

# Novell Identity Manager Fan-Out Driver

3.5

March 19, 2007

CORE DRIVER ADMINISTRATION  
GUIDE

[www.novell.com](http://www.novell.com)



Novell®

## Legal Notices

Novell, Inc. and Omnibond Systems LLC. make no representations or warranties with respect to the contents or use of this documentation, and specifically disclaim any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. and Omnibond Systems LLC. reserve 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. and Omnibond Systems LLC. make no representations or warranties with respect to any software, and specifically disclaim any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. and Omnibond Systems LLC. reserve the right to make changes to any and all parts of the software, at any time, without any obligation to notify any person or entity of such changes.

You may not export or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

Copyright © 2004 Omnibond Systems, LLC. All Rights Reserved. Licensed to Novell, Inc. Portions Copyright © 2004 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.

The Solaris\* standard IO library has kernel limitations that interfere with the operation of the Provisioning Manager. Therefore, components for Solaris use the AT&T\* SFIO library. Use of this library requires the following notice:

The authors of this software are Glenn Fowler, David Korn and Kiem-Phong Vo.

Copyright (c) 1991, 1996, 1998, 2000, 2001, 2002 by AT&T Labs - Research.

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

This software is being provided as is, without any express or implied warranty. In particular, neither the authors nor AT&T Labs make any representation or warranty of any kind concerning the merchantability of this software or its fitness for any particular purpose.

Novell, Inc.  
404 Wyman Street, Suite 500  
Waltham, MA 02451  
U.S.A.  
[www.novell.com](http://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](http://www.novell.com/documentation).

## **Novell Trademarks**

DirXML is a trademark of Novell, Inc.

eDirectory is a trademark of Novell, Inc.

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 Client is a trademark of Novell, Inc.

Novell Directory Services and NDS are registered trademarks of Novell, Inc. in the United States and other countries.

## **Third-Party Materials**

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



# Contents

<b>About This Guide</b>	<b>7</b>
<b>1 Core Driver Planning</b>	<b>9</b>
1.1 Configuration Planning	9
1.2 Configuration and Performance Guidelines	11
1.2.1 eDirectory	11
1.2.2 Object Services and the Event Subsystem	12
1.2.3 Event Journal Services	12
1.2.4 Authentication Services	13
1.2.5 Platform Systems	13
1.2.6 Platform Services / Authentication Services Relationship	13
1.3 Requirements	14
1.3.1 User Rights Requirements	14
1.3.2 Secure Sockets Layer Entropy Requirements for UNIX Systems	14
1.3.3 Password Replication Requirements	14
1.3.4 Core Driver Requirements	15
1.3.5 Requirements for Workstations Used for Installation and Administration	16
1.3.6 Platform Services Requirements	16
1.4 Installation Planning Worksheet	16
1.4.1 Installation Planning Worksheet	16
1.4.2 Items on the Installation Planning Worksheet	18
<b>2 Installing the Driver</b>	<b>21</b>
2.1 The ASAM Directory	21
2.2 Installing the Driver	21
2.3 Activating the Driver	23
<b>3 Configuring and Administering the Core Driver</b>	<b>25</b>
3.1 Configuration Overview	25
3.1.1 Core Driver Configuration	26
3.1.2 Platform Services Configuration	26
3.2 Driver System Security Overview	26
3.2.1 Connection Security	26
3.2.2 ASAM Master User Security	27
3.3 Administration Overview	28
3.3.1 Monitoring Core Drivers	28
3.3.2 Monitoring Platform Services	28
3.3.3 Maintaining the Census	29
3.4 How to Use the Web Interface	30
3.4.1 Rights Required for Web Interface Use	30
3.4.2 Accessing the Web Interface	30
3.4.3 Logging Out of the Web Interface	30
3.4.4 Obtaining Additional Information	30
3.4.5 Maintaining Lists	31
3.5 Management Tasks	31
3.5.1 Configuring the Census	31
3.5.2 Configuring Core Drivers	34
3.5.3 Configuring the iManager Plug-In	42

3.5.4	Configuring Logs . . . . .	42
3.5.5	Configuring Platforms. . . . .	42
3.5.6	Configuring Platform Sets . . . . .	44
3.5.7	Configuring Provisioning . . . . .	46
3.5.8	Configuring Search Objects . . . . .	46
3.5.9	Configuring UNIX UID/GID Sets . . . . .	48
3.5.10	Displaying Component Status . . . . .	49
3.5.11	Viewing Driver Documentation. . . . .	49
3.5.12	Viewing Logs . . . . .	49
3.5.13	Displaying Provisioning Details . . . . .	50
3.5.14	Reviewing Naming Exceptions. . . . .	51
3.5.15	Reviewing Platform Errors . . . . .	51
3.5.16	Managing Trawls . . . . .	52
<b>4</b>	<b>Troubleshooting the Core Driver</b>	<b>53</b>
4.1	Obtaining Debugging Output . . . . .	53
4.1.1	Debugging the Core Driver . . . . .	53
4.2	Troubleshooting Core Driver Configuration Issues. . . . .	54
4.2.1	Rights Issues . . . . .	54
4.2.2	Platform Services Process / Authentication Services Issues. . . . .	54
4.2.3	Platform Receiver / Event Journal Services Issues . . . . .	54
4.2.4	Census Issues . . . . .	54
4.2.5	LDAP Issues . . . . .	55
4.3	Troubleshooting Network Issues . . . . .	55
4.4	Troubleshooting eDirectory Issues. . . . .	56
<b>A</b>	<b>Migrating from Novell Account Management 3.0</b>	<b>57</b>
A.1	Migration Procedure . . . . .	57
A.2	Object Migration Details . . . . .	58
<b>B</b>	<b>Password Change Validation Exit</b>	<b>61</b>

# About This Guide

This guide provides you with the information you need to plan for, install, configure, administer, and troubleshoot the core driver of the Novell® Identity Manager Fan-Out driver. This guide assumes that you have knowledge of eDirectory™ and the operating system on which the core driver is installed, and that you are familiar with the concepts and facilities of the driver.

This guide is organized into the following sections:

- ♦ Chapter 1, “Core Driver Planning,” on page 9
- ♦ Chapter 2, “Installing the Driver,” on page 21
- ♦ Chapter 3, “Configuring and Administering the Core Driver,” on page 25
- ♦ Chapter 4, “Troubleshooting the Core Driver,” on page 53
- ♦ Appendix B, “Password Change Validation Exit,” on page 61

## Additional Documentation

The following publications contain information about the Identity Manager Fan-Out driver. These publications are available at the [Identity Manager Driver Web site \(http://www.novell.com/documentation/dirxml/drivers\)](http://www.novell.com/documentation/dirxml/drivers).

*Concepts and Facilities Guide*

*Core Driver Administration Guide*

*Platform Services Planning Guide and Reference*

*Platform Services Administration Guide for Linux and UNIX*

*Platform Services Administration Guide for MVS*

*Platform Services Administration Guide for OS/400*

*NetWare Intercept and API Administration Guide*

*API Developer Guide*

*Messages Reference*

*Core Driver Quick Start Guide for Linux and Solaris*

*Core Driver Quick Start Guide for NetWare*

*Core Driver Quick Start Guide for Windows*

*Platform Services Quick Start Guide for AIX*

*Platform Services Quick Start Guide for FreeBSD, HP-UX, Linux, and Solaris*

*Platform Services Quick Start Guide for MVS CA-ACF2*

*Platform Services Quick Start Guide for MVS CA-Top Secret*

*Platform Services Quick Start Guide for MVS RACF*

*Platform Services Quick Start Guide for OS/400*

*NetWare Intercept and API Quick Start Guide*

Documentation for related products, such as Identity Manager and eDirectory, is available at the [Novell Documentation Web site \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

## Documentation Updates

For the most recent versions of -Identity Manager Fan-Out driver documentation, see the [Identity Manager Driver Web site \(http://www.novell.com/documentation/dirxmldrivers\)](http://www.novell.com/documentation/dirxmldrivers).

## 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. 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 UNIX\*, should use forward slashes as required by your software.

## User Comments

We want to hear your comments and suggestions about this manual and the other documentation included with the driver. To contact us, send e-mail to [namdoc@novell.com](mailto:namdoc@novell.com).



# Core Driver Planning

# 1

This section helps you plan for your deployment of the Novell® Identity Manager Fan-Out driver. If the Identity Manager Fan-Out driver is new to you, read the information presented in the *Concepts and Facilities Guide* before proceeding.

## 1.1 Configuration Planning

There are a number of issues to resolve in planning for your deployment of the Identity Manager Fan-Out driver. Considering these issues now will make your installation go more smoothly.

- ♦ Decide how you will deploy the use of the driver throughout your enterprise.

Do you want to start with a small subset of your platform systems? Do you want to start with a small subset of your user community?

Platforms can operate with Include/Exclude lists to control which users the driver handles for authentication, and which users the driver defers to the native authentication mechanism. Platforms can also operate with Include/Exclude lists to control which user accounts the driver manages using provisioning events and which user accounts are managed locally. For more information, see the *Platform Services Planning Guide and Reference*.

- ♦ Decide who will administer your driver configuration.

The Web interface is used to monitor and administer the driver. Make it available to these persons and ensure that they have the necessary rights to use it. For details about the rights needed for administrative functions, see [Section 3.4.1, “Rights Required for Web Interface Use,” on page 30](#)

- ♦ Decide which eDirectory™ servers in your network will run core drivers.

A writable replica of the partition holding the ASAM System container must reside on the LDAP host server used by a core driver.

Each object that is covered by a Census Search object must be present in a replica (full or filtered) on the system that hosts the primary core driver.

- ♦ Will you install additional core drivers to provide redundancy for Authentication Services?

The Platform Services Process includes load balancing and failover support to provide for continued processing should a core driver become unavailable.

- ♦ Will you install additional core drivers to provide redundancy for Identity Provisioning?

The Platform Receiver includes failover support to provide for continued processing if the core driver it normally uses for Identity Provisioning becomes unavailable.

- ♦ Decide where in your eDirectory tree the ASAM System container and ASAM Master User objects should go. Creating a special container for them is a good practice.

Make sure you set password policies appropriate for the ASAM Master User object.

For more information about requirements for the ASAM Master User, see [Section 3.2.2, “ASAM Master User Security,” on page 27](#).

- ♦ Decide upon your Census parameters.

Which objects in your eDirectory tree will be used as the source of Enterprise Users and Enterprise Groups? This depends on how you place User and Group objects in your directory.

When do you want to run a Census Trawl? Because the Census is maintained in real time using provisioning events, Trawls are used primarily to verify the consistency of the Census. Once a day is reasonable for most cases.

Do you want Enterprise Users whose User objects have been deleted from eDirectory to be automatically removed from the Census? They can be removed after remaining inactive for a specified number of days, or you can choose to manage inactive users manually.

Do you want to delay user password expiration until the end of the day of expiration? This can result in smoother operation for users on platforms with third-party systems that cache and reuse passwords during the day.

Do you want to immediately delete users and groups from platforms when they are deleted from eDirectory or are no longer covered by a Search object, or do you want to provide a grace period to recover from accidental changes?

For information about setting these parameters, see [“Configuring the Census” on page 31](#).

- ◆ How will you resolve naming exceptions?

For more information, see [Section 3.5.14, “Reviewing Naming Exceptions,” on page 51](#).

- ◆ Decide which systems in your network will run Platform Services.

User names, passwords, and group names must conform to the character set and length restrictions imposed by the platform operating system in order to participate in Authentication Services and Identity Provisioning on that platform. Determine how you will handle those that do not meet the restrictions.

- ◆ Decide how you will organize your Platform Sets. Each platform belongs to exactly one Platform Set. A Platform Set provides the relationship between a group of platforms and the Search objects that define their user and group population.
- ◆ Users and Groups have the same UID number and GID number on each UNIX platform in a Platform Set.

What UID and GID numbers do you want to reserve for local administrator use on UNIX platforms?

- ◆ Will any of your platforms use password replication? If so, you must ensure that the driver is notified of changes to passwords.

If your eDirectory is configured to fully support Universal Password, the driver is notified of password changes in eDirectory.

If you do not use Universal Password, you must install and configure the appropriate password intercepts.

For more information, see [“Password Replication Requirements” on page 14](#).

- ◆ Platforms configured to use password replication do not normally receive provisioning events for user accounts until the passwords for these accounts are known to the -driver.

The driver uses system intercepts or Universal Password to collect password information. Users must either change their passwords where these are installed and configured, or authenticate on a driver platform before they can be populated onto a platform that uses password replication (Permit Password Replication specified as Yes for the Platform object in the Web interface).

By planning a staged deployment of the Identity Manager Fan-Out driver to the platforms in your enterprise so that most users have authenticated using other platforms first, you ensure the

availability of these users to password replication platforms when you are ready to deploy the driver on them.

- ♦ You can use the Identity Manager (DirXML®) to provision accounts to a different tree from the eDirectory tree you install the driver in. You can use the Novell Client™ Password Intercept to provide password change information back to the driver for password replication purposes from this tree. For more information, see “[External Password Sources](#)” on page 37.
- ♦ Consider how your own applications could benefit from the use of the AS Client API.  
Using the AS Client API is simple and straightforward. For more information about using the Client API, see the *API Developer Guide*.
- ♦ Will any of your Platform Receiver scripts need attributes other than those configured in the driver by default?

For a list of the attributes configured by default, see [Section 1.3.4, “Core Driver Requirements,”](#) on page 15.

To configure additional attributes, you must add them to the Event Subsystem DirXML Subscriber filter. For details about adding attributes to the DirXML Subscriber filter, see the *Identity Manager Administration Guide*.

The attribute names that you use in the DirXML Subscriber filter must be the eDirectory names.

If you are using attributes on an OS/400\* platform, you might need to map attribute names to their System Distribution Directory field names. This is done using the Attribute Name Mapping file. For more information about the Attribute Name Mapping file on OS/400, see the *Platform Services Administration Guide for OS/400*.

## 1.2 Configuration and Performance Guidelines

Many factors affect the performance of the Identity Manager Fan-Out driver. Performance is most critical for Authentication Services, such as Check Password and Get Context.

There are many relationships in the driver, and one or more of the factors described in the following sections can affect all of these relationships. Use the following as guidelines in planning and troubleshooting your Identity Manager Fan-Out driver installation.

Acceptable Authentication Services performance is achievable using two or three low-end servers for core drivers. However, if your present network experiences problems, such as slow logins related to eDirectory, Identity Manager Fan-Out driver operations will experience similar response problems.

For fault tolerance, your configuration should include core drivers running on several servers.

For fault tolerance, each core driver should use a different LDAP host server.

For optimal performance, each core driver and its LDAP host server should run on the same server.

### 1.2.1 eDirectory

Tuning eDirectory on your network is beyond the scope of this document. Much documentation on this subject is available elsewhere, including Novell Technical Information Documents (TIDs), which are available at the [Novell Support Web site \(http://support.novell.com\)](http://support.novell.com). The health and performance of eDirectory is critical to the ability of the driver to respond to Authentication Services requests and to deliver provisioning events in a timely manner. Therefore, the health and

performance of eDirectory should be your starting point in doing any performance planning and troubleshooting with the driver.

Factors in driver performance relative to eDirectory include

- ♦ The size of the eDirectory tree
- ♦ Communication links between the LDAP host servers used by core drivers, and servers holding replicas of the ASAM System container and other objects referenced by the driver
- ♦ LAN traffic
- ♦ Size of partitions containing relevant objects
- ♦ Performance of CPU and disks in servers holding relevant replicas
- ♦ Amount of memory in servers holding relevant replicas

The driver interfaces with eDirectory through LDAP. For LDAP tuning guidance, see the *Novell eDirectory Administration Guide*.

## 1.2.2 Object Services and the Event Subsystem

The Object Services component of the core driver is primarily responsible for maintaining the Census and other objects in the ASAM System container. Object Services receives provisioning events from the Event Subsystem, updates the Census as required, and passes the provisioning events to Event Journal Services. It is important for Identity Provisioning that the core driver be running at all times, but it is mostly a background process that does not require a great deal of processing power and is, for the most part, not a time-critical process.

Object Services performs Trawls to initially build and to verify the Census by performing a series of requests based on the Census Search objects defined in your configuration. For each Organizational Unit represented in the configuration, Object Services issues a single request to eDirectory to return all the objects contained in the given Organizational Unit.

Focus your Search objects to the specific directory locations of your users and groups rather than specifying a top level container object. This provides better feedback information during a Trawl and reduces the likelihood of an LDAP time-out because of slow servers or slow network links.

The Event Subsystem uses the Identity Manager to provide events to Object Services. The Event Subsystem requires minimal processing power, but it does require replicas for all objects that are monitored. Network connectivity and eDirectory synchronization are the primary performance factors for the Event Subsystem.

For optimal performance, a writable partition of all replicas containing objects contained in the Census should reside on the same server as the LDAP host server used by a core driver. However, be aware that operations that lock the directory on the local server, such as running NDSRepair, sometimes delay requests or cause them to fail.

Avoid using dynamic groups as Census Search objects because changes to dynamic groups do not trigger the Event Subsystem and are not recognized until the next Trawl.

## 1.2.3 Event Journal Services

Event Journal Services waits for Platform Receivers to connect, then provides pending events and a snapshot of User and Group objects for processing. Network connectivity to the platforms, and

proximity of the core driver to servers holding replicas of managed User and Group objects are the primary performance factors for Event Journal Services.

Platforms with very large numbers of managed users and groups should be connected to Event Journal Services with connections of adequate bandwidth to ensure that Full Sync Mode and Check Mode processing will complete within an acceptable time.

To reduce the number of concurrent connections that must be serviced by a core driver host, avoid using Persistent Mode on Platform Receivers.

## 1.2.4 Authentication Services

Authentication Services is responsible for processing requests made by Platform Services.

For optimal performance, LDAP host servers used by core drivers should hold a writable replica that contains the User objects represented in the Census, and other objects that might be referenced often by Authentication Services.

## 1.2.5 Platform Systems

Platform Services sends requests to the core driver. Platforms can be anything from a desktop workstation to a high-end mainframe system. The inherent performance of these systems is based on a number of factors, including

- ♦ System load
- ♦ The power of the system
- ♦ Network traffic
- ♦ Connectivity and bandwidth to the core drivers
- ♦ The number of core drivers defined in the configuration

Consider each of these as you configure each platform and as you select the location of the core drivers.

## 1.2.6 Platform Services / Authentication Services Relationship

The performance of the Platform Services / Authentication Services transaction is the most important performance relationship in the driver. The communication relies on the TCP/IP stack of the platform and Authentication Services server. TCP/IP configuration on the platform, the Authentication Services server, and the routers in between is the most important factor in the performance of servicing Authentication Services requests. Guidelines for configuring TCP/IP are beyond the scope of this guide. Refer to appropriate Novell and platform operating system documentation and TIDs for further information.

The Maximum Transmission Unit (MTU) TCP/IP parameter has been shown in testing to have an appreciable effect on performance in a situation in which the Authentication Services server is low on power. See Novell TID 2911035 (on the [Support Knowledgebase Web page \(http://support.novell.com\)](http://support.novell.com)) for more information on this topic.

Platform system planners should be aware of a mandatory three-second delay in reporting a bad password on a password check request. This delay is in eDirectory itself. It cannot be configured by the driver.

## 1.3 Requirements

The system requirements for driver components are described in the following sections. -Identity Manager Fan-Out driver components do not require the systems they run on to be dedicated solely to them.

### 1.3.1 User Rights Requirements

The installation and configuration of the driver require a user with full administrative rights and privileges in eDirectory and on the target systems. You can grant more limited rights to other users to use the Identity Manager Fan-Out driver Web interface for administrative functions. For details of rights needed for administrative functions, see [Section 3.4.1, “Rights Required for Web Interface Use,” on page 30](#).

### 1.3.2 Secure Sockets Layer Entropy Requirements for UNIX Systems

Secure Sockets Layer (SSL), used for secure communication between components, requires a source of entropy. Some UNIX implementations provide a `/dev/random` device for entropy. If your UNIX implementation does not include a `/dev/random` device, you must install an entropy daemon. You must also include an Entropy configuration parameter in your core driver configuration to specify the source of entropy. For more information about the Entropy parameter, see [“System Entropy Source” on page 36](#).

Solaris versions before Solaris 9 do not include a `/dev/random` device. Sun\* has released this functionality for versions 2.6 onward in Patch ID 112438-01.

### 1.3.3 Password Replication Requirements

If you use password replication, you must ensure that the driver is notified of changes to passwords.

- ♦ If your eDirectory is configured to fully support Universal Password, the driver is notified of password changes in eDirectory.
- ♦ If you do not use Universal Password, you must install and configure the appropriate password intercepts.
  - ♦ You must install the Novell Client Password Intercept on each Windows\* workstation that uses eDirectory. This intercept is distributed in the `intercepts\client32` directory of the distribution media.
  - ♦ You must install and run the NetWare® Password Intercept on all NetWare servers that run applications that use the eDirectory application programming interface (API) to change passwords in eDirectory. This intercept is distributed in the `intercepts\netware` directory of the distribution media.
- ♦ The OS/400 Password Validation Program Exit provides password change information from OS/400 platforms.

For information about installing and configuring the password intercepts, see the administration guide and the appropriate Quick Start for your platform operating system type.

## 1.3.4 Core Driver Requirements

- ☐ Novell Nsure Identity Manager 2.0.1 or later.
- ☐ Novell eDirectory versions supported by the Identity Manager version in use.
- ☐ One of the following OS platforms, in a version supported by the Identity Manager and eDirectory version in use:
  - ♦ NetWare
  - ♦ Windows
  - ♦ Linux\*
  - ♦ Solaris
- ☐ TCP/IP network connectivity.
- ☐ A writable replica of the partition that holds the ASAM System container must reside on the LDAP host server used by the core driver.
- ☐ Replicas (full or filtered) of objects covered by a Census Search object (primary core driver only).

The Identity Manager Fan-Out driver is configured for the attributes in the following lists. If you use filtered replicas, include the attributes shown in the following lists. If you add other attributes to the Subscriber filter, you must ensure that they are also available in your filtered replicas.

### Alias Attributes

- ♦ Aliased Object Name
- ♦ CN
- ♦ GUID

### User Attributes

- ♦ CN
- ♦ Group Membership
- ♦ GUID
- ♦ Login Disabled
- ♦ Surname

### ASAM-enterpriseUser Attributes

- ♦ ASAM-addTime
- ♦ GUID

### Group Attributes

- ♦ CN
- ♦ GUID
- ♦ Member

### Organizational Role Attributes

- ♦ CN
- ♦ GUID
- ♦ Role Occupant

---

**TIP:** iManager provides a wizard for setting up filtered replicas.

---

### 1.3.5 Requirements for Workstations Used for Installation and Administration

The workstations used to install, configure, and administer the driver must meet the following requirements.

- ☐ TCP/IP network connectivity.
- ☐ The ability to run iManager.
- ☐ Connectivity to the tree to be managed by the driver.
- ☐ If the installation computer runs UNIX, gzip and tar utilities.
- ☐ Connectivity to the file system of the computer that is to receive components being installed. If the installation computer is not the same as the target host, a drive must be mapped to the target host.

### 1.3.6 Platform Services Requirements

For a list of supported Platform Services operating systems and version requirements, see the *Concepts and Facilities Guide*.

## 1.4 Installation Planning Worksheet

You must provide certain information during the installation process. The Installation Planning Worksheet provides you with a convenient place to concisely record that information ahead of time for reference during the installation process.

For an overview of the installation process, see [Section 2.2, “Installing the Driver,” on page 21](#).

### 1.4.1 Installation Planning Worksheet

For a detailed explanation of the items on the Installation Planning Worksheet, see [“Items on the Installation Planning Worksheet” on page 18](#).

#### Census Search Objects

---

Object Name	Include Users	Include Groups	Expand	Include Aliases	Depth
-------------	---------------	----------------	--------	-----------------	-------

---



## Administrative Users

User Object	Rights

## UID/GID Sets

UID/GID Set Name	Reserved Range Lower Bound	Reserved Range Upper Bound

## Platform Sets

Platform Set Name	UID/GID Set	Search Objects

## Platforms

Platform Name	Platform Set	Permit PW Replication	Network Address

Platform Name	Platform Set	Permit PW Replication	Network Address

## 1.4.2 Items on the Installation Planning Worksheet

This section describes each of the items on the Installation Planning Worksheet

### Census Search Objects

Record Census Search object names and attributes. These describe how the Census is to be populated.

#### Object Name

The fully distinguished name of each Census Search object.

A Census Search object can be a User object, a Group object, an Organizational Role object, an Organization container object, or an Organizational Unit container object.

#### Include Users

Whether or not User objects covered by this Census Search object are added to the Census.

#### Include Groups

Whether or not Group objects covered by this Census Search object are added to the Census.

#### Expand

Whether or not users who are members of Group objects or occupants of Organizational Role objects covered by this Census Search object are added to the Census.

#### Include Aliases

Whether or not Alias objects covered by this Census Search object are added to the Census. The user or group object that is represented by an alias object is provisioned to platforms.

#### Depth

For container Census Search objects only: Indicate how many steps down the directory tree hierarchy beyond the Census Search object the driver searches for users and groups to add to the Census. Zero causes the search to stop at the container Search object.

### Administrative Users

The users to grant rights to administer the driver and the types of functions you will allow them to perform. For details, see [Section 3.4.1, “Rights Required for Web Interface Use,” on page 30.](#)

## **UID/GID Sets**

### **UID/GID Set Name**

The common name to give each UID/GID set in the ASAM System container.

### **Reserved Range Lower Bound and Reserved Range Upper Bound**

The low and high bounds of the range to reserve for the system administrator to use locally on the platform. The -driver does not assign UID/GID numbers in the reserved range.

## **Platform Sets**

A Platform Set provides the relationship between the Search objects that describe a collection of users and groups, and one or more platform systems that share the same users and groups.

### **Platform Set Name**

The name to give each Platform Set configuration object in the ASAM System container.

### **UID/GID Set**

The name of a previously defined UID/GID Set that is to be used to assign UID numbers and GID numbers for UNIX users and groups associated with the Platform Set.

### **Search Objects**

Search objects identify the users and groups to be used to populate the platforms that you add to this Platform Set.

A Platform Set Search object can be a User object, a Group object, an Organizational Role object, an Organization container object, an Organizational Unit container object, or a Dynamic Group object.

## **Platforms**

### **Platform Name**

The common name to give the Platform Configuration object in the ASAM System container.

### **Platform Set**

The name of the Platform Set this platform is to belong to.

### **Password Replication**

Whether or not requests for password replication information from eDirectory are honored for this platform.

### **Network Address**

The IP address or DNS name of the platform to be used for TCP/IP communications with other driver components. If your platform uses more than one network interface, list all of the addresses.



# Installing the Driver

# 2

Before you begin the installation of the Novell® Identity Manager Fan-Out driver, you should complete the planning process described in [Chapter 1, “Core Driver Planning,” on page 9](#), and you should be familiar with the topics presented in the *Concepts and Facilities Guide*.

Always check the [Novell Support Web Site \(http://support.novell.com\)](http://support.novell.com) for the latest support pack and product update information. Check the Release Notes and Readme files for the version you are installing for any special actions that might be required.

Many installation steps make use of the Identity Manager Fan-Out driver Web interface. If you are not familiar with using the Web interface, review [Section 3.4, “How to Use the Web Interface,” on page 30](#).

The topics in this section are

- ♦ [Section 2.1, “The ASAM Directory,” on page 21](#)
- ♦ [Section 2.2, “Installing the Driver,” on page 21](#)
- ♦ [Section 2.3, “Activating the Driver,” on page 23](#)

## 2.1 The ASAM Directory

The file system of each server that holds one or more Identity Manager Fan-Out driver components includes an ASAM directory. The ASAM directory contains the binary files, configuration information, and other related files used by the driver.

Because the ASAM directories contain sensitive information, you should implement the appropriate access controls to restrict their use to the driver system itself, and to its administrators.

## 2.2 Installing the Driver

For a smoother installation, complete the [Section 1.4, “Installation Planning Worksheet,” on page 16](#) before beginning, and refer to it during the installation process.

An overview of the process of installing the driver follows. For detailed step-by-step instructions, see the Quick Start guide for your operating system type. If you are upgrading from Account Management 3.0, see [Appendix A, “Migrating from Novell Account Management 3.0,” on page 57](#) for additional information.

- 1 Verify that the prerequisites have been met. For details, see [Section 1.3, “Requirements,” on page 14](#).
- 2 Verify that you have the latest support pack and product updates.
- 3 Obtain the core driver distribution package for your target operating system.
- 4 Run the core driver installation program and respond to the prompts, performing initial configuration.
- 5 Configure the Identity Manager (DirXML®) driver.
- 6 Populate your Census with the users and groups that you will use for your initial testing.

To do this, define Census Search objects and then run a Census Trawl. For details about this procedure, see [“Configuring the Census” on page 31](#).

The installation of the core driver creates indexes for specific attributes of objects in eDirectory™. For installation into a very large tree, these indexes take some time to bring online. Before you begin your first Trawl, verify that the indexes are in the online state. For the attributes indexed by the core driver installation, see the list that follows this procedure.

To view the Server object indexes and their state:

**6a** In iManager, select eDirectory Maintenance > Index Management.

**6b** Select the Server object for the core driver.

**7** Give Web interface users the rights they need.

For details, see [Section 3.4.1, “Rights Required for Web Interface Use,” on page 30](#).

**8** Define the UID/GID Sets that you will use for your initial testing. For details, see [“Configuring UNIX UID/GID Sets” on page 48](#).

**9** Define the Platform Sets that you will use for your initial testing. For details, see [“Configuring Platform Sets” on page 44](#).

You must define at least one UID/GID Set before you can define a Platform Set.

**10** Define the platforms that you will use for your initial testing. For details, see [“Configuring Platforms” on page 42](#).

You must define at least one Platform Set before you can define a platform.

**11** After testing, install additional core drivers for performance and redundancy.

**12** Activate the Identity Manager Fan-Out driver.

You can use the driver for evaluation purposes for 90 days. The driver will not work thereafter unless it has been activated. For details, see [Section 2.3, “Activating the Driver,” on page 23](#).

**13** Fully deploy the Identity Manager Fan-Out driver throughout your enterprise as you gain confidence and experience.

## Attributes Indexed by the Core Driver Installation

---

GUID	Object_Class
ASAM_inputGUID	ASAM_eGroupMembers
ASAM_eGroupMembership	ASAM_inputReference
ASAM_platformAssociation	ASAM_platformAssociation_SS
ASAM_aliases	ASAM-NetAddressList
ASAM_eventsUpTo	ASAM_deletesUpTo
ASAM_deletePendingsUpTo	ASAM_passwordsUpTo
ASAM_eventError_SS	ASAM_platformSetAssociation_SS
ASAM_UIDGIDAssociation_SS	ou
Country	Locality
Organization	Tree_Root

## 2.3 Activating the Driver

Identity Manager and Identity Manager drivers must be activated within 90 days of installation, or they shut down. You can activate Identity Manager products to a fully licensed state at any time.

To activate Identity Manager products:

- 1** Purchase the appropriate licenses.
- 2** Generate a Product Activation Request.
- 3** Submit the Product Activation Request to Novell.
- 4** Install the Product Activation Credential received from Novell.

For detailed information about completing these steps, see Activating Identity Manager Products in the *Identity Manager Administration Guide* (<http://www.novell.com/documentation/lg/dirxml20>).





# Configuring and Administering the Core Driver

# 3

This section tells you about configuring and administering the Novell® Identity Manager Fan-Out driver.

- ♦ [Section 3.1, “Configuration Overview,” on page 25](#)
  - ♦ [Section 3.1.1, “Core Driver Configuration,” on page 26](#)
  - ♦ [Section 3.1.2, “Platform Services Configuration,” on page 26](#)
- ♦ [Section 3.2, “Driver System Security Overview,” on page 26](#)
- ♦ [Section 3.3, “Administration Overview,” on page 28](#)
- ♦ [Section 3.4, “How to Use the Web Interface,” on page 30](#)
- ♦ [Section 3.5, “Management Tasks,” on page 31](#)
  - ♦ [“Configuring the Census” on page 31](#)
  - ♦ [“Configuring Core Drivers” on page 34](#)
  - ♦ [Section 3.5.3, “Configuring the iManager Plug-In,” on page 42](#)
  - ♦ [Section 3.5.4, “Configuring Logs,” on page 42](#)
  - ♦ [“Configuring Platforms” on page 42](#)
  - ♦ [“Configuring Platform Sets” on page 44](#)
  - ♦ [Section 3.5.7, “Configuring Provisioning,” on page 46](#)
  - ♦ [“Configuring Search Objects” on page 46](#)
  - ♦ [“Configuring UNIX UID/GID Sets” on page 48](#)
  - ♦ [“Displaying Component Status” on page 49](#)
  - ♦ [Section 3.5.11, “Viewing Driver Documentation,” on page 49](#)
  - ♦ [“Viewing Logs” on page 49](#)
  - ♦ [“Displaying Provisioning Details” on page 50](#)
  - ♦ [Section 3.5.14, “Reviewing Naming Exceptions,” on page 51](#)
  - ♦ [Section 3.5.15, “Reviewing Platform Errors,” on page 51](#)
  - ♦ [Section 3.5.16, “Managing Trawls,” on page 52](#)

## 3.1 Configuration Overview

There are two principal parts of the Identity Manager Fan-Out driver: the core driver and Platform Services. This section describes the core driver configuration. Additional configuration is performed on each platform.

### 3.1.1 Core Driver Configuration

Core driver configuration information is maintained in the Driver object and in objects in the ASAM System container. The core driver installation process creates the initial configuration.

You use iManager to maintain the configuration information.

For information about managing the Driver object configuration parameters, see [“Driver Object Configuration Parameters” on page 34](#). For information about managing the objects in the ASAM System container, see [Section 3.4, “How to Use the Web Interface,” on page 30](#) and [Section 3.5, “Management Tasks,” on page 31](#).

### 3.1.2 Platform Services Configuration

The core driver maintains configuration objects that represent each target platform for its own use in the ASAM System container.

Target platforms each obtain local configuration information from their respective platform configuration file. For more information about the platform configuration file, see the *Platform Services Planning Guide and Reference*.

## 3.2 Driver System Security Overview

### 3.2.1 Connection Security

The connections between core driver components and between Event Journal Services and Platform Receivers use Secure Sockets Layer (SSL). Some types of the Platform Services Process use SSL for their connections to Authentication Services, and others use DES encryption. SSL connections are authenticated through the use of certificates.

The certificates used by the Identity Manager Fan-Out driver are minted by the Certificate Services component of the core driver. When you install and configure a new component, you obtain a certificate.

Because platforms cannot examine the configuration objects for the core driver in the ASAM System container, core driver network address information is included in their certificates. This enables platforms to verify core driver component identity. If the network configuration of a core driver is changed, a new certificate must be minted.

The core driver certificate is minted when you start the core driver for the first time. When you update network address information for a core driver, a new certificate is automatically minted for it. You must restart a core driver after changing its network address information in order for the new certificate to take effect.

Obtain a new certificate for a platform by starting the Platform Receiver with the appropriate command line parameter. For details, see the administration guide for your platform operating system type.

Identity Manager Fan-Out driver components store their security certificates and related information in their certs directory. Ensure that access to the certs directory is restricted to the driver system itself and to its administrators.

- ♦ **Core Driver:** `asam\data\coredriver\certs`
- ♦ **Platform Services:** `asam\data\platformservices\certs`

### 3.2.2 ASAM Master User Security

The core driver performs an LDAP bind as the ASAM Master User to gain access to eDirectory™. You must not place restrictions on the ASAM Master User object that would interfere with its use by the driver. Set maximum password length for the ASAM Master User to at least 32 characters. Disable intruder detection for the ASAM Master User object so that it cannot be disabled by someone without the appropriate rights.

The ASAM Master User must have Supervisor rights to the container in eDirectory that holds the users and groups that can be added to the Census. This is known as the User and Group Subtree. These rights are granted during installation.

To use the AS Client API to access objects outside of the User and Group Subtree, you must grant additional rights to the ASAM Master User.

- ♦ You must grant the ASAM Master User Browse object rights and Compare property rights to any object that is accessed through the AS Client API.
- ♦ You must grant the ASAM Master User Read property rights to any object whose Security Equals list or Group Membership list, or other attribute value is accessed through the AS Client API.

Because the ASAM Master User is granted significant rights, you must ensure that its password remains secure.

-The core driver obtains the password of the ASAM Master User from the Driver object. If your security practices prescribe periodic password changes, you can create a second User object to be used as an alternate ASAM Master User. Then you can swap back and forth between these User objects when it is necessary to change the password.

#### Creating an Alternate ASAM Master User Object

- 1 Use iManager to create a new User object. We recommend that you use the same directory context as the original ASAM Master User object.
- 2 Use iManager to assign the new User object Security Equivalence to the original ASAM Master User object.

Now you have two User objects with the necessary rights to act as the ASAM Master User.

#### Changing the Password and Updating the Configuration

In the following procedure, we assume that you have created a second ASAM Master User object as described in the preceding section. We assume that one object is named “ASAM1” and the other is named “ASAM2”. We also assume that ASAM1 is in use and that it is the one listed in the driver configuration parameters.

To change the ASAM Master User object to use a new password:

- 1** Use iManager to set the new password for ASAM2.
- 2** Update the Driver object for each core driver, specifying ASAM2 for the Authentication ID, and the new password for the Application Password.
  - 2a** In iManager, select DirXML Management > Overview.
  - 2b** Locate the driver in its driver set.
  - 2c** Click the driver status indicator in the upper right corner of the driver icon, then click Edit Properties.
  - 2d** Click DirXML > Driver Configuration. Authentication ID and Application Password are located under the Authentication heading.
- 3** Use iManager to change the password of ASAM1 to an undisclosed randomly chosen value.

ASAM2 is now the ASAM Master User, using a new password. The old password (of the ASAM1 user) can no longer be used.

---

**NOTE:** The core driver does an LDAP bind as the ASAM Master User upon startup. There is no need to restart the driver now. It will use ASAM2 the next time it is started.

---

## 3.3 Administration Overview

You use the Web interface for most core driver configuration and administration tasks. For details about using the Web interface, see [Section 3.4, “How to Use the Web Interface,” on page 30](#).

The ongoing tasks of administering the driver can be grouped into the following categories.

- ♦ Monitoring the operation of the core drivers
- ♦ Monitoring the operation of Platform Services
- ♦ Maintaining the Census
- ♦ Reviewing your overall system management plan and making changes to the driver as appropriate

### 3.3.1 Monitoring Core Drivers

You can use the Web interface to view component status. For additional information, see [“Displaying Component Status” on page 49](#).

From time to time, depending on the size of the organization and the amount of activity, a system administrator should review the logs written by core driver components in order to check the health of the system. For example, you might want to investigate the cause of a large number of denied SSL connection requests. For more information about viewing logs, see [“Viewing Logs” on page 49](#).

The messages generated by the driver are documented in the *Messages Reference*.

### 3.3.2 Monitoring Platform Services

It is a good idea to monitor the logs written by Platform Services. For details about these logs, see the administration guide for your platform operating system.

### 3.3.3 Maintaining the Census

Administrative personnel should periodically use the Web interface to monitor naming exceptions and inactive users and groups. The frequency at which this is done is a function of the size of the organization being managed, the rate at which changes take place, and the rules in place within the organization concerning unique user IDs in eDirectory. If the organizational structure is appropriate, the same people who manage User objects also maintain the Census.

The actions taken depend on the policies of the individual organization. Some guidelines follow. For a review of the concepts, see the *Concepts and Facilities Guide*.

#### Naming Exceptions

A naming exception results if a new User object or a new Group object is encountered with the same name as an Enterprise User object or Enterprise Group object that is already in the Census. In an organization with a policy of unique usernames, this is generally the result of a mistake when adding a new user or group. In this case, the name of the new user or group should be changed to a unique name.

It is also possible that the new user or group was inadvertently added to the Census as a result of a mistake in changing the Census parameters so that the driver is now looking in unintended places for users or groups. In this case, correct the Census parameters.

It is also possible that a departmental administrator is attempting to breach security by taking the user ID of a previously existing user.

#### Inactive Users and Groups

An inactive user or group is an Enterprise User or Enterprise Group whose corresponding User object or Group object has been deleted from the directory or is no longer covered by a Census Search object. Deletion of a user might be the legitimate result of someone leaving the organization. If this is true, the entry should be removed from the Census.

It is possible that the user or group has been inadvertently omitted from the Census as a result of a mistake in changing the Census parameters. If this is the case, correct the Census parameters.

You can use the Web interface to set Census parameters to automatically remove inactive users and groups from the Census if this is appropriate for your organization. For details, see [“Specifying Automatic Removal of Inactive Users and Groups” on page 33](#).

Enterprise User objects in the Census relate to eDirectory User objects using a globally unique identifier (GUID). Identity Provisioning uses the GUID to prevent the reuse of a User object name from resulting in inappropriate access to the old user's accounts on platform systems. You must ensure that the deleted ID has been appropriately removed from all target platforms not managed by Identity Provisioning.

A user that is inactive or is not present in the Census, but does exist in eDirectory, is able to log in to eDirectory directly, but is not able to authenticate through the driver where the Enterprise User ID is required (such as is the case with MVS\* or UNIX).

A user that is present in the Census but is not present in eDirectory is not able to authenticate through the driver.

## 3.4 How to Use the Web Interface

You configure and administer the -Identity Manager Fan-Out driver using iManager Roles and Tasks.

The left side of the display lists actions you can take. Information pertaining to the action you select is displayed on the right side.

For more information about iManager, see the *Novell iManager Administration Guide*.

### 3.4.1 Rights Required for Web Interface Use

To use the Web interface, a user must have greater than normal user rights as shown in the following table.

Function	Rights
Log in and perform basic functions	Read object rights to the ASAM System container
Configure objects	Read and Create object rights to the ASAM System container
Start a Trawl	Read and Create object rights to the ASAM System container

### 3.4.2 Accessing the Web Interface

To access the Web interface, log in to iManager, click the Roles and Tasks icon at the top of the iManager screen, and click the desired -Fan-Out Driver Configuration or Fan-Out Driver Utilities task.

### 3.4.3 Logging Out of the Web Interface

To log out of the Web interface, click the exit door icon at the top of the iManager screen.

### 3.4.4 Obtaining Additional Information











**Figure 3-1** *Additional Information Icon*



Additional information is available for the items and procedures in the Web interface. To display this information, click the Additional Information icon.

## 3.4.5 Maintaining Lists

**Figure 3-2** *List of Items*

① Platforms		
Remove	Platforms	Platform Set
	 <a href="#">Guests</a>	 <a href="#">Academic Systems</a>
	 <a href="#">Students</a>	 <a href="#">Academic Systems</a>
	 <a href="#">Teachers</a>	 <a href="#">Academic Systems</a>
		

Many items in the Web interface are grouped into lists.

To add an item to a list, click the Add button.

To view or change the attributes of an item, click its name in the list.

To remove an item from a list, click the Remove button for that item. A confirmation page is displayed. Click Yes to confirm removal, or click your Web browser's Back button to abort.

## 3.5 Management Tasks

This section describes how to perform management tasks for the Identity Manager Fan-Out driver.

- ♦ [“Configuring the Census” on page 31](#)
- ♦ [“Configuring Core Drivers” on page 34](#)
- ♦ [Section 3.5.3, “Configuring the iManager Plug-In,” on page 42](#)
- ♦ [Section 3.5.4, “Configuring Logs,” on page 42](#)
- ♦ [“Configuring Platforms” on page 42](#)
- ♦ [“Configuring Platform Sets” on page 44](#)
- ♦ [Section 3.5.7, “Configuring Provisioning,” on page 46](#)
- ♦ [“Configuring Search Objects” on page 46](#)
- ♦ [“Configuring UNIX UID/GID Sets” on page 48](#)
- ♦ [“Displaying Component Status” on page 49](#)
- ♦ [Section 3.5.11, “Viewing Driver Documentation,” on page 49](#)
- ♦ [“Viewing Logs” on page 49](#)
- ♦ [“Displaying Provisioning Details” on page 50](#)
- ♦ [Section 3.5.14, “Reviewing Naming Exceptions,” on page 51](#)
- ♦ [Section 3.5.15, “Reviewing Platform Errors,” on page 51](#)
- ♦ [Section 3.5.16, “Managing Trawls,” on page 52](#)

### 3.5.1 Configuring the Census

- ♦ [“Specifying Search Objects” on page 32](#)
- ♦ [“Specifying Trawl Times” on page 32](#)
- ♦ [“Specifying Automatic Removal of Inactive Users and Groups” on page 33](#)

- ♦ [“Delaying Password Expiration Until Midnight” on page 33](#)
- ♦ [“Specifying a Platform Object Delete Pending Duration” on page 33](#)

## Specifying Search Objects

Search objects specify how users and groups are selected from eDirectory to be included in the Census. For details about Search objects, see [“Configuring Search Objects” on page 46](#).

To update the Census after you make Search object changes, start a Trawl. For details about starting a Trawl, see [“Starting a Census Trawl” on page 52](#).

To add a new Census Search object:

- 1 Click Fan-Out Driver Configuration > Configure Census. The Census Configuration page is displayed.
- 2 Click Search Objects > Add. The Add a Search Object page is displayed.
- 3 Specify the Search object distinguished name and attributes as desired, then click Apply.  
For details about Search object attributes, see [“Search Object Attributes” on page 47](#).

To change a Census Search object:

- 1 Click Fan-Out Driver Configuration > Configure Census. The Census Configuration page is displayed.
- 2 In the list of Search objects, click the name of the Search object to modify. The Modify Search Object page is displayed.
- 3 Update the attributes of the Search object as desired, then click Apply.  
For details about Search object attributes, see [“Search Object Attributes” on page 47](#).

To remove a Census Search object:

- 1 Click Fan-Out Driver Configuration > Configure Census. The Census Configuration page is displayed.
- 2 In the list of Search objects, click the name of the Search object to be deleted. The Modify Search Object page is displayed.
- 3 In the list of Platform Sets under Platform Set Associations, click each Remove button. The Remove Search Object confirmation page is displayed each time you click a Remove button. Click Yes for each.
- 4 Under the In Census heading, click the Remove button. The Remove Search Object confirmation page is displayed. Click Yes.

## Specifying Trawl Times

Object Services is notified by the Event Subsystem of events in eDirectory that affect the Census. Object Services also periodically verifies the consistency of the Census by examining objects in the directory in a procedure known as a Trawl. Use the Web interface to specify the times when a Trawl runs.

- 1 Click Fan-Out Driver Configuration > Configure Census. The Census Configuration page is displayed.



- 2 Trawl times are listed (24-hour clock) under Trawl Time Configuration. If no times are listed, Object Services does not automatically start any Trawls.

Time of day values used by the driver are specified in Universal Time, formerly known as GMT, and commonly abbreviated as Z.

To add a new Trawl time, click Add.

To remove a Trawl time from the list, click its Remove button.

## Specifying Automatic Removal of Inactive Users and Groups

You can choose to have Enterprise Users and Enterprise Groups whose corresponding User object or Group object is deleted from eDirectory or no longer covered by a Census Search object remain in the Census in an inactive state. This prevents another person from receiving access to resources as an unintended result of the reuse of a user name. Inactive users cannot authenticate through Authentication Services.

You can also specify that inactive users and groups be removed from the Census automatically during a Trawl after they have reached a given number of inactive days.

To specify inactive user and group options:

- 1 Click Fan-Out Driver Configuration > Configure Census. The Census Configuration page is displayed.
- 2 Inactive user and group options are listed on the Census Configuration page under Inactive Enterprise User and Group Actions. Specify the action you want, then click Apply.

To view inactive users and groups, use the Provisioning Details utility and specify Search Type > Inactive Users and Groups. For more information about using the Provisioning Details utility, see [“Displaying Provisioning Details” on page 50](#).

## Delaying Password Expiration Until Midnight

You can choose to delay the expiration of user passwords by Authentication Services from the exact date and time set for them in eDirectory until the end of the day (local time of the core driver host server) on which they expire. This can result in smoother operation for users on platforms with third-party systems that cache and reuse passwords during the day.

To specify password expiration options:

- 1 Click Fan-Out Driver Configuration > Configure Census. The Census Configuration page is displayed.
- 2 Password expiration options are listed on the Census Configuration page under Delay User Password Expiration. Select the option you prefer, then click Apply.

## Specifying a Platform Object Delete Pending Duration

You can use the Web interface to specify a Delete Pending Duration. During this interval, User and Group objects associated with a platform that have either been deleted from eDirectory or are no longer covered by a Search object, are not deleted from their corresponding platforms. The results of a Delete User or Delete Group Receiver script can be difficult to reverse. This provides a grace period to allow recovery from a mistake affecting many users.

The User Delete Pending or Group Delete Pending script is called when a delete event becomes pending for a user or group, but the Delete User or Delete Group script is not called until the Delete Pending Duration expires.

To specify when users and groups are deleted from platforms:

- 1 Click Fan-Out Driver Configuration > Configure Census. The Census Configuration page is displayed.
- 2 Deletion options are listed under Platform Object Delete Pending Duration. Select the option you prefer, then click Apply.

## 3.5.2 Configuring Core Drivers

Core drivers provide the Web interface, perform Census maintenance functions, and provide Authentication Services and Identity Provisioning to platforms.

### Starting a Core Driver

- 1 In iManager, select DirXML Management > Overview.
- 2 Locate the driver in its driver set.
- 3 Click the driver status indicator in the upper right corner of the driver icon, then click Start Driver.

### Stopping a Core Driver

- 1 In iManager, select DirXML Management > Overview.
- 2 Locate the driver in its driver set.
- 3 Click the driver status indicator in the upper right corner of the driver icon, then click Stop Driver.

### Driver Object Configuration Parameters

The core driver uses Driver object configuration parameters to identify the ASAM System container, the ASAM Master User object, an LDAP Services for eDirectory host server, and to obtain other related information. The Driver object is created during core driver installation.

To view and modify Driver object configuration parameters:

- 1 In iManager, select DirXML Management > Overview.
- 2 Locate the driver in its driver set.
- 3 Click the driver status indicator in the upper right corner of the driver icon, then click Edit Properties.
- 4 Click DirXML > Driver Configuration. Driver configuration parameters are located under the Driver Settings heading.
- 5 Update the settings as desired. Then click OK or Apply. To end without saving any changes, click Cancel.

## LDAP Host and Port

Specifies the IP address or DNS name and the TCP port of the LDAP Services for eDirectory host server that the core driver components use to access the ASAM System container. The LDAP host server must hold a writable replica of the ASAM System container.

The default is port 636 on the local host.

For best performance, use the local host.

## Install Directory

Specifies the file path for the ASAM directory where the core driver is installed. The core driver uses this parameter to find files needed for execution.

## Locale

Specifies the two-character ISO 639 language identifier for the language to be used by the core driver.

The default value of Locale is en (English).

## ASAM Master User

Specifies the fully distinguished name of the ASAM Master User object. Driver components do an LDAP bind as the ASAM Master User.

---

**IMPORTANT:** The ASAM Master User and ASAM Master User Password driver settings are used for installation compatibility only. If you want to change these values after you have completed the installation process, you must use the Authentication ID and Application Password configuration values. These configuration values are located under the Authentication heading.

---

## ASAM Master User Password

Specifies the password of the ASAM Master User object.

---

**IMPORTANT:** The ASAM Master User and ASAM Master User Password driver settings are used for installation compatibility only. If you want to change these values after you have completed the installation process, you must use the Authentication ID and Application Password configuration values. These configuration values are located under the Authentication heading.

---

## ASAM System Container

Specifies the fully distinguished name of the ASAM System container. The ASAM System container holds system configuration and operational objects.

## Storage Key

Specifies the key that is used for storing and retrieving password replication information. It must not be changed after the driver has begun storing password information.

The value of the key must be sixteen printable characters. The same value must be used by every core driver in your configuration.

The Storage Key is generated during installation of the first core driver. When you install additional core drivers, the installation process obtains the Storage Key from the primary core driver.

### Debug Options

Specifies debugging options for the core driver. Leave this empty unless instructed otherwise by Novell Technical Support.

### Debug Log File

Specifies the name of the file where debugging information is written.

### Debug to DSTrace

Specifies whether or not debugging information is written to DSTrace (in addition to the Debug Log file).

### Migration Mode Password

Specifies the special password that is used with Password Migration. Users with this password and with Login Disabled set are in the migration state. For more information about Password Migration, see the *Platform Services Administration Guide for MVS*.

### Syslog Facility

Specifies the SYSLOG facility name used for logging system messages for a core driver installed on a UNIX host system. The SYSLOG Facility parameter is not used for other operating systems.

The possible values for a specific UNIX system are mapped by the syslog.h file of that system.

The default SYSLOG facility is LOG\_DAEMON.

### System Entropy Source

Specifies the file where core driver components installed on a UNIX host system obtain entropy for SSL. The Entropy parameter is not used on other operating systems.

If Entropy is not specified, the default is to use the /dev/random device for entropy. If there is no /dev/random device, the default entropy file is /etc/entropy.

If your system has a /dev/random device, you do not need to specify Entropy.

### Change Password Exit Library

Specifies the file path for the optional Password Change Validation Exit library. For information about the Password Change Validation Exit, see [Appendix B, “Password Change Validation Exit,” on page 61](#).

### Change Password Exit Function

Specifies the function name for the optional Password Change Validation Exit exported in the library identified by the Change Password Exit Library parameter. For information about the Password Change Validation Exit, see [Appendix B, “Password Change Validation Exit,” on page 61](#).

## External Password Sources

Specifies a comma-separated list of names of additional trees from which the core driver accepts password change information.

If no External Password Source is specified, the core driver rejects password change information from trees other than the tree the core driver is installed in.

Password change information is provided to the core driver by Identity Manager Fan-Out driver password intercepts, and is used to provide password information to password replication platforms.

## Maintain Password Case

Specifies whether or not Event Journal Services changes password case when sending password replication information to Platform Receivers.

Password replication information is provided to the core driver from many different sources. Maintaining password case can be undesirable because some sources of password information present passwords in uppercase.

By default, Event Journal Services converts passwords to lowercase before sending password replication events to Platform Receivers.

## Core Driver DN

Displays the name of this Driver object.

## Discard Events

Specifies whether or not the Event Subsystem ignores event notifications from eDirectory. This should be set to false, except as instructed by Novell Technical Support.

## Activation Group

Displays the Identity Manager integration modules that you have activated.

## Core Driver System Configuration Object Attributes

### Network Address

The core driver configuration must list all of the network addresses of the core driver's host server. Network address information for the host server is entered when the core driver is installed. You must update this information if the host server network address is changed or if an additional network interface is installed in the server.

One network address is designated as the default. Identity Manager Fan-Out driver core driver components use the default address to connect to each other.

The platform configuration file used by a Platform Services component specifies the network address of each core driver that is used by that component. If you change the network address of a core driver that is specified in a platform configuration file, you must update that platform configuration file. For details about the platform configuration file, see the *Platform Services Planning Guide and Reference*.

If you change the network address configuration of a core driver, a new certificate is automatically minted for the core driver.

---

**IMPORTANT:** You must restart the core driver for the new certificate to take effect.

---

### Core Driver Port

The TCP port number used by the core driver defaults to 3451. You can change the core driver TCP port number if necessary.

If you change a core driver TCP port number, you must also make the corresponding changes to each platform configuration file that references the core driver.

### Authentication Services MVS and NDS-AS Compatibility Port

The TCP port number used by the core driver to communicate with Platform Services for MVS and with NDS<sup>®</sup> Authentication Services (NDS-AS) version 3 Clients. The default is 2000.

### Cache Size and Time to Live

Authentication Services maintains an encrypted cache of recent successful authentication requests to provide better performance for applications, such as Web servers, that make large bursts of requests to authenticate the same user in a short period of time.

You can specify the amount of memory that is allocated for this cache and the maximum length of time an entry is to be kept in the cache.

### Primary Core Driver

One core driver is designated as the primary core driver. Other core drivers are known as secondary core drivers. The primary core driver serves the Web interface and provides environmental information during the installation process for other core drivers. Only the primary core driver listens for events from eDirectory and performs Trawls.

### Designating the Primary Core Driver

- 1 In the Web interface, click Fan-Out Driver Configuration > Configure Core Drivers. The Core Driver Configuration page is displayed.
- 2 Click Set as Primary.
- 3 Click Yes to confirm.
- 4 Restart the previous and new core drivers. For details about this procedure, see [“Stopping a Core Driver” on page 34](#) and [“Starting a Core Driver” on page 34](#).
- 5 Configure the iManager plug-in to use the new primary core driver. For details, see [Section 3.5.3, “Configuring the iManager Plug-In,” on page 42](#).

Before changing which core driver is the primary core driver, ensure that the proposed new primary core driver holds replicas of all objects covered by Census Search objects.

### Adding a Core Driver

For step-by-step instructions to add a core driver, see the Quick Start for your operating system type.

- ♦ *Core Driver Quick Start Guide for Linux and Solaris*

- ♦ *Core Driver Quick Start Guide for NetWare*
- ♦ *Core Driver Quick Start Guide for Windows*

## Changing the Core Driver Configuration

- 1 In the Web interface, click Fan-Out Driver Configuration > Configure Core Drivers. The Core Driver Configuration page is displayed.
- 2 Click the name of the core driver whose configuration you want to change. The Modify Core Driver page is displayed.
- 3 Specify attributes for the core driver as appropriate.

## Removing a Core Driver

- 1 Remove the core driver from the platform configuration file of all platforms where it is present. For information about the platform configuration file, see the *Platform Services Planning Guide and Reference*.
- 2 Stop the core driver.  
For details, see [“Stopping a Core Driver” on page 34](#).
- 3 Uninstall the core driver software and related files from the core driver host.
  - ♦ If the host server operating system is NetWare® or UNIX, delete the ASAM directory from the file system.
  - ♦ If the host server operating system is Windows, use Windows Control Panel > Add/Remove Programs.
- 4 Remove the Driver object from Identity Manager (DirXML®).
  - 4a In iManager, select DirXML Management > Overview.
  - 4b Locate the driver set for the driver, then click Delete Driver.
  - 4c Select the core driver from the list and confirm its deletion.
- 5 In the Web interface, click Fan-Out Driver Configuration > Configure Core Drivers. The Core Driver Configuration page is displayed.
- 6 Click the Remove button for the core driver to be removed. The Remove core driver confirmation page is displayed. Click Yes to confirm.

## Maintaining Logs Used by the Core Driver

Audit Services writes operational and audit log messages for the core driver to the `asam\data\coredriver\logs` directory.

You can use the Web interface to view logs and to configure how messages are managed. For information about viewing the logs, see [“Viewing Logs” on page 49](#). For details about configuring the logs, see [Section 3.5.4, “Configuring Logs,” on page 42](#).

## Configuring Core Drivers for Remote Loader Operation

The Fan-Out core driver can be configured to load under the Novell Identity Manager Java Remote Loader. This configuration provides the Fan-Out core driver with greater system resources and provides an isolated environment for eDirectory and Identity Manager fault-tolerance.

To configure the Fan-Out core driver to use the Java Remote Loader, follow the initial installation steps outlined in the Quick Start guide, then perform the following additional steps:

- 1** Locate the directory for Fan-Out Driver Remote Loader files on the Connected System (created by the Identity Manager Connected System installation).

Default Paths:

Linux or Solaris: `/var/opt/novell/dirxml/rdxml`

Windows: `C:\Novell\RemoteLoader`

- 2** Edit Driver properties in Novell iManager:

- 2a** Under Driver Module, select the Connect to Remote Loader option.

- 2b** Set the Driver Object Password and make a note of it.

- 2c** Under Authentication, enter the following for Remote loader connection parameters:

`hostname={Connected System DNS name/IP address} port={Remote Loader port} kmo={certificate object}`

The default port is 8090, and it's recommended to use the SSL CertificateIP certificate, so a sample string would be:

`hostname=localhost port=8090 kmo="SSL CertificateIP"`

- 2d** Also under Authentication, set the Remote Loader Password and make a note of it.

- 2e** Under Driver Parameters, set the Is Remote Loader parameter to true.

The Driver Parameters should reflect the operating system of the Connected System. This will affect the Debug Log File and Install Directory settings.

- 2f** Also, on Linux and Solaris, Debug to DTrace and Log to DTrace should be disabled .

- 3** Export Certificate:

- 3a** In iManager, select eDirectory Administration > Modify Object.

- 3b** Locate the certificate object you specified in the kmo parameter above. The certificates are located in the top-level organization of the tree.

Example: `SSL CertificateIP - myserver.myorg`

Click OK to modify the object.

- 3c** Click the Certificates tab.

- 3d** Click the Export button to export the Trusted Root Certificate.

- 3e** Select No when asked to export the private key and click Next.

- 3f** Select File in Base64 format and click Next.

- 3g** Click Save the exported certificate to a file. Save the file with a .pem extension.

- 3h** Transfer the file to the directory you created above.

- 4** Create the Configuration File:

On Linux or Solaris:

- ♦ Create a text file in the directory you created on the Connected System, (Example: fanout.conf).

- ♦ Enter the contents of the file:

Description: Fan-Out Driver



Commandport: 8000

Connection: port=8090 rootfile={certificate file}

Module: /usr/local/ASAM/bin/CoreDriver/libasamcdrv.so

- ♦ Specify your certificate file in the -connection parameter above. The above values are default values which can be changed if necessary. See your *Identity Manager Administration Guide* for more parameter information.

On Windows:

- ♦ Start the Identity Manager Remote Loader Console application.
- ♦ Click the Add button to create a new instance.
- ♦ Enter a description in the Description box (Example: Fan-Out Driver).
- ♦ Select {ASAM folder}\bin\CoreDriver\asamcdrv.dll for the Driver.
- ♦ Specify a path and filename for the Config File.
- ♦ Enter the Remote Loader and Driver Object Passwords that you specified for the Driver in iManager.
- ♦ Check the box beside Use an SSL Connection, and select the certificate file that you exported.
- ♦ Change other settings as desired, and click OK.

#### 5 Secure the Remote Loader Driver:

The Remote Loader uses passwords to authenticate to IDM. Use the Remote Loader program to set these passwords.

On Linux or Solaris:

```
rdxml -config {config_file} -sp {Remote Loader password} {Driver  
Object password}
```

In the command above, substitute the passwords you specified when configuring the Driver in iManager.

On Windows: See step 4.

#### 6 Start the Remote Loader Driver:

**6a** Start the Driver engine component in iManager, as you would for a local driver.

**6b** Run the Remote Loader program on the Connected System:

Linux or Solaris: `rdxml -config {config_file}`

Windows: Select the Driver instance in the Remote Loader Console and click Start.

#### 7 Stop the Remote Loader Driver (when needed):

**7a** You will need to specify the Remote Loader Password in order to stop the instance.

Linux or Solaris: `rdxml -config {config_file} -u`

Windows: Select the Driver instance in the Remote Loader Console and click Stop.

**7b** You may then stop the Driver engine component in iManager.

### Reverting a Core Driver to Native Mode

To revert a core driver to native mode:

- 1 Stop the Driver and Driver Shim.

- 2 For the Driver object password and Remote loader password items, click Clear password.

---

**IMPORTANT:** If this is not done, the Fan-Out driver will not be able to authenticate and will not start up.

---

- 3 Under Driver Module, select the Native option and enter the native module for the OS:  
Linux or Solaris: `libasamcdrv.so`  
Windows: `libasamcdrv.dll`
- 4 Under Driver Settings, set Remote Loader Driver to false.
- 5 Make sure that other settings reflect the OS of the Identity Manager server hosting the Fan-Out Driver.
- 6 Save changes and restart the driver.

### 3.5.3 Configuring the iManager Plug-In

Each administrative user must configure the iManager plug-in to use the primary core driver.

- 1 In the Web interface, click Fan-Out Driver Configuration > Configure iManager Plug-In. The Configure iManager Plug-In page is displayed.
- 2 Specify the DNS name or IP address of the primary core driver host server.
- 3 Specify the TCP port number for the primary core driver. The default is 3451.
- 4 Click Apply.

### 3.5.4 Configuring Logs

Audit Services maintains the Operational Log and Audit Log files written by the core driver. You can use the Web interface to manage log files. You can choose to have log messages kept for a given number of days, or you can choose to have log messages kept permanently. You can also specify the components whose messages are written to the logs.

- 1 Click Fan-Out Driver Configuration > Configure Logs. The Log Configuration page is displayed.
- 2 Select the option that you want for log retention.
- 3 Select the components whose messages you want included in the logs.
- 4 Click Apply.

You can use the Web interface to view log messages. For more information, see [“Viewing Logs” on page 49](#).

The Log Configuration page is also used to configure debugging logging. For more information, see [Section 4.1, “Obtaining Debugging Output,” on page 53](#).

### 3.5.5 Configuring Platforms

A Platform object contains the configuration information the core driver uses to serve a platform for Authentication Services and Identity Provisioning. Additional configuration of Platform Services is performed on the platform. For detailed information about configuring and administering Platform

Services, see the *Platform Services Planning Guide and Reference* and the administration guide for your platform operating system type.

## Platform Attributes

### Platform Set

Each platform is a member of exactly one Platform Set. The Platform Set is used to associate users and groups with its member platforms. You specify the Platform Set that a platform belongs to when you create the Platform object. The Platform Set a platform belongs to cannot be changed after the Platform object is created.

### Permit Password Replication

You can specify whether or not requests from a platform for password replication information are honored. Enable this only for those platforms that need, and are trusted with, password information from eDirectory.

**No:** No password information is provided to the platform.

**Yes:** Password information is provided to the platform. No events for an account are sent to the platform unless password information for the account is available to the driver.

**If Available:** Password information is provided to the platform when it is available. Events for an account are sent to the platform even if no password information is available for the account. This setting can result in accounts being unprotected if it is used without password redirection.

After you enable password replication for a platform, you must restart the Platform Receiver if it is running in Persistent Mode or Polling Mode.

In order for password replication information to be available to a platform, the appropriate password change intercepts must be installed and correctly configured on all systems that can change passwords in eDirectory. For more information, see [“Password Replication Requirements” on page 14](#), the *Concepts and Facilities Guide*, and the administration guide for your platform operating system type.

### Platform Network Address

The DNS name or IP address of the platform system. If the platform system has more than one network interface, list all of the network addresses.

### DES Key

Information about the DES key that is used to encrypt communications with platforms that use the DES interface is stored in the Platform Configuration object. The platform configuration file of platforms that use the DES interface must contain the same DES key as the Platform Configuration object or communication attempts fail.

When you change the DES key, the previous key is saved in the Platform Configuration object. You can specify a time interval during which communications using the old key are accepted from the platform system. Specify an interval that gives you enough time to update the platform configuration file with the new DES key.

## Adding a New Platform

- 1 In the Web interface, click Fan-Out Driver Configuration > Configure Platforms. The Platform Configuration page is displayed.
- 2 Click Add. The New Event Driven Platform page is displayed.
- 3 Type a name for the platform, select the Platform Set the new platform is to join, then click Apply. The Modify Platform page is displayed.
- 4 Specify attributes for the platform as appropriate.  
For details, see [“Platform Attributes” on page 43](#).
- 5 Install the platform distribution package on the target server. For details, see the administration guide and the Quick Start for your platform operating system type.

## Changing Platform Attributes

- 1 In the Web interface, click Fan-Out Driver Configuration > Configure Platforms. The Platform Configuration page is displayed.
- 2 In the list of platforms, click the name of the platform to modify. The Modify Platform page is displayed.
- 3 Update the attributes of the platform as desired. For details, see [“Platform Attributes” on page 43](#).

## Removing a Platform

- 1 Remove the driver installation from the platform system. For details, see the administration guide for your platform operating system type.
- 2 In the Web interface, click Fan-Out Driver Configuration > Configure Platforms. The Platform Configuration page is displayed.
- 3 In the list of platforms, click the Remove button of the Platform object that you want to remove. The Remove Platform confirmation page is displayed. Click Yes to confirm.

## 3.5.6 Configuring Platform Sets

A Platform Set contains one or more Platform objects that share the same users and groups.

When you add a new Platform Set, you give it a name and associate a UID/GID Set with it. Then you add Search objects that describe what users and groups are provisioned to the platforms that belong to the Platform Set.

You may specify an Alternate Naming Attribute. When a user or group is provisioned to a Platform within this Platform Set, the Alternate Naming Attribute indicates the name that will be used.

After you have defined a Platform Set, you can create the Platform objects that represent its target platforms. For information about creating Platform objects, see [“Configuring Platforms” on page 42](#).

The Platform Set object's user and group population is described by one or more Search objects. For details about Search objects, see [“Configuring Search Objects” on page 46](#).

## Platform Set Attributes

### UID/GID Set Association

When you create a Platform Set, you specify a UID/GID Set that is used to assign UID numbers and GID numbers to UNIX platforms that are members of the Platform Set. You cannot change the UID/GID Set assigned to Platform Set after the Platform Set has been created.

### Alternate Naming Attribute

The Alternate Naming Attribute specifies which attribute of user and group objects contains the name to be used when provisioned to Platforms. The content of an attribute that is designated as an Alternate Naming Attribute should be either a single value or multiple values of the form.

### Search Objects

Search Objects designate the users and groups from the Census that are used to populate the platforms that are members of the Platform Set. For information about Search objects, see [“Configuring Search Objects” on page 46](#).

### Platforms

Upon creation, each Platform object is associated with exactly one Platform Set.

## Adding a Platform Set

- 1 In the Web interface, click Fan-Out Driver Configuration > Configure Platform Sets. The Platform Set page is displayed.
- 2 Click Add. The New Platform Set page is displayed.
- 3 Specify an Alternate Naming Attribute if one should be used.
- 4 Type a name for the new Platform Set, select the UID/GID Set that is to be used by the new Platform Set, then click Apply. The Modify Platform Set page is displayed.
- 5 Add one or more Search objects to describe the user and group population for the Platform Set. Click Search Objects > Manage.

For details about Search objects, see [“Configuring Search Objects” on page 46](#).

- 6 Add one or more Platform objects to describe the target platforms that constitute the Platform Set. Click Platforms > Add to create a new Platform object and add it to the Platform Set.

For details about adding Platform objects, see [“Configuring Platforms” on page 42](#).

## Changing Platform Set Attributes

- 1 In the Web interface, click Fan-Out Driver Configuration > Configure Platform Sets. The Platform Set page is displayed.
- 2 In the list of Platform Sets, click the name of the Platform Set to modify. The Modify Platform Set page is displayed.
- 3 Update the attributes of the Platform Set as desired.

## Removing a Platform Set

- 1 Remove all platforms associated with the Platform Set.

For information about removing a platform, see [“Removing a Platform” on page 44](#).

- 2 In the Web interface, click Fan-Out Driver Configuration > Configure Platform Sets. The Platform Set page is displayed.
- 3 Click the Remove button of the Platform Set you want to remove. The Remove Platform Set confirmation page is displayed. Click Yes to confirm.

## 3.5.7 Configuring Provisioning

### Provisioning Configuration Attributes

#### Objects Excluded from Provisioning

You can specify that certain objects are globally excluded from Identity Provisioning by the Identity Manager Fan-Out driver. You can list a fully distinguished LDAP object name or a simple common name. If you add an object that has already been provisioned to target platforms, the object is deleted from the target platforms.

#### Web Interface LDAP Time-Out

The time-out interval, in seconds, for LDAP operations initiated by the Web interface. If an LDAP request does not return within the time-out value, the operation fails.

#### Trawl and Provisioning LDAP Time-Out

The time-out interval, in seconds, for core driver LDAP operations. If an LDAP request by a core driver does not return within the time out-value, the operation fails.

### Changing Provisioning Attributes

- 1 In the Web interface, click Fan-Out Driver Configuration > Configure Provisioning. The Provisioning Configuration page is displayed.
- 2 Modify provisioning attributes as desired.

## 3.5.8 Configuring Search Objects

Search objects determine the users and groups that are included in the Census and Platform Set populations.

Start a Trawl after you make Search object changes. For details about starting a Trawl, see [“Starting a Census Trawl” on page 52](#).

## Search Object Types

Search objects can be any of the following:

- ♦ **User Objects:** Users who are Search objects are added to the Census.
- ♦ **Group Objects:** Groups that are Search objects are added to the Census. Members of groups that are Search objects are added to the Census.
- ♦ **Organizational Role Objects:** Occupants of Organizational Role objects that are Search objects are added to the Census.
- ♦ **Organization Objects and Organizational Unit Objects:** Container objects are scanned for users and groups to add to the Census.
- ♦ **Dynamic Group Objects:** Members of Dynamic Group objects that are Search objects are added to the Census.

The settings of the Include Users and Include Groups attributes described in the following section take precedence in determining which objects are added to the Census.

## Search Object Attributes

**Include Users:** Determines if users covered by the Search object are added to the Census.

**Include Groups:** Determines if groups covered by the Search object are added to the Census.

**Expand:** Determines if users who are members of Group objects or occupants of Organizational Role objects found inside a container Search object are added to the Census.

**Include Aliases:** Determines if Alias objects covered by the Search object are added to the Census. The User or Group object that is represented by an Alias object is provisioned to platforms.

**Depth:** Determines how many steps down the eDirectory tree hierarchy the core driver looks beyond the container object for users and groups to add to the Census. A Depth of zero causes the search to stop at the Search object container.

**In Census:** Determines if users and groups covered by this Search object are included in the Census.

**Platform Set Associations:** Specifies which Platform Sets this Search object is used to populate.

## Adding Search Objects

- 1 Click Fan-Out Driver Configuration > Configure Search Objects. The Search Objects page is displayed.
- 2 Click Add. The Add a Search Object page is displayed.
- 3 Specify the Search object distinguished name and attributes as desired, then click Apply.  
For details about Search object attributes, see [“Search Object Attributes” on page 47](#).

## Changing Search Object Attributes

- 1 Click Fan-Out Driver Configuration > Configure Search Objects. The Search Objects page is displayed.
- 2 In the list of Search objects, click the name of the Search object to modify. The Modify Search Object page is displayed.

- 3 Update the attributes of the Search object as desired, then click Apply.  
For details about Search object attributes, see [“Search Object Attributes” on page 47](#).

### Removing Search Objects

- 1 Click Fan-Out Driver Configuration > Configure Search Objects. The Search Objects page is displayed.
- 2 In the list of Search objects, click the name of the Search object to be deleted. The Modify Search Object page is displayed.
- 3 In the list of Platform Sets under Platform Set Associations, click each Remove button. The Remove Search Object confirmation page is displayed each time you click a Remove button. Click Yes for each.
- 4 Under the In Census heading, click the Remove button. The Remove Search Object confirmation page is displayed. Click Yes.

## 3.5.9 Configuring UNIX UID/GID Sets

A UID/GID Set contains entries for users and groups, together with their corresponding UNIX UID and GID numbers.

A UID/GID Set is associated with each Platform Set so that the UID and GID numbers of users and groups managed by driver are the same on all UNIX platforms within the Platform Set.

When a new user or group is added to a Platform Set, it receives the next available UID/GID number.

You can reserve a range of numbers for local use by the platform administrators. The driver does not assign UID or GID numbers within the reserved range.

### UID/GID Set Attributes

#### Highest Used UID/GID

The highest UID/GID number that has been assigned to a user or group.

#### Reserved UID/GID Range

Specifies a range of UID/GID numbers that the driver does not assign to users or groups.

#### Associated Platform Sets

The Platform Sets that use this UID/GID Set.

### Adding a UID/GID Set

- 1 In the Web interface, click Fan-Out Driver Configuration > Configure UID/GID Sets. The UID/GID Set Configuration page is displayed.
- 2 Click Add. The New UID/GID Set page is displayed.
- 3 Type a name for the UID/GID Set configuration object in the ASAM System container.



- 4 Specify the lowest and highest numbers to be reserved for local system administrator use, then click Apply.

The value for these numbers cannot be changed after you create the UID/GID Set.

### Viewing UID/GID Set Details

- 1 In the Web interface, click Fan-Out Driver Configuration > Configure UID/GID Sets. The UID/GID Set Configuration page is displayed.
- 2 In the list, click the name of the UID/GID Set you want to view. The UID/GID Set Details page is displayed.

### Removing a UID/GID Set

- 1 Remove all Platform Sets associated with the UID/GID Set.  
For information about removing a Platform Set, see [“Removing a Platform Set” on page 46](#).
- 2 In the Web interface, click Fan-Out Driver Configuration > Configure UID/GID Sets. The UID/GID Set Configuration page is displayed.
- 3 Click the Remove button of the UID/GID Set you want to remove. The Remove UID/GID Set confirmation page is displayed. Click Yes.

## 3.5.10 Displaying Component Status

To display a status overview of your Identity Manager Fan-Out driver system, click Fan-Out Driver Utilities > Component Status in the Web interface.

To display status details for a component, click the component name on the Status Overview page.

## 3.5.11 Viewing Driver Documentation

You can use the Web interface to view documentation for the Identity Manager Fan-Out driver. To view the documentation, click Fan-Out Driver Utilities > Documentation.

## 3.5.12 Viewing Logs

You can use the Web interface to view log files. You can also use Audit to view log information.

### Starting the Log Viewer

To start the Log Viewer, click Fan-Out Driver Utilities > Log Viewer. The Component Log Viewer page is displayed.

### Controlling the Display

You can control the display of log files by setting the values of the following fields. Click Update Criteria after you have specified new values.

- ♦ **Component:** The component whose log you want to view.
- ♦ **Log Type:** The type of log for the selected component that you want to view. This can be the Operational Log or the Audit Log.

- ♦ **Lines to Return:** The number of lines to be returned at one time. This value determines the size of a set of lines used in scrolling operations, such as Next and Find Next.
- ♦ **Date:** The date of the log information that you want to display. Type this date in yyyy-mm-dd format. For example, specify June 26, 2004 as 2004-06-26.
- ♦ **Time:** The time of the first log record to display. Type the time in hh:mm:ss (24-hour clock) format. Seconds are optional. For example, specify 1:30 p.m. as 13:30.
- ♦ **Find:** A search string. The first set of lines containing the Find String, written after the time specified, is displayed. All lines containing the find string are marked with an icon so that they can be easily identified as you scroll through the log.

### Obtaining an Explanation for a Message

To view the documentation for a given message, click its Message ID in the log display. An explanation for the message is displayed.

### Navigating through a Log

Navigation links are provided for the following functions:

- ♦ **Beginning of Day:** Scrolls the log display to the beginning of the day specified by Date.
- ♦ **End of Day:** Scrolls the log display to the end of the day specified by Date.
- ♦ **Most Current:** Scrolls the log display to most current set of lines.
- ♦ **Previous:** Scrolls the display to the previous set of lines. Scrolling stops at the beginning of the day specified by Date.
- ♦ **Next:** Scrolls the display to the next set of lines. Scrolling stops at the end of the day specified by Date.
- ♦ **Find Previous:** Scrolls the display to the previous set of lines that include the find string. Scrolling stops at the beginning of the day specified by Date.
- ♦ **Find Next:** Scrolls the display to the next set of lines that include the find string. Scrolling stops at the end of the day specified by Date.

## 3.5.13 Displaying Provisioning Details

You can use the Web interface to search for and display objects in the Census and in the user and group population of a Platform Set.

- 1 Click Fan-Out Driver Utilities > Provisioning Details. The Provisioning Details page is displayed.
- 2 Select the Search Type you want.
- 3 Type the Search String.  
Objects whose name begins with the string you type are matched. If you leave this field blank, all objects are matched.
- 4 Select the maximum number of results to be returned.
- 5 Click Search.  
Objects matching the search string are returned, up to the maximum count that you specified.

- 6 Click the name of an object in the results list to view its attributes. The Object Details page is displayed for that object.

### 3.5.14 Reviewing Naming Exceptions

Naming exceptions are produced when a new User or Group object covered by a Census Search object is found with the same name as an Enterprise User or Enterprise Group object that is already present in the Census.

To review naming exceptions in the Web interface, click Fan-Out Driver Utilities > Review Naming Exceptions.

#### Resolving Naming Exceptions

- 1 In the Web interface, click Fan-Out Driver Utilities > Review Naming Exceptions.
- 2 Use iManager or a similar utility to change the name of the User or Group object that is causing the conflict.
- 3 To remove the record of the naming exception, click the Remove button for the exception in the list on the Review Naming Exceptions page of the Web interface.

Trawl processing automatically removes naming exceptions from the list after you have resolved them.

#### Excluding Recurring Exceptions

If you have recurring exceptions that are normal for you, you can permanently exclude them from the Census and the exception list.

- 1 In the Web interface, click Fan-Out Driver Utilities > Review Naming Exceptions.
- 2 In the desired row, click the button for the action you want to take.
  - ♦ To exclude all users and groups with this common name, click Exclude Name.  
If the user or group already exists in the Census and on platforms, the platforms receive a Delete Pending event and, after the Delete Pending Duration, a Delete event. The object is not provisioned to the platform again.
  - ♦ To exclude this specific user or group, click Exclude DN.

### 3.5.15 Reviewing Platform Errors

The Platform Receiver can return an error indication for its processing of a provisioning event. Such events remain pending for the platform, but are marked in an error state. You can use the Web interface to clear these events or to mark them to be sent to the Platform Receiver again.

- 1 In the Web interface, click Fan-Out Driver Utilities > Review Platform Errors. The Review Platform Errors page is displayed.
- 2 Click the name of the platform whose errors you want to handle. The Errors on Platform page is displayed.
- 3 Select the desired action for the events that are in error.

If additional events for a user or group associated with a platform are created (by a Trawl or by the Event Subsystem), pending events that are in error are cleared for that user or group.

## 3.5.16 Managing Trawls

Object Services examines portions of eDirectory specified by Census Search objects to build and maintain the Census. This process is known as a Trawl. Only the primary core driver performs Trawls. For information about setting the primary core driver, see [“Designating the Primary Core Driver” on page 38](#).

You can use the Web interface to display information about the last Trawl, to start a Trawl, and to stop a Trawl that is in progress.

### Displaying Trawl Information

To display Trawl information, click Fan-Out Driver Utilities > Trawl.

### Starting a Census Trawl

- 1 Click Fan-Out Driver Utilities > Trawl. The Trawl Status page is displayed.
- 2 Click Start.

For information about scheduling Trawls to run automatically, see [“Specifying Trawl Times” on page 32](#).

### Stopping a Census Trawl

You can use the Web interface to stop a Trawl.

- 1 Click Fan-Out Driver Utilities > Trawl. The Trawl Status page is displayed.
- 2 Click Stop.

It can take a few moments for the Trawl to stop.

# Troubleshooting the Core Driver

# 4

Novell® Identity Manager Fan-Out driver components record messages to their Audit Log, Operational Log, and their host system log. Examining these should be foremost in your troubleshooting efforts.

The Audit and Operational logs of core driver components are maintained in their logs directory.

By its very nature, the Identity Manager Fan-Out driver is highly dependent upon the proper operation of your network and eDirectory™. If you are having problems with the driver, ensure that the various driver components are able to communicate with one another, and that eDirectory is functioning properly.

For information pertaining to performance issues, see [Section 1.2, “Configuration and Performance Guidelines,” on page 11](#).

---

**IMPORTANT:** Make sure that you upgrade the Identity Manager Fan-Out driver, including all of your platforms, when new versions or support packs become available.

---

## 4.1 Obtaining Debugging Output

Identity Manager Fan-Out driver components support the option to produce extensive debugging output. Although this output is intended primarily for use by Novell Technical Support, you might find it useful for your own troubleshooting efforts.

Because debugging mode adversely affects performance, it should not be used for routine operations.

### 4.1.1 Debugging the Core Driver

To obtain debugging output for the core driver:

- 1 Specify the destination for debugging information by setting the Debug Log File and Debug to DSTrace configuration parameters as desired.

For more information, see [“Driver Object Configuration Parameters” on page 34](#).

- 2 Specify the debugging information to be produced.
  - 2a In iManager, click Fan-Out Driver Configuration > Configure Logs. The Log Configuration page is displayed.
  - 2b Select the core driver components you want debugging information for.
  - 2c Click Apply.

## 4.2 Troubleshooting Core Driver Configuration Issues

Problems with core driver configuration can result in improper driver operation. The messages logged by Identity Manager Fan-Out driver components can lead you to the source of such problems.

### 4.2.1 Rights Issues

Ensure that rights are properly set to enable the driver to perform its functions.

- ♦ For the rights required by the ASAM Master User object, see [Section 3.2.2, “ASAM Master User Security,” on page 27](#).
- ♦ For the rights required by administrative users, see [Section 3.4.1, “Rights Required for Web Interface Use,” on page 30](#).

### 4.2.2 Platform Services Process / Authentication Services Issues

- ♦ Ensure that your platform has a valid certificate. For more information, see the administration guide for your platform operating system type.
- ♦ For platforms that use the DES interface, ensure that the DES encryption key specified for the platform in the Platform Configuration object and the DES encryption key specified in the platform configuration file are identical.
- ♦ Ensure that the core drivers referred to by your platform configuration file are running and that they are using the network address and TCP port number specified in the platform configuration file.
- ♦ Examine the core driver and Platform Services Process log files.
- ♦ Ensure that your platforms have been upgraded to the current version when you upgrade the core driver.

### 4.2.3 Platform Receiver / Event Journal Services Issues

- ♦ Verify that LDAP is running on the servers that hold replicas of User and Group objects covered by Census Search objects.
- ♦ Verify that the platform certificate has been created on the host running the Platform Receiver.
- ♦ Ensure that the core drivers referred to by your platform configuration file are running and that they are using the network address and TCP port number specified in the platform configuration file.
- ♦ Examine the logs generated by the Platform Receiver and the core driver for error messages.

### 4.2.4 Census Issues

- ♦ Ensure that Census Trawls are being run at appropriate intervals and that they complete without errors.

You can check to see when daily Census Trawls are scheduled through the Web interface. For details, see “[Specifying Trawl Times](#)” on page 32.

You can view the Exceptions to see if any naming exceptions have occurred. For details, see [Section 3.5.14, “Reviewing Naming Exceptions,”](#) on page 51.

You can check the core driver Operational Log to see when the last Census Trawl was completed. Examine the core driver Operational Log for any potential errors that could have prevented the successful creation of Census information.

- ◆ Ensure that your Census Search object parameters are set so that all intended users are included in the Census. For details, see “[Configuring Search Objects](#)” on page 46. You can review the contents of the Census by using the Web interface. For further details, see “[Displaying Provisioning Details](#)” on page 50.
- ◆ Census entries relate to objects in eDirectory using their globally unique identifier (GUID). This prevents accidental reuse of a name from resulting in unintended access to resources. If a user that is represented in the Census is removed from eDirectory, the Census entry is marked inactive. If a new User object with the same name and context is created in eDirectory, the old Census entry remains inactive and a naming exception occurs.

## 4.2.5 LDAP Issues

For problems with LDAP secure communications, see Novell Technical Information Document (TID) 10050254 at the [Novell Support Web Site \(http://support.novell.com/cgi-bin/search/searchtid.cgi?/10050254.htm\)](http://support.novell.com/cgi-bin/search/searchtid.cgi?/10050254.htm).

## 4.3 Troubleshooting Network Issues

The details of network troubleshooting are beyond the scope of this document and depend on a number of factors particular to your environment. This section can help you determine if the various -Identity Manager Fan-Out driver components can communicate with one another.

To verify IP connections between platforms and the core driver, use the ping command.

- ◆ From a command prompt on MVS, OS/400, UNIX, or Windows, enter `ping ipaddr` , where *ipaddr* is the IP address of the remote computer.
- ◆ From a NetWare® console, enter `LOAD TPING ipaddr` , where *ipaddr* is the IP address of the remote computer.

If your installation uses router filters to prevent the use of ping, consult with those responsible for managing your network to learn how to verify connectivity.

You can use other NetWare utilities, such as MONITOR, CONFIG, INETCFG, and TCPCON to examine and change other aspects of server status that pertain to networking. Refer to your NetWare documentation for further details. *Utilities Reference*, *Basic Protocol Configuration Guide*, and *Advanced Protocol Configuration and Management Guide* provide detailed information about using these and other NetWare utilities.

## 4.4 Troubleshooting eDirectory Issues

eDirectory is complex, and the details of troubleshooting are beyond the scope of this document. This section can help you ensure that the directory is healthy before you continue on to investigate other areas when you experience problems with the driver.

Use the TIME command to see if time is synchronized to the network on a given server. From a NetWare console, enter TIME.

Use the DSREPAIR utility to perform a number of checks into the health of eDirectory on a given server.

- 1 From a NetWare console, enter `LOAD DSREPAIR`.
- 2 Select Time Synchronization to check that time is in sync for servers in the server's local database.
- 3 Select Report Synchronization Status to check the server's replica synchronization status. If the Total Errors count at the top of the screen is not zero, the cause should be identified and corrected before you proceed.

Figure 4-1 DSREPAIR Screen



```
NetWare 5.0 DS Repair 5.21                      NetWare Loadable Module
DS.NLM 7.44   Tree name: AS5XMS
Server name: .AS5XMS50A.AS5XMS                      Total errors: 1

View Log File (Last Entry): "SYS:SYSTEM\DSREPAIR.LOG" (2645)

Partition: .[Root].
  Replica: .AS5XMS50A.AS5XMS                      3-09-2000 08:55:37
All servers synchronized up to time:                3-09-2000 08:55:37

Partition: .usr1.AS5XMS
  Replica: .AS5XMS50A.AS5XMS                      3-09-2000 08:52:07
All servers synchronized up to time:                3-09-2000 08:52:07

Partition: .usr2.AS5XMS
  Replica: .AS5XMS51A.AS5XMS                      ***** -622
  Replica: .AS5XMS50A.AS5XMS                      3-09-2000 08:21:50

Partition: .usr3.AS5XMS
  Replica: .AS5XMS50A.AS5XMS                      3-09-2000 08:58:40
All servers synchronized up to time:                3-09-2000 08:58:40

*** END ***

Esc=Exit the editor          F1=Help          Alt+F10=Exit
```

Refer to your NetWare documentation for further details. *Utilities Reference* and *Supervising the Network* provide detailed information on using these and other NetWare utilities. Additional information can be found on the [Novell Support Web site \(http://support.novell.com\)](http://support.novell.com).



# Migrating from Novell Account Management 3.0

# A

This section describes migration to the Novell® Identity Manager Fan-Out driver from Novell Account Management 3.0. For related information, see the What's New topic in the *Concepts and Facilities Guide*.

## A.1 Migration Procedure

- 1** Prepare to upgrade your Account Management 3.0 Manager to become the Identity Manager Fan-Out driver primary core driver.
  - 1a** Record all of the user and group attributes that are sent to platforms by Account Management 3.0. You will need this information to perform [Step 3 on page 57](#).

To use the Account Management 3.0 Web interface to view these attributes, click **Configure > Manager**.
  - 1b** Ensure that replicas of all objects covered by a Census Search object exist on the Manager server. For more information, see [Section 1.3.4, “Core Driver Requirements,” on page 15](#).
  - 1c** Ensure that an Account Management 3.0 Agent on a server other than the Manager server is available, and that all platforms specify it in their platform configuration files.
  - 1d** Stop all Account Management 3.0 processes that are running on the Account Management 3.0 Manager server. This includes the Manager, Event Listener, and Agent.
  - 1e** Stop any other Event Listeners in your Account Management 3.0 configuration, and ensure that they do not start again.

To stop an Event Listener, in iManager, click **DirXML Management > Overview**, locate the ASAMDriver driver object in the ASAMDriverSet driver set, click the driver status indicator in the upper right corner of the driver icon, then click **Stop Driver**.

To set the Event Listener to not start again, click the status indicator > **Edit Properties**, then set the **Driver Configuration Startup Option** to **Disabled**.
- 2** Install the core driver and iManager plug-in for the Identity Manager Fan-Out driver onto the Account Management 3.0 Manager server. For details, see the *Core Driver Quick Start Guide* for the target server operating system type.
  - ♦ *Core Driver Quick Start Guide for Linux and Solaris*
  - ♦ *Core Driver Quick Start Guide for NetWare*
  - ♦ *Core Driver Quick Start Guide for Windows*

The installation program transfers the settings in your Core Services configuration file to the Driver object configuration parameters for the new core driver.

The core driver contains the functionality of both the Account Management 3.0 Manager and the Account Management 3.0 Agent. These functions are consolidated to a single TCP port, which is 3451 by default. Remember to make the appropriate changes to the platform configuration files.
- 3** Add all of the user and group attributes sent to platforms by Account Management 3.0 (recorded in [Step 1a on page 57](#)) to the Identity Manager Fan-Out driver Subscriber filter.

For details about adding attributes to the Subscriber filter, see the *Identity Manager Administration Guide*.

- 4 Run a Trawl. This migrates the user and group objects to the Identity Manager Fan-Out driver format.

- 4a Click Fan-Out Driver Utilities > Trawl. The Trawl Status page is displayed.

- 4b Click Start.

- 5 Upgrade the additional Agents in your Account Management 3.0 configuration to secondary core drivers by performing the core driver installation procedure on their servers. For details, see the *Core Driver Quick Start Guide* for the target server operating system type.

The installation program transfers the settings in your Core Services configuration file to the Driver object configuration parameters for the new core driver.

The core driver contains the functionality of both the Account Management 3.0 Manager and the Account Management 3.0 Agent. These functions are consolidated to a single TCP port, which is 3451 by default. Remember to make the appropriate changes to the platform configuration files.

- 6 Upgrade your platforms to Identity Manager Fan-Out driver Platform Services. For details, see the *Platform Services Quick Start Guide* for the platform operating system type.

- ♦ *Platform Services Quick Start Guide for AIX*
- ♦ *Platform Services Quick Start Guide for FreeBSD, HP-UX, Linux, and Solaris*
- ♦ *Platform Services Quick Start Guide for MVS CA-ACF2*
- ♦ *Platform Services Quick Start Guide for MVS CA-Top Secret*
- ♦ *Platform Services Quick Start Guide for MVS RACF*
- ♦ *Platform Services Quick Start Guide for OS/400*
- ♦ *NetWare Intercept and API Quick Start Guide*

Identity Manager Fan-Out driver Platform Services includes failover support for the Provisioning Manager. You can include more than one PROVISIONING statement in the platform configuration file. For details, see the *Platform Services Planning Guide and Reference*.

## A.2 Object Migration Details

The format of the objects in eDirectory™ that the Identity Manager Fan-Out driver uses for users and groups available to platforms is different from the format used by Account Management 3.0. Each user and group is automatically migrated to the new format the first time it is processed by the core driver. After all users and groups have been migrated to the new format, trawl processing begins to remove the obsolete objects.

Because removing a large number of objects at one time can affect eDirectory performance, only a small number of obsolete objects is deleted by each Trawl. By default, each Trawl deletes no more than 1,000 objects made obsolete by migration. You can use the Web interface to change this limit.

- 1 In iManager, click Fan-Out Driver Configuration > Configure Census. The Census Configuration page is displayed.
- 2 Specify the desired limit under Object Cleanup Limit.

After migration cleanup is complete, you can reduce the size of your eDirectory database by running DSRRepair > Advanced Options > Repair Local DS > Reclaim Database Free Space. For more information, see the *eDirectory Administration Guide*.

To view migration status, in iManager, click Fan-Out Driver Utilities > Component Status > Provisioning Services.



# Password Change Validation Exit

# B

Novell® Identity Manager Fan-Out driver core drivers can call a user-provided routine to enforce local password rules. This routine is called when a password change request is received from a password redirection platform.

The Password Change Validation Exit is passed the fully distinguished name of the user, the old password, the new password, and a message buffer. The exit can accept or reject the password change request and, if the request is rejected, provide an explanation in the message buffer. The explanation is written to the core driver Audit log and is displayed to the user.

A sample Password Change Validation Exit is provided in the ASAM directory created by the installation process in `asam\bin\coredriver\chgpaswdexit\verpass.c`.

To implement the Password Change Validation Exit:

- 1 Design, write, and build your Password Change Validation Exit. You can use the sample Password Change Validation Exit `verpass.c` as a guide.
- 2 Place a copy of the library containing your Password Change Validation Exit on each server that runs a core driver.
- 3 Specify the appropriate Change Password Exit Function and Change Password Exit Library configuration parameters for each core driver. For details, see “[Driver Object Configuration Parameters](#)” on page 34.