

Novell Identity Manager Fan-Out Driver

3.6

www.novell.com

Oct 23, 2008

QUICK START

Installation for Linux* and UNIX* Systems

This *Quick Start* provides basic steps for installing the Identity Manager Fan-Out Driver on Linux and UNIX systems, including AIX*, FreeBSD*, HP-UX, and Solaris*. It condenses information from other documentation that includes more details and additional tasks required to install, configure, and deploy the Fan-Out Driver.

There are two main sections to this *Quick Start*: the Core Driver setup and the Platform Services setup. If you have already installed and configured the Core Driver and are adding an additional Fan-Out Driver platform, follow the steps in "[Installing Platform Services](#)" on page 4.

REQUIRED KNOWLEDGE AND SKILLS

This *Quick Start* assumes you are familiar with concepts, key components and facilities of the Fan-Out Driver, Novell eDirectory™, and the administration of the target operating system.

For complete installation, configuration and administration information, see the *Identity Manager Fan-Out Driver for Linux and UNIX Administration Guide* at the [Identity Manager 3.6 Drivers Documentation Web site](#) (<http://www.novell.com/documentation/idm36drivers>).

Before installing Fan-Out Driver components, obtain the latest support pack and product updates, and review the release notes and readme files. For the latest support information, see the [Novell Support Web site](#) (<http://support.novell.com>).

PREREQUISITES

Verify you are running Identity Manager 3.5.1 or higher, as well as the required versions of eDirectory, iManager, and your target platforms. For more about these requirements, see the associated readme files on [the Identity Manager Documentation Web site](#) (<http://www.novell.com/documentation/idm36drivers>).

The Fan-Out Driver includes two major components:

- ◆ The *Core Driver*, which integrates with the system on which Identity Manager is running.
- ◆ *Platform Services*, which is installed on the target system you wish to connect to Identity Manager.

Novell®

Both the Core Driver and Platform Services use Secure Sockets Layer (SSL) for communications. SSL requires a source of entropy. If your systems do not have a `/dev/random` device to provide entropy, you must install and configure an entropy daemon on both the Identity Manager system and the target connected system prior to installing the Fan-Out Driver.

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.

For your convenience, the Pseudo Random Number Generator Daemon PRNGD is included in the `/prngd` directory of the distribution.

For the LDAP server that you will use with the Core Driver, set the option to dereference aliases when resolving names, as follows:

- 1 In iManager, select *LDAP > LDAP Overview > View LDAP Servers*.
- 2 Click the LDAP Server.
- 3 Under *Nonstandard Behaviors*, select *Dereference Aliases When Resolving Names*, then click *Refresh*.

If the Core Driver you install will be designated as *primary*, ensure that the target server holds replicas of all objects to be covered by a Census Search object.

If the Core Driver you install will be designated as *secondary*, ensure that the primary Core Driver is available, since it provides installation configuration information.

INSTALLING THE CORE DRIVER

Install the Core Driver on a Linux, Solaris or Windows* system running Identity Manager as follows:

- 1 From your installation media, locate and execute the installation software.
 - ◆ For Linux or Solaris, use one of the following self-extracting installers appropriate to your system:

```
sh linux_x86_coredriver.bin
```

```
sh linux_x86_64_coredriver.bin
```

```
sh solaris_sparc_coredriver.bin
```

NOTE: The x86 (32-bit) installer is compatible with both 32-bit and 64-bit versions of Linux. To use the x86_64 (64-bit) installer, you must first install and configure the 64-bit LDAP SDK.

- ◆ For Windows, run the following command:

```
fan-out\IDMCoreDrivers\Win\win_x86_coredriver.exe
```

This x86 (32-bit) executable is compatible with both x86 and x64 versions of Windows.

- 2 Accept the license, select your installation directory and proceed to install the product files by responding to the prompts.
- 3 You may need to change the port setting for the Core Driver's built-in remote loader. This is especially likely if you are also using the standard remote loader that comes with Identity Manager. Both versions of the remote loader use port 8090 as their default setting.

The port setting for the Core Driver's built-in remote loader resides in the `fanout.conf` file, which is located as follows:

- ◆ For Linux and Solaris: `/usr/local/ASAM/data/ASAM/data/`
- ◆ For Windows: `C:\Novell\ASAM\data\`

Edit the following line to reflect the desired port:

```
-connection "ca=/user/local/ASAM/keys/ca.pem port=8090"
```

- 4 Start the Core Driver shim. To start the shim:
 - ◆ In Linux or Solaris, enter `/etc/init.d/asamcdrvd start`
 - ◆ In Windows, start the *Fan-Out Driver Shim* service
- 5 Import and configure the Fan-Out Driver.
 - 5a In iManager, select *Identity Manager Utilities > Import Drivers*. Select a new or existing driver set, then click *Next*.

NOTE: If you are running a version of iManager that does not include the Fan-Out Driver application plug-in, see ["Installing the iManager Plug-In \(if Necessary\)" on page 4](#).
 - 5b Select the Fan-Out Driver from the list of drivers to import, then click *Next*.

NOTE: If the driver is not available in the list, select *Import a configuration from the client* and select the file `\rules\Fan-Out-IDM3_6_0-V1.xml` in the directory where the Driver Shim is installed (`C:\Novell\ASAM` by default).
 - 5c Provide the requested information, then click *Next*.
 - 5d Click *Define Security Equivalences*, add your ASAM Master User object, then click *OK*.
 - 5e Click *Exclude Administrative Roles*, add the Admin user, your ASAM Master User, and any other high-privilege users to the *Excluded Users* list, then click *OK*.
 - 5f Click *Finish*.
- 6 Restart eDirectory to bring the new indexes online.
- 7 Start the Fan-Out Driver.
 - 7a Select *Identity Manager Management > Overview*.

7b Locate the driver in its driver set.

7c Click the status indicator in the upper right corner of the driver icon, then click *Start Driver*.

INSTALLING THE IMANAGER PLUG-IN (IF NECESSARY)

- 1 Login to iManager as an administrative user.
- 2 Click the *Configure* icon at the top.
- 3 Click *Available Novell Plug-in Modules* under *Plug-in Installation* on the left menu.
- 4 Click *Add* above the list of plug-ins.
- 5 Select `fan-out\iManagerPlugIn\FanOutWeb.npm` from your installation media and click *OK*.
- 6 Check the box next to *Novell Identity Manager - Fan-Out Driver Plug-in* and click *Install* above the list of plug-ins.
- 7 Restart the Tomcat or Tomcat5 service on your iManager system, and exit and log back into iManager.
- 8 If the Fan-Out Driver Configuration role has not appeared, continue with the following steps.
- 9 Click the *Configure* icon at the top.
- 10 Click *RBS Configuration* under *Role Based Services* on the left menu.
- 11 Click the number under the *Not-Installed* column in the table.
- 12 Check the box next to *FanOutWeb* and click *Install* above the list.
- 13 Click the *Roles and Tasks* icon at the top.

This procedure adds two new roles to iManager: Fan-Out Driver Configuration and Fan-Out Driver Utilities. The first time you use one of these roles, you are prompted for the DNS name or IP address and the TCP port number of the primary Core Driver. After you provide this information, the Fan-Out Driver is ready for you to continue with your deployment and testing plan.

INSTALLING PLATFORM SERVICES

Install Platform Services on a Linux or UNIX system as follows:

- 1 If you do not have an appropriately configured Platform Set object, use iManager to create a Platform Set object.

Associate users and groups with your Platform Set using the appropriate Search object configuration.

Platform Sets are established for platforms that share a common population of users and groups. Multiple types of platforms can reside in a single Platform Set, and individual users and groups can appear on multiple Platform Sets.

Whenever you modify Search objects, start a Trawl to populate the platforms.

- 2 Use the iManager Fan-Out Driver plug-in to create a Platform object for your platform in an appropriate Platform Set.

You must define all of the IP addresses for the platform so that mutually authenticated SSL can function properly.

- 3 Log in as `root` to the server where you are installing Platform Services.
- 4 From your installation media, locate and execute the appropriate self-extracting installer:

```
sh aix_platformservices.bin
sh freebsd_x86_platformservices.bin
sh hpux_platformservices.bin
sh hpux_ia64_platformservices.bin
sh linux_x86_platformservices.bin
sh linux_x86_64_platformservices.bin
sh debian_x86_platformservices.bin
sh linux_s390x_platformservices.bin
sh solaris_sparc_platformservices.bin
sh solaris_x86_platformservices.bin
sh tru64_platformservices.bin
```

- 5 Accept the license, select your installation directory and proceed to install the product files by responding to the prompts.
- 6 When you are asked to choose a provisioning option to configure this platform:
 - ♦ Select *a* to provision users and groups to `/etc/passwd` and `/etc/group`.
 - ♦ Select *b* to setup the system's Name Service Switch (NSS) for virtual provisioning.
 - ♦ Select *c* to configure this platform for API use only (no provisioning).
- 7 When you are asked to choose an option for user password authentication:
 - ♦ Select *a* to redirect authentication requests to the Metadirectory.
 - ♦ Select *b* to authenticate users locally from `/etc/shadow`.
 - ♦ Select *c* to redirect authentication requests to the Metadirectory but synchronize passwords to provide local failover.
- 8 Review the contents of the platform configuration file `/usr/local/ASAM/data/asamplat.conf`.

If your system does not have a `/dev/random` device, you must include an `ENTROPY` statement to specify a source of entropy.

For an example `asamplat.conf` file, see `/usr/local/ASAM/data/sampleplat.conf`.
- 9 If you are using Authentication Redirection, configure PAM to call Platform Services.

FreeBSD: Edit your `/etc/pam.d/*` files to call the `pam_ascauth.so` module.

HP-UX: Edit your `/etc/pam.conf` file to call the `/usr/lib/security/libpam_ascauth.1` module.

Linux: Edit your `/etc/pam.d/*` files to call the `/lib/security/pam_ascauth.so` module.

Solaris: Edit your `/etc/pam.conf` file to call the `/usr/lib/security/pam_ascauth.so.1` module.

Sample PAM configuration files are included in `ASAM/bin/PlatformServices`.

10 If you are not using the Name Service Switch, set up Receiver scripts.

The Platform Receiver responds to events by running corresponding Receiver scripts. The Platform Receiver runs Receiver scripts from `/usr/local/ASAM/bin/PlatformServices/PlatformReceiver/scripts`. The base set of Receiver scripts is delivered in a subdirectory of `/usr/local/ASAM/bin/PlatformServices/PlatformReceiver/scripts` called `platformName-passwd`. The install script offers to install the base scripts for you. If you accept, then the `plat-config` script copies all of the scripts in `platformName-passwd` up one level to `/usr/local/ASAM/bin/PlatformServices/PlatformReceiver/scripts`.

If you have developed your own set of custom scripts, copy your custom scripts to `/usr/local/ASAM/bin/PlatformServices/PlatformReceiver/scripts`.

For information about developing your own custom scripts, see `/usr/local/ASAM/bin/PlatformServices/PlatformReceiver/scripts/scriptwriters.README`.

Legal Notice

Copyright © 2004, 2007-2008 Omnibond Systems, LLC. All rights reserved. Licensed to Novell, Inc. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher. For Novell trademarks, see the [Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html). All third-party products are the property of their respective owners. A trademark symbol (®), TM, etc.) denotes a Novell trademark; an asterisk (*) denotes a third-party trademark.