administration/data/ampxjj0.html).

- ♦ The Check Password Status task in iManager does not work for a connected system if the Password Policy has Universal Password enabled and does not have the setting selected for synchronizing Universal Password with NDS Password.

The Check Password Status task lets you see whether a user's password in Identity Manager is synchronized with the password on connected systems.

If you are using the eDirectory driver and the password policy for a user specifies in the Configuration Options tab that the NDS Password should not be updated when the Universal Password is updated, then the Check Password Status task for that user always shows that the password is not synchronized. The password status is shown as not synchronized, even if the Identity Manager Distribution Password and the Universal Password on the connected system are in fact the same.

This is because the Identity Vault check-password functionality is checking the NDS Password at this time, instead of going through NMAST™ to refer to the Universal Password.

By default, the NDS Password is updated when the Universal Password is updated in the password policy. If you select this option, Check Password Status should be accurate for the connected system.

Managing the Driver

7

As you work with the eDirectory™ 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 Common Driver Administration Guide*.

Refer to the following sections for information about troubleshooting problems you might encounter with the eDirectory™ driver:

- ♦ [Section 8.1, “Troubleshooting Driver Processes,” on page 31](#)
- ♦ [Section 8.2, “Adding Driver Configuration Parameters,” on page 31](#)

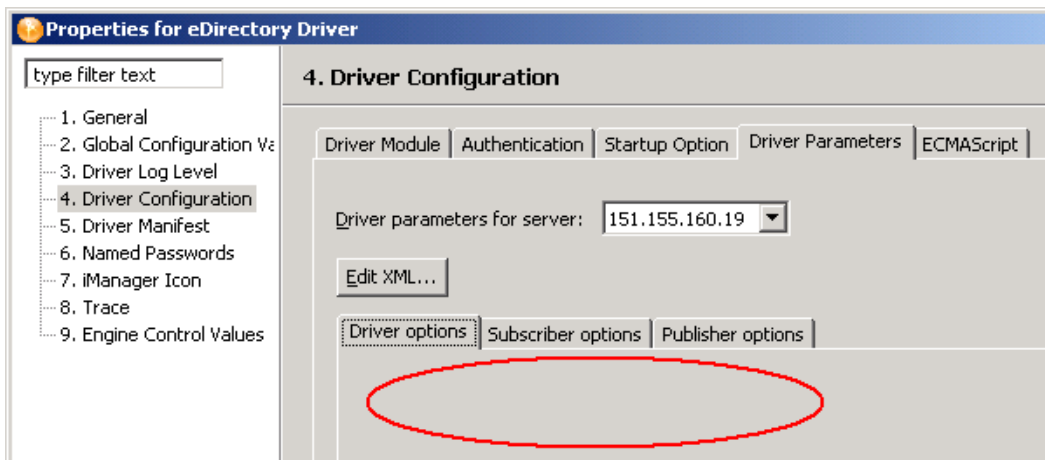
8.1 Troubleshooting Driver Processes

Viewing driver processes is necessary to analyze unexpected behavior. To view the driver processing events, use DSTrace. You should only use it during testing and troubleshooting the driver. Running DSTrace while the drivers are in production increases the utilization on the Identity Manager server and can cause events to process very slowly. For more information, see “[Viewing Identity Manager Processes](#)” in the *Identity Manager 3.6 Common Driver Administration Guide*.

8.2 Adding Driver Configuration Parameters

If no parameters appear on the eDirectory driver’s *Driver Parameters* tab:

Figure 8-1 Empty Tabs on the Driver Parameters Page

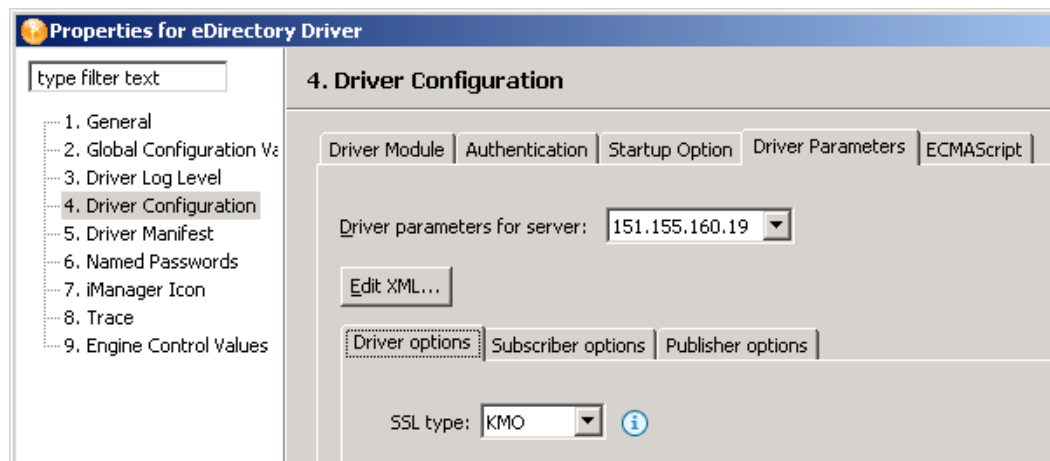


- 1 On the Novell® Support Web site, open [Novell Support TID 2970417](http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=InfoDocument-2970417&sliceId=&dialogID=29785513&stateId=0%200%2029791519) (<http://www.novell.com/support/search.do?cmd=displayKC&docType=kc&externalId=InfoDocument-2970417&sliceId=&dialogID=29785513&stateId=0%200%2029791519>).

Although this TID was written for Identity Manager 2.0.1, the information applies to Identity Manager 3.6.

- 2 Download `idm201edirir1.tgz`.
- 3 Unzip the file.
- 4 Open `options.xml` with a text editor, then copy the entire text.
- 5 In Designer or iManager, click *Edit XML* on the Driver Parameters page.

- 6 Overwrite the text in the Driver Parameters XML window by pasting the contents of `options.xml` into the window.
- 7 Click *OK*.




Settings and values appear on the *Driver options*, *Subscriber options*, and *Publisher options* tabs. For a description of these settings, see [Section A.1.5, “Driver Parameters,”](#) on page 36.

Driver Properties

A


This section provides information about the Driver Configuration and Global Configuration Values properties for the eDirectory™ driver. These are the only unique properties for the eDirectory driver. 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 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 for Identity Manager, it is marked with a Designer  icon.

- ♦ [Section A.1, “Driver Configuration,” on page 33](#)
- ♦ [Section A.2, “Global Configuration Values,” on page 38](#)

A.1 Driver Configuration

In iManager:

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

In Designer:

- 1 Open a project in the Modeler, then right-click the driver line and click *Properties > Driver Configuration*.



The Driver Configuration options are divided into the following sections:

- ♦ [Section A.1.1, “Driver Module,” on page 33](#)
- ♦ [Section A.1.2, “Driver Object Password \(iManager Only\),” on page 34](#)
- ♦ [Section A.1.3, “Authentication,” on page 35](#)
- ♦ [Section A.1.4, “Startup Option,” on page 36](#)
- ♦ [Section A.1.5, “Driver Parameters,” on page 36](#)
- ♦ [Section A.1.6, “ECMAScript,” on page 38](#)

A.1.1 Driver Module

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

Table A-1 *Driver Module*

Option	Description
<i>Java</i>	Used to specify the name of the Java* class that is instantiated for the shim component of the driver. This class can be located in the <code>classes</code> directory as a class file, or in the <code>lib</code> directory as a <code>.jar</code> file. If this option is selected, the driver is running locally.
<i>Native</i>	This option is not used with the eDirectory driver.
<i>Connect to Remote Loader</i>	<p>The Remote Loader is not used with the eDirectory driver. However, Designer includes two suboptions, one (Driver Object Password) of which is required to set up authentication between two eDirectory drivers. If you use a driver object password, you need to select the <i>Connect to Remote Loader</i> option, set the password, click <i>Apply</i> to save the password, then select the <i>Java</i> option again.</p> <ul style="list-style-type: none">◆  <i>Driver Object Password</i>: Specifies a password for the eDirectory driver. This password must match the Application password set for the destination eDirectory driver.◆  <i>Remote Loader Client Configuration for Documentation</i>: This option is not used with the eDirectory driver.

A.1.2 Driver Object Password (iManager Only)

The driver object password is used to enable the eDirectory driver's Subscriber channel to authenticate to the Publisher channel of the destination eDirectory driver. This authentication, while optional, provides an extra layer of security between the two drivers.

In Designer, this setting is located under the **Connect to Remote Loader** option.

For additional information about setting up authentication between the two drivers, see **Chapter 5, "Securing Driver Communication,"** on page 23.







Table A-2 *Driver Object Password*





Option	Description
<i>Driver Object Password</i>	Specifies a password for the eDirectory driver. This password must match the Application password set for the destination eDirectory driver.

A.1.3 Authentication

The Authentication section stores the information required to authenticate to the connected system. For the eDirectory driver, it stores the information required to authenticate to the connected eDirectory driver and tree.

Table A-3 *Authentication*


Option	Description
 Authentication information for server	Displays or specifies the server that the driver is associated with.
<i>Authentication ID</i>	This ID is used by the driver to authenticate to the destination eDirectory driver. The ID is automatically generated and stored in this field when you run the NDS-to-NDS Driver Certificates wizard. For information, see Chapter 5, "Securing Driver Communication," on page 23 .
<i>Authentication Context</i>	Specify the host name or IP address of the destination server as well as the decimal port number (for example, 187.168.1.1:8196).
or	
 <i>Connection Information</i>	<p>You can specify a separate port for Subscriber and Publisher channels by specifying a second port number following a second colon. If a second port number is specified, the Publisher channel uses the second port number rather than using the same port number as the Subscriber channel (for example, 255.255.255.255:2000:2001).</p> <p>If your server has multiple IP addresses, you can specify the IP address you want the Publisher channel to use. This requires specifying the remote IP address, the Subscriber channel port, the local IP address, and the Publisher channel port. For example, 137.65.134.81:2000:137.65.134.83:2000 specifies that the Subscriber channel will communicate with the remote tree on 137.65.134.81, port 2000, and that the Publisher channel will listen on address 137.65.134.83, port 2000.</p> <p>If you see <code>java.net.ConnectException: Connection Refused</code>, no port connection is available on the remote side. This error might be caused by one of the following:</p> <ul style="list-style-type: none"> ♦ The driver on the remote side is not running. ♦ The driver is running but is configured to use a different port.
<i>Remote Loader Connection Parameters</i>	The eDirectory driver does not support the use of the Remote Loader. These options do not apply.
or	
 <i>Host name</i>	
 <i>Port</i>	
 <i>KMO</i>	
 <i>Other parameters</i>	

Option	Description
<i>Driver Cache Limit (kilobytes)</i> or  <i>Cache limit (KB)</i>	Specify the maximum event cache file size (in KB). If it is set to zero, the file size is unlimited.  Click <i>Unlimited</i> to set the file size to unlimited in Designer.
<i>Application Password</i> or  <i>Set Password</i>	The application password, when used in conjunction with the driver object password, enables the eDirectory driver's Subscriber channel to authenticate to the Publisher channel of the destination eDirectory driver. This authentication, while optional, provides an extra layer of security between the two drivers. This password be the same as the driver object password for the destination eDirectory driver. For more information, see Chapter 5, "Securing Driver Communication," on page 23 .
<i>Remote Loader Password</i> or  <i>Set Password</i>	The eDirectory driver does not support the use of the Remote Loader. These options do not apply.

A.1.4 Startup Option

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

Table A-4 *Startup Option*

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 <i>Disabled</i> , this file is deleted and no new events are stored in the file until the driver state is changed to <i>Manual</i> or <i>Auto Start</i> .
 <i>Do not automatically synchronize the driver</i>	This option applies only if the driver is deployed and was previously disabled. If this is not selected, the driver re-synchronizes the next time it is started.

A.1.5 Driver Parameters

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

By default, there is only one driver parameter. It is the *Publisher heartbeat interval* under *Publisher Options*. The other parameters are displayed only if you manually add them as described in [Section 8.2, "Adding Driver Configuration Parameters," on page 31](#).

Table A-5 *Driver Parameters*

Option	Description
Driver Options	
<i>SSL type</i>	Specifies whether to use a Key Material Object (KMO) for SSL or use a Java keystore file. For more information, click the <i>Information</i> icon.
Subscriber Options	
<i>Address or host name of remote publisher</i>	Specifies the IP address or DNS name of the server hosting the remote eDirectory driver that the local subscriber connects to.
<i>TCP port of remote publisher</i>	If the remote publisher options specify a TCP port, this must be set to <i>specify</i> and the value from the remote Publisher channel entered into the <i>Port number</i> field. (These two fields must match what is set in the remote Publisher channel's options, which have corresponding fields).
<i>Port number</i>	Specifies the port number that the remote publisher is configured to run on. Displays only if you select <i>specify</i> in the <i>TCP port of remote publisher</i> field.
<i>Advanced options</i>	Displays additional fields when you select <i>show</i> .
<i>Socket local bind</i>	The <i>local bind</i> fields specify which IP address the Subscriber channel's socket will be bound to. This is generally only useful if the server has more than one IP address and it is important to bind to a particular address because of firewall settings.
<i>Local bind address for subscriber socket</i>	The <i>local bind</i> fields specify which IP address the Subscriber channel's socket will be bound to. This is generally only useful if the server has more than one IP address and it is important to bind to a particular address because of firewall settings.
<i>Receive timeout in minutes</i>	<p>In order to detect a lost TCP/IP connection, the eDir-to-eDir driver periodically sends small packets. This value determines how long after entering a receive-wait condition the Subscriber channel waits until sending a keep-alive packet to determine if the TCP/IP connection has been lost. Generally, do not change this value except under instruction from Novell®.</p> <p>The default value for the Subscriber channel is one minute.</p>
Publisher Options	
<i>Publisher heartbeat interval</i>	Specifies how often you want the driver to send a status message along the Publisher channel when there has not been any traffic during the interval time.
<i>Local bind address for publisher socket</i>	Specifies which IP address the Subscriber channel's socket will be bound to. This is generally only useful if the server has more than one IP address and it is important to bind to a particular address because of firewall settings. This setting applies to the local publisher's "server" socket on which the local publisher listens for connections from the remote Subscriber channel.

Option	Description
<i>Receive timeout in minutes</i>	In order to detect a lost TCP/IP connection, the eDirectory driver periodically sends small packets. This value determines how long after entering a receive-wait condition the Publisher channel waits until sending a keep-alive packet to determine if the TCP/IP connection has been lost. Generally, do not change this value except under instruction from Novell.
	The default value for the Publisher channel is ten minutes.


A.1.6 ECMAScript

Enables you to add ECMAScript resource files. The resources extend the driver's functionality when Identity Manager starts the driver.

A.2 Global Configuration Values


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

The eDirectory driver includes several GCVs that are created from information supplied during importing the driver configuration file (see [Chapter 3, "Creating a New Driver," on page 15](#)) and one that is not.

The driver also includes the GCVs that are used with password synchronization. In Designer, you must click the  icon next to a password synchronization GCV to edit it. This displays the Password Synchronization Options dialog box that has a better view of the relationship between the different settings. In iManager, you should edit the password synchronization settings on the *Server Variables* tab rather than under the GCVs. The Server Variables page has a better view of the relationship between the different GCVs.

You can add your own GCVs if you discover you need additional ones as you implement policies in the driver.

To access the driver's GCVs in iManager:

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

or

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

To access the driver's GCVs in Designer:



- 1 Open a project in the Modeler.
- 2 Right-click the driver icon  or line, then select *Properties > Global Configuration Values*.
or
To add a GCV to the driver set, right-click the driver set icon , then click *Properties > GCVs*.

Table A-6 *Global Configuration Values > Password Configuration*

Option	Description
<i>Application accepts passwords from Identity Manager</i>	If True, allows passwords to flow from the Identity Manager data store to the connected system.
<i>Identity Manager accepts passwords from application</i>	If True, allows passwords to flow from the connected system to Identity Manager.
<i>Publish passwords to NDS password</i>	Use the password from the connected system to set the non-reversible NDS® password in eDirectory.
<i>Publish passwords to Distribution Password</i>	Use the password from the connected system to set the NMAS™ Distribution Password used for Identity Manager password synchronization.
<i>Require password policy validation before publishing passwords</i>	If True, applies NMAS password policies during publish password operations. The password is not written to the data store if it does not comply.
<i>Reset user's external system password to the Identity Manager password on failure</i>	If True, on a publish Distribution Password failure, attempt to reset the password in the connected system by using the Distribution Password from the Identity Manager data store.
<i>Notify the user of password synchronization failure via e-mail</i>	If True, notify the user by e-mail of any password synchronization failures.
<i>Connected System or Driver Name</i>	The name of the connected system, application, or Identity Manager driver. This value is used by the e-mail notification templates.

Option	Description
<i>eDirectory Publisher Placement type</i>	<p>Select one of the following options:</p> <ul style="list-style-type: none"> ♦ Mirrored: Synchronizes objects hierarchically between the local and remote trees. If you choose this option, use the same option for configuring both eDirectory trees you are synchronizing. This option in the driver configuration synchronizes User, Group, Organization, Country, and Organizational Unit objects. It also mirrors the structure of a subtree in the other tree. ♦ Flat: Synchronizes all Users and Groups into specific containers. This option synchronizes User and Group objects and places all users in one container and all groups in another container. This option is typically used in conjunction with the Department option (or a similar configuration) in the other tree. This option doesn't create the containers that hold the users and groups. You must create those manually. ♦ Department: Synchronize Users and Groups by department (OU). This option synchronizes User and Group objects and places all users and groups in a container based on the Department field in your management console. This configuration is typically used in conjunction with the Flat option (or a similar configuration) in the other tree. This option doesn't create the containers for each department. You must create those manually. They must be the same as the container specified during import.
<i>Remote Tree Base Container</i>	Specify the source container for the objects in the destination eDirectory tree.

Synchronized Attributes

B

The filter for the basic driver configuration synchronizes the following attributes:

Table B-1 *eDirectory Driver Attributes That Are Synchronized*

accessCardNumber	Initials	preferredDeliveryMethod
ACL	instantMessagingID	preferredName
assistant	internationaliSDNNumber	Private Key
assistantPhone	Internet EMail Address	Public Key
businessCategory	jackNumber	registeredAddress
city	jobCode	roomNumber
CN	L	S
co	Language	SA
company	Mailbox ID	Security Equals
costCenter	Mailbox Location	Security Flags
costCenterDescription	mailstop	See Also
departmentNumber	manager	siteLocation
Description	managerWorkforceID	Surname
destinationIndicator	mobile	Telephone Number
directReports	NSCP:employeeNumber	teletexTerminalIdentifier
EMail Address	otherPhoneNumber	telexNumber
employeeStatus	O	Timezone
employeeType	OU	Title
Equivalent To Me	pager	tollFreePhoneNumber
Facsimile Telephone Number	personalTitle	UID
Full Name	photo	uniqueID
Generational Qualifier	Physical Delivery Office Name	vehicleInformation
Given Name	Postal Address	workforceID
Group Membership	Postal Code	x121Address
Higher Privileges	Postal Office Box	x500UniqueIdentifier