Novell
Identity Manager Fan-Out Driver

3.6

www.novell.com

QUICK START

Oct 22, 2008

Installation for Mainframe Systems

This *Quick Start* provides basic steps for installing the Identity Manager Fan-Out Driver on mainframes running the z/OS* operating system to interface with the z/OS-based applications RACF, CA Top Secret and CA ACF2. It condenses information from other documentation that includes more details and additional tasks required to install, configure, and deploy the Fan-Out Driver.

This *Quick Start* includes five main installation tasks:

- "Installing the Core Driver" on page 2
- "Installing Platform Services" on page 5
- "Installing the Platform Services Process" on page 6
- "Installing the Exits" on page 6
- "Installing the Platform Receiver" on page 9

If you have already installed and configured the Core Driver and are adding an additional Fan-Out Driver platform, you can skip the first task, "Installing the Core Driver."

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 Mainframes 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).

Novell®

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 mainframe system you wish to connect to Identity Manager.

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 mainframe 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 FTP the z/OS installation files from the distribution media `mvsplatformservices` directory to the target z/OS system.

You must specify the `BINARY` and `QUOTE SITE LRECL=80 RECFM=FB` ftp commands.

4 Use the TSO `RECEIVE` command to extract the samples libary, load library, and scripts library to places appropriate for your site.

5 APF authorize the load library.

6 Add ASCTEST as an APF-authorized TSO command.

Add ASCTEST to the AUTHCMD section of your PARMLIB(IKJTSO*xx*) member, then use the TSO `PARMLIB` command to activate your changes.

7 Install the Platform Services Process. See “Installing the Platform Services Process” on page 6.

You must run the Platform Services Process on each system that shares the security database. For initial testing, you can install the Platform Services Process to a single system.

8 Install and configure the exits for your particular application (RACF, CA ACF2, or CA Top Secret). See “Installing the Exits” on page 6.

You must install the exits on each system that runs the z/OS Platform Services Process.

9 Install the Platform Receiver. See “Installing the Platform Receiver” on page 9.

You must run only one instance of the Platform Receiver in your complex that shares the security database.

10 Integrate Platform Services into your routine operation.

10a Install Platform Services on all remaining systems that share the security database.

10b Add ASCLIENT and PLATRCVR operation into your routine system startup and shutdown scheduling procedures.

ASCLIENT must be active on every z/OS image in your complex. PLATRCVR must be active on only one system in the complex that shares the security database.

10c Change the Include/Exclude lists to match your production environment.

INSTALLING THE PLATFORM SERVICES PROCESS

1. Copy the ASCLIENT member from the samples library to your started task procedure library, and customize it to use your own data set names.
2. Ensure that the ASCLIENT user ID is defined as a UNIX* user.
3. Set up your ASCLIENT configuration member.

   The ASCLIENT configuration member must belong to an LRECL=80 RECFM=FB PDS allocated to the ASCPARMS DD statement of the ASCLIENT JCL.

   You can use member ASCPRMXX of the samples library as a model. For details about the configuration statements, see the *Identity Manager Fan-Out Driver for Mainframes Administration Guide*.
4. Assign a DES key for the platform.

   Use the KEY statement of the configuration member to set the key for ASCLIENT.

   Use the Web interface to set the identical key in the Platform object for the platform.
5. Assign ASCLIENT to a Service Class, such as SYSSTC, appropriate for its role in logon processing.
6. Start ASCLIENT.
7. Use ASCTEST to perform preliminary testing. For details, see the *Identity Manager Fan-Out Driver for Mainframes Administration Guide*.
8. Establish Include/Exclude lists for initial testing of Authentication Services.

INSTALLING THE EXITS

The steps you should take for installing exits will depend on the target mainframe application (RACF, CA Top Secret, CA ACF2) that will interface with Identity Manager. Therefore, choose from the following tasks accordingly:

- “Installing the RACF Exits” on page 7
- “Installing the Top Secret Exit” on page 7
- “Installing the ACF2 Exits” on page 8

Installing the RACF Exits

1 Install ICHRIX01, the RACINIT pre-process exit.

- If you do not have an existing ICHRIX01 exit, customize and run the job in the RACRIX0A member of the samples library.
- If you already have an ICHRIX01 exit, customize and run the job in the RACRIX0B member of the samples library. RACRIX0B installs a router that calls the Platform Services RACINIT exit and your existing exit.

2 Install ICHPWX01, the RACF new password exit.

- If you do not have an existing ICHPWX01 exit, customize and run the job in the RACPWX0A member of the samples library.
- If you already have an ICHPWX01 exit, customize and run the job in the RACPWX0B member of the samples library. RACPWX0B installs a router that calls the Platform Services new password exit and your existing exit.

3 IPL with the CLPA option.

4 Update RACF options.

To avoid user confusion while phasing in your conversion to the driver, ensure that your RACF and eDirectory password rules are the same.

After your migration is complete, turn off the RACF password rules. Enter:

```
setropts password( nohistory interval(254) norevoke norules )
```

Installing the Top Secret Exit

1 Review the section pertaining to the use of the CA-Top Secret Installation Exit TSSINSTX in the *CA Top Secret User Guide*.

2 Modify TSSINSTX to use the driver PREINIT function.

2a If you already use the PREINIT function, review the considerations for sites with a pre-existing PREINIT function in the Identity Manager Fan-Out Driver for Mainframes Administration Guide.

2b Change the ##MATRIX byte for PREINIT to a value of #####YES.

2c Insert the following instructions immediately after the PREINIT label:

```
LR     R1,R9             <AM> | Copy parmlist ptr to R1
LR     R11,R13           <AM> | Save TSS’s savearea ptr
LA     R13,WORKAREA      <AM> | Use WORKAREA as savearea
L      R15,=V(ASCTSSPI)  <AM> | Get addr of AM preinit exit
BALR   R14,R15           <AM> | Call it
LR     R13,R11           <AM> | Restore TSS’s savearea ptr
B      EXIT              <AM> | Exit with exit’s returncode
```

3 Place the modified TSSINSTX exit module in your TSS product library.

  3a Customize and run the job in the ASMINSTX member of the samples library.

  3b If your TSS product library is in the linklist, refresh LLA with the following operator command:

```
F LLA,REFRESH
```

4 Activate the modified TSSINSTX exit.

  4a If TSSINSTX is already in use, issue the following operator commands:

```
F TSS,EXIT(OFF)
```

  4b Issue the following operator command:

```
F TSS,EXIT(ON)
```

Installing the ACF2 Exits

1 Install SEVPRE, the system entry validation exit.

- If you do not have an existing SEVPRE exit, customize and run the job in the ACFSVP0A member of the samples library.
- If you already have an SEVPRE exit, customize and run the job in the ACFSVP0B member of the samples library. ACFSVP0B installs a router that calls the Platform Services system entry validation exit and your existing exit.

2 Install NEWPXIT, the new password exit.

- If you do not have an existing NEWPXIT exit, customize and run the job in the ACFNPX0A member of the samples library.
- If you already have an NEWPXIT exit, customize and run the job in the ACFNPX0B member of the samples library. ACFNPX0B installs a router that calls the Platform Services new password exit and your existing exit.

3 IPL with the CLPA option.

4 Set ACF2 options to call the exits. Specify a value of ASCSVPRE for exit SEVPRE, and a value of ASCNPXIT for exit NEWPXIT.

5 Remove the ACF2 password rules.

Set the following values:

MAXTRY(255)	MINPSWD(1)	PASSLMT(255)
PSWDALT	NOPWDHIST	PSWDNUM
WRNDAYS(0)		

6 Install the new values with the following operator command:

```
MODIFY ACF2,REFRESH
```

Installing the Platform Receiver

1 Customize and run job PAXRST0A from the samples library.

This job creates and populates the `ASAM` directory in HFS.

2 Copy the PLATRCVR member from the samples library to your started task procedure library, and customize it to use your own data set names.

3 Ensure that the PLATRCVR user ID is defined as a UNIX user.

4 Assign PLATRCVR the appropriate security system authority to manage users and groups.

5 Set up the platform configuration file for PLATRCVR.

Configuration statements must be placed in a sequential file allocated to ddname ASAMCONF in the PLATRCVR JCL.

You can use member ASAMCONF of the samples library as a model. For details about configuration statements, see the *Identity Manager Fan-Out Driver for Mainframes Administration Guide*.

6 Obtain a security certificate for the platform by customizing and running the SETCERT member of the script library, and responding to the prompts.

7 Establish Include/Exclude lists for initial testing of Identity Provisioning.

8 Customize and extend the Receiver scripts as appropriate for your management plan.

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). 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.