Novell Nsure™ Identity Manager Driver for Linux* and UNIX*

2.0.1

www.novell.com

IMPLEMENTATION GUIDE

September 29, 2004

Novell®

Legal Notices

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.

www.novell.com

Novell Nsure Identity Manager Driver for Linux and UNIX 2.0.1 Implementation Guide
September 29, 2004

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

DirXML is a registered trademark of Novell, Inc. in the United States and other countries.
eDirectory is a trademark of Novell, Inc.
Novell is a registered trademark of Novell, Inc., in the United States and other countries.
Novell eDirectory Services and NDS are registered trademarks of Novell, Inc. in the United States and other countries.

Third-Party Trademarks

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

Contents

About This Guide

The Identity Manager driver for Linux and UNIX is a solution to synchronize network-wide user and group information between eDirectory™ and traditional UNIX data stores such as Files, NIS, and NIS+. This configurable solution gives organizations the power to streamline business processes through the seamless synchronization of user and group accounts in UNIX and eDirectory.

This document is for Novell® eDirectory administrators, DirXML® administrators, and UNIX administrators who are using the Nsure Identity Manager driver for Linux and UNIX.

This guide contains the following sections:

Additional Documentation

For documentation on using DirXML and the other DirXML drivers, see the DirXML Documentation Web site (http://www.novell.com/documentation/beta/dirxml20/index.html).

Documentation Updates

For the most recent version of this document, see the Nsure Identity Manager Driver for Linux and UNIX Web site (http://www.novell.com/documentation/lg/dirxmldrivers/index.html).

Documentation Conventions

In this document, the term *NIS* is used to refer to Files, NIS(YP), and NIS+. Also, the term *driver* refers to all components of Nsure Identity Manager driver for Linux and UNIX and not to any one particular component.

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in 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.

1 Introduction to the Nsure Identity Manager Driver for Linux and UNIX

The DirXML® driver for Linux and UNIX 2.0 is a solution to synchronize user data between Novell® eDirectory™ and later, and UNIX data stores that contain information in Files, NIS(YP), and NIS+. It uses Identity Manager to communicate with eDirectory.

In mixed networks, eDirectory communicates with a variety of data stores spread across complex and heterogeneous computer systems in order to maintain network-wide information. On UNIX systems, such information is maintained in three different types of data stores: Files, NIS(YP), and NIS+.

IMPORTANT: In this document, the term NIS is used to refer to Files, NIS, and NIS+.

Overview

This section discusses the following:

New Features

The following section contains information about the new driver features, as well as new features provided in Identity Manager 2.0.

Driver Features

- Bi-directional Password Synchronization
- Driver Heartbeat
- Account Entitlements
- Support for HP-UX*
- Support for MD5 passwords

Bug Fixes

- Fix for TID-2964698
- Fix for TID-2964711

Identity Manager 2.0 Features

Identity Manager 2.0 includes the following new features. For complete details, refer to the *Identity Manager Administration Guide* (http://www.novell.com/documentation/beta/dirxml20/admin/data/alxnk27.html).

Password Management

The new password management framework includes the following benefits:

- New Password Policies let you create rules for passwords and assign them to users, containers, or the whole eDirectory tree. You can enable Universal Password, which lets you enforce detailed criteria for passwords and allows for special characters.
- Password Synchronization 2.0 is now cross-platform, and it lets you enforce your Password Policies across connected systems. New notification templates let you automatically send messages to users about their password synchronization status.

  The Nsure Identity Manager driver for Linux and UNIX supports bidirectional password synchronization. The driver can accept passwords from NIS and can distribute passwords from NIS to eDirectory.
- Using Password Policies, you can also provide Forgotten Password Self-Service and Reset Password Self-Service to your users. These new features can help you reduce help desk calls. Notification templates are also included for automatically sending forgotten password and password hint messages to users.

Policy Builder Interface and DirXML Script for Creating Policies

For the most common tasks, you can now use the new Policy Builder interface to create policies easily for your driver without having to write XSLT code. The Policy Builder helps you set up the most common rules using the new DirXML Script.

Novell Nsure Audit

Novell Nsure Audit is a centralized, cross-platform auditing service. It collects event data from multiple applications across multiple platforms and writes the data to a single, non-repudiable data store. Nsure Audit is also capable of creating filtered data stores. Based on criteria you define, Nsure Audit captures specific types of events and writes those events to secondary data stores.

Global Configuration Values

Global configuration values (GCVs) are new settings that are similar to driver parameters. Global configuration values can be specified for a driver set as well as an individual driver. If a driver does not have a value for a particular GCV, the driver inherits the value for that GCV from the driver set.

GCVs allow you to specify settings for new Apollo features such as password synchronization, as well as settings that are specific to the function of an individual driver configuration. Some GCVs are provided with the drivers, but you can also add your own. You can refer to these values in a policy to help you customize your driver configuration.

Files, NIS, and NIS+

The three main data stores that maintain user and group account information in UNIX systems are briefly described below.

- “Files” on page 11

- “Network Information Service (NIS(YP))” on page 11
- “Network Information Service Plus (NIS+)” on page 11

Files

The Files data store uses local files on a machine to store information. These files are modified by different utilities to add, modify, and delete information. Information related to user accounts and groups is stored in the /etc/passwd and /etc/group files respectively, in ASCII format.

Network Information Service (NIS(YP))

Local files are inadequate to store information pertaining to a large number of clients in client/server networks. NIS(YP), a data storage mechanism designed to meet this need, uses a central NIS(YP) server to store domain-level information that client machines can access. NIS(YP) maintains user account and group account information in data stores called *maps*. Information is stored in DBM format in maps files.

Network Information Service Plus (NIS+)

NIS(YP) was designed for use in client/server networks that had a few hundred clients and a few multi-purpose servers. It proved to be inadequate in larger networks that hosted many specialized servers. NIS+ was designed to replace NIS(YP).

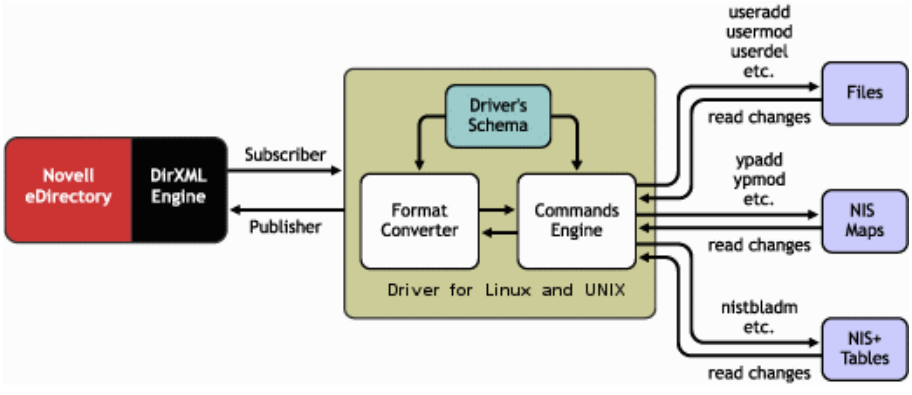
NIS+ stores network-wide information in a distributed, hierarchical domain structure and provides additional security to service clients across untrusted public networks. Information related to user accounts and groups is stored in the passwd and group tables in a relational database format. NIS+ uses a transaction log to send updates, which can be viewed using the *nislog* command.

Driver Architecture

The Nsure Identity Manager driver for Linux and UNIX synchronizes information between NIS data stores and eDirectory so there is a one-to-one correspondence between user or group account information as stored in eDirectory and in NIS.

The following illustration describes the architecture of the Nsure Identity Manager driver for Linux and UNIX.

Figure 1 Nsure Identity Manager Driver for Linux and UNIX Architecture



The Nsure Identity Manager driver for Linux and UNIX communicates with two main modules, the DirXML engine and the external NIS database. The driver is represented through objects in eDirectory. The eDirectory object that represents the driver stores the driver's configuration and rule values.

The Nsure Identity Manager driver for Linux and UNIX 2.0 can operate with three UNIX authentication data stores—Files, NIS, and NIS+. A PAM module is provided to support password synchronization by capturing passwords and sending them to the driver.

You can access and configure the driver using the DirXML snap-in in iManager.

Driver Components

The Nsure Identity Manager driver for Linux and UNIX provides:

- "Subscriber Channel" on page 12
- "Publisher Channel" on page 13

The driver interfaces with the NIS databases on both the Subscriber and Publisher channels.

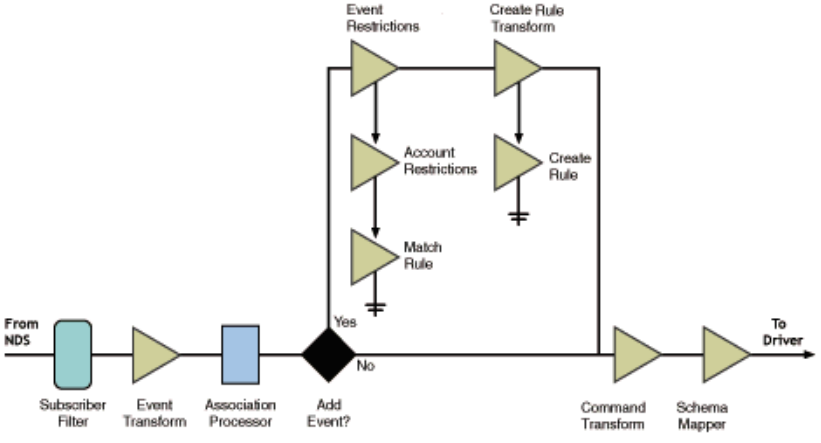
- On the Subscriber channel, the driver updates the NIS databases (/etc/passwd, /etc/shadow and the /etc/group files or the NIS(YP) or the NIS+ tables).
- On the Publisher channel, the changes in the NIS databases are periodically gathered and send to the driver.

Subscriber Channel

The Subscriber channel receives eDirectory events related to addition, modification, deletion, and renaming of user and group objects and updates the NIS databases to reflect the changes.

If the driver is configured to support Universal password, any set/reset of Universal password is synchronized to Files/NIS/NIS+.

Figure 2 Subscriber Channel



A few password policies are created on the Subscriber channel for the Universal password feature. A new policy is created for Role-Based Entitlements also.

The following table lists the Subscriber events that are supported by the driver, and the action taken upon receiving the event:

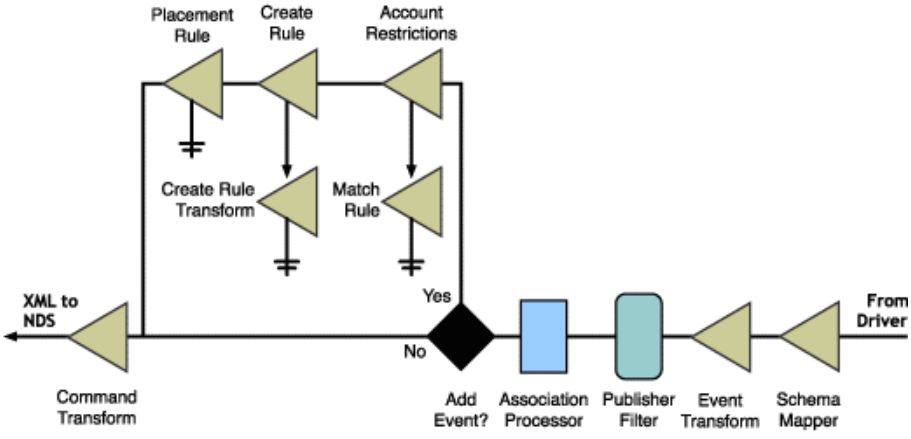
Subscriber Event	Action
A user or group with a UNIX profile is added in eDirectory	The user or group is created in NIS
A user or group without a UNIX profile with the driver ID generation option being set to yes is added to eDirectory	The user or group is created in NIS
A user's or group's UNIX profile is modified in eDirectory	The user or group is modified in NIS
A user or group is deleted in eDirectory	The user or group is deleted in NIS
A user or group is renamed in eDirectory	The user or group is renamed in NIS. (This will result in a delete and add operation and hence the password of the user will be lost)

NOTE: Rename operation in eDirectory is not supported if multiple drivers are configured.

Publisher Channel

The Publisher channel polls the NIS databases for changes in user and group information and updates the eDirectory.

Figure 3 Publisher Channel



A few password policies are created on the Publisher channel for Universal password feature.

The following table lists the Publisher events that are supported by the driver, and the action taken upon receiving the event:

Publisher Event	Action
A user or group is created in NIS	A user or group with a UNIX profile is created in eDirectory or a user or group is updated in eDirectory if it is already present

Publisher Event	Action
A user or group is modified in NIS	The UNIX profile of user or group is modified in eDirectory
A user or group is deleted in NIS	The user or group is deleted in eDirectory

IMPORTANT: Renaming a user or group is not supported in Files and NIS(YP).

The Driver and Its Configuration in eDirectory

The behavior of the DirXML driver is governed by its configuration. The configuration of the driver is stored in the NIS driver object in eDirectory. The various configuration parameters, rules, and transformations are stored as objects and attributes for this driver object. This section describes the various configuration objects and attributes that form the driver configuration.

- "Filter" on page 14
- "Schema Mapping Policies" on page 15
- "Policies" on page 15
- "DirXML Policies" on page 17

Filter

The filter attribute is used to restrict the data that is sent to eDirectory from NIS or from NIS to eDirectory to the Nsure Identity Manager driver for Linux and UNIX. For example, if your driver is configured to synchronize only user account information on the Subscriber channel, the filter can restrict eDirectory to send the driver only when changes are made to User objects.

Using filters, you can also set the datastore (eDirectory or NIS) that would be the merge-authority in case of a conflict.

The following table lists the class and attributes for filter on the Subscriber channel:

Class	Attributes
User	CN, uidNumber, gidNumber, authPassword, homeDirectory, loginShell, gecos, shadowMax, shadowMin, shadowWarning, shadowLastChange, shadowInactive, shadowExpire, shadowFlag, nspmDistributionPassword, DirXML-SPEntitlements
Group	CN, gidNumber, Member

The following table lists the class and attributes for filter on the Publisher channel:

Class	Attributes
User	CN, uidNumber, gidNumber, gecos, authPassword, GroupMembership, homeDirectory, loginShell, shadowMax, shadowMin, shadowWarning, shadowLastChange, shadowInactive, shadowExpire, shadowFlag,
Group	CN, gidNumber, Member

Schema Mapping Policies

The schema mapping policies specifies how eDirectory objects and attributes correspond to NIS entries.

The Nsure Identity Manager driver for Linux and UNIX has been developed according to the RFC-2307 convention. The attributes from RFC-2307 except those listed below are directly mapped. The following are the mappings for the eDirectory objects and attributes:

eDirectory Name for Object/Attribute	Application Name for Object/Attribute
User	User
Group	Group
CN (User)	loginName (User)
CN (Group)	groupName (Group)
GroupMembership (User)	gidNumber (User)
Member (Group)	memberUid (Group)

Policies

This sections explains about the policies used by the Nsure Identity Manager driver for Linux and UNIX:

- “Matching Policies” on page 15
- “Placement Policies” on page 16
- “Creation Policies” on page 16

Matching Policies

The Matching Policies imposes a restriction on the correspondence between eDirectory objects and NIS entries before DirXML can create an association.

In the case of the Nsure Identity Manager driver for Linux and UNIX, matching is based on the CN attribute for both users and groups.

The following table lists the user and group attributes for the Matching Policies on the Subscriber channel:

User Attribute	Group Attribute
CN	CN

The following table lists the user and group attributes for the Matching Policies on the Publisher channel:

User Attributes	Group Attributes
CN	CN

The User and Group containers are prompted, in which Users or Groups are to be matched in the Matching Policies on the Publisher channel during configuration.

Placement Policies

This policy specifies the location of the container where the objects synchronized from NIS are to be placed in eDirectory.

The DN of the User and Group containers in which Users or Groups are to be placed are prompted, in which Users or Groups are to be placed in the Placement Policies on the Publisher channel during configuration.

NOTE: There is no Placement Policy for the Subscriber channel.

Creation Policies

The Creation Policies specifies the mandatory information that the driver must have before a new entry can be created in NIS. For example, you could specify that the first name and login name must be supplied in order to create a corresponding record.

The driver requires the following mandatory attributes for creating user and group in NIS on the Subscriber channel:

User Attributes	Group Attributes
CN	CN
uidNumber	gidNumber
gidNumber	
homeDirectory	

The uidNumber of User and gidNumber of Group are not mandatory attributes if ID Generation is configured. For more information, refer “ID Generation” on page 58.

The following table lists the mandatory attributes for creating user and group in eDirectory on the Publisher channel:

User Attributes	Group Attributes
CN	CN

User Attributes	Group Attributes
uidNumber	gidNumber
GroupMembership	
homeDirectory	

DirXML Policies

The driver uses the following DirXML policies:

- "Create Rule Transform" on page 17
- "Command Transform" on page 18
- "Account Restrictions" on page 18
- "Event Restrictions" on page 20

Create Rule Transform

The Create Rule Transform policy for the Publisher channel is used to specify the default values for Surname and uniqueID attributes for Add events of users. The value that is used is the value of the CN attribute. This is required because SurName and uniqueID are mandatory attributes for creating user and UNIX profile in eDirectory.

The Create Rule Transform policy for the Subscriber channel is used to specify the default values for gidNumber, homeDirectory, default password, and loginShell.

The default password allows you to set up passwords for initial User account creation on UNIX machines. The Create Rule Transform policy must be configured for the driver that creates a default password for Users. The clear-text password must be provided in the policy in the <password> tag. The driver will then set this as the initial driver password for the User.

To edit the Create Rule Transform policy from Subscriber channel:

1. In iManager, click DirXML Management > Overview.
2. Locate the driver in its driver set.
3. Click the driver to open the Driver Overview Page.
4. Click the Creation Policies on the Subscriber channel.
5. Click the Create Rule Transform policy and replace */home* with the desired home directory prefix for user in the last line of the following section of the policy:

   ```
   <do-add-dest-attr-value name="homeDirectory">
     <arg-value>
     <token-text>/home</token-text>
   ```

   This prefix is used as a prefix to build the home directory path with the user's name concatenated to it.
6. Replace */bin/sh* with the desired login shell for user in the following:

   ```
   <do-add-dest-attr-value name="loginShell">
     <arg-value>
   ```

```
<token-text>/bin/sh</token-text>
```

NOTE: Ensure that the shell exists on the application platform

7 Replace 500 with the desired primary group ID for the user in the following:

```
<do-add-dest-attr-value name="gidNumber">
  <arg-value>
    <token-text>500</token-text>
```

8 Replace *./add-attr[@attr-name='CN']/value* with the desired default password in the following line:

```
<do-set-dest-password>
  <arg-string>
   <token-xpath expression="string(./add-attr[@attr-name='CN']/value)" />
```

NOTE: If multiple drivers are running, only one driver should have a default password enabled for users, and only one driver should have ID generation enabled for a particular user or group.

Command Transform

The Command Transform policy is available both on the Subscriber and Publisher channels.

On the Subscriber channel, the Command Transform policy does the following:

- Suppresses any add or modify events for member attributes of groups that do not correspond to secondary memberships.
- Converts the add or modify event value of gidNumber for users to the corresponding group DN.

On the Publisher channel, the Command Transform policy does the following:

- Allows only posixAccount and shadowAccount classes for users.
- Allows only posixGroup for groups.
- Allows updating the secondary members of a group. The previous secondary members are deleted and new secondary members are added upon a modify event for a group's member attribute.
- Allows updating of group membership for users. The previous primary group is deleted and new group is added upon an add or modify event for a groupmembership attribute.
- Allows adding an add or modify attribute node for gidNumber based on an add or modify attribute node for GroupMembership.

IMPORTANT: Do not edit the contents of this policy.

Account Restrictions

The Account Restrictions policy restricts the hashed, as well as the privileged user and group accounts from being synchronized to or from eDirectory. This restriction is based on the user's uidNumber and the group's gidNumber being greater than a specified value.

In order to prevent the hashed users' (commented out users) Ex: #loginName from being synchronized to eDirectory, edit the Account Restrictions policy on the Publisher channel.

To edit the Create Rule Transform policy from Publisher channel:

1. In iManager, click DirXML Management > Overview.
2. Locate the driver in its driver set.
3. Click the driver to open the Driver Overview Page.
4. Click the Creation Policies on the Publisher channel.
5. Click the Create Rule Transform policy and replace the following line:

   ```
   <!--if-xpath op="true">not(starts-with(normalize-space(add-attr[@attr-name='CN']/value),'#'))</if-xpath-->
   ```

   with

   ```
   <if-xpath op="true">not(starts-with(normalize-space(add-attr[@attr-name='CN']/value),'#'))</if-xpath>
   ```

On the Subscriber channel, this policy specifies a minimum value of 100 for the uidNumber for the user and gidNumber for group attributes because on UNIX systems all smaller values of uidNumber and gidNumber are reserved. This restricts the events going from eDirectory to NIS.

To edit this value, you can change it in the Account Restrictions policy:

1. In iManager, click DirXML Management > Overview.
2. Locate the driver in its driver set.
3. Click the driver to open the Driver Overview Page.
4. Click the Matching Policy on the Subscriber channel.
5. Click the Account Restrictions policy and replace the value 100 with the required value of uidNumber in the following line:

   ```
   <if-xpath op="true">add-attr[@attr-name='uidNumber']/value[number(.) <= 100]</if-xpath>
   ```

6. Replace the value 100 with the required value of gidNumber in the following line:

   ```
   <if-xpath op="true">add-attr[@attr-name='gidNumber']/value[number(.) <= 100]</if-xpath>
   ```

NOTE: If ID Generation is configured, the Account Restrictions policy is not attached in the Subscriber channel. For more information, refer to “ID Generation” on page 58.

On the Publisher channel, the Account Restrictions policy for the user specifies a minimum value of 100 for the uidNumber for the user and gidNumber for the group because on UNIX systems all smaller values of uidNumber and gidNumber are reserved. This restricts the events going from NIS to eDirectory.

To edit this value, you can also change it in the Account Restrictions policy:

1. In iManager, click DirXML Management > Overview.
2. Locate the driver in its driver set.
3. Click the driver to open the Driver Overview Page.
4. Click the Matching Policy on the Publisher channel.
5. Click the Account Restrictions policy and replace the value 100 with the required value of uidNumber in the following line:

   ```
   <if-xpath op="true">add-attr[@attr-name='uidNumber']/value[number(.) <= 100]</if-xpath>
   ```

6 Replace the value 100 with the required value of gidNumber in the following line:

```
<if-xpath op="true">add-attr[@attr-name='gidNumber']/value[number(.) <=
100]</if-xpath>
```

Event Restrictions

The Event Restrictions policy specifies the container in eDirectory from where the users or groups are synchronized to the NIS database. This policy enables you to allow add events for users and groups only from the specified containers in eDirectory.

On the Subscriber channel, replace the *\TREE-NAME\ORG_O\USERS_OU* variable for the user with the user container and *\TREE-NAME\ORG_O\GROUPS_OU* variable for group with the FDN of the group container.

To edit this value, you can also change it in the Event Restrictions policy:

1 In iManager, click DirXML Management > Overview.

2 Locate the driver in its driver set.

3 Click the driver to open the Driver Overview Page.

4 Click the Matching Rule on the Subscriber channel.

5 Click the Event Restrictions policy and replace the variable *\TREE-NAME\ORG_O\USERS_OU* with the required fully distinguished name of the container in slash format whose users are to be synchronized in the following line:

```
<if-src-dn op="not-in-container">\TREE-NAME\ORG_O\USERS_OU</if-src-dn>
```

6 Replace the variable *\TREE-NAME\ORG_O\GROUPS_OU* with the required fully distinguished name of the container in slash format whose groups are to be synchronized in the following line:

```
<if-src-dn op="not-in-container">\TREE-NAME\ORG_O\GROUPS_OU</if-src-dn>
```

Ensure that the FDN of containers for users and groups is the same as the DN of containers for users and groups in Placement and Matching policies.

NOTE: There is no Event Restrictions policy for the Publisher channel.

2 Installing the Nsure Identity Manager Driver for Linux and UNIX

This section helps you meet the prerequisites for the driver and install the driver components.

Before You Start

Before you install and configure the DirXML® driver for Linux and UNIX, keep in mind the following constraints:

- The driver can be run only on the application platform; that is, the machine where the Files, NIS, or NIS+ databases exist. If Novell® eDirectory™ and the DirXML Engine 2.0 are not installed on the application platform, you must use the Remote Loader to run the driver. For more information, refer to "Configuring the Remote Loader" on page 43.

  NOTE: Nsure Identity Manager driver for Linux and UNIX needs to be installed on the Remote Loader platform.

- The driver application shim utility tries to locate the dependent utilities at the paths /usr/bin/, /bin/, /usr/sbin/, /usr/local/bin/, and /usr/lib/yp/.
  - Ensure that the awk, make, and makedbm utilities are available at any one of the paths mentioned above.
  - On Solaris, nawk utility must be available in any one of the paths mentioned above.
  - On HP-UX, nawk utility must be available, if not, create a soft link to gawk" as "nawk" at any of the paths mentioned above.
- NIS or NIS+ should be configured before running drivers on the application platform.
- If the application platform hosts either NIS or NIS+, you must run the driver on the NIS(YP) and NIS+ master servers only.
- The makedbm utility should be available on the application platform.

This is required for the Files and NIS(YP) drivers only. This utility is available when you install the ypserv package.

- For remote installation of NIS 2.0 PAM module, SSH must be set up between the source machine and the target machine.

Supported Platforms

- Solaris Sparc* 2.7 or 2.8
- Linux Red Hat* AS 2.1 or SuSE Linux 8.1
- IBM* AIX* 5.2
- HP-UX 11i

System Requirements

- ❑ Novell eDirectory 8.7.3
- ❑ Novell Identity Manager 2.0
- ❑ iManager 2.0.1 or later
- ❑ eDirectory Administration Utilities (for extending the schema). For more information, refer to the *Novell eDirectory Administration Guide* (http://www.novell.com/documentation/lg/edir873/index.html)

Installation

To install the Nsure Identity Manager driver for Linux and UNIX:

1. Log in with the Root account on the machine where you want to install the Nsure Identity Manager driver for Linux and UNIX.
2. Execute the nis-drv-install script from the setup directory of the application platform.
3. Specify the choice of the desired language to read the License Agreement in.
4. Press Enter to read the License Agreement.
5. Enter **y** to accept the License Agreement.

   The DXMLnis package, now installed on your system contains the following items:

- NDS2NIS.jar: Driver Jar file in the /usr/lib/dirxml/classes directory
- dxnis: Binary executable command in the /usr/sbin directory
- NIS.xml and NIS_en.xlf: preconfigured XML files for Files, NIS, and NIS+ in the /usr/lib/dirxml/rules/nds2nis directory
- pam_dxml: Shared library in the /usr/lib/dirxml/rules/nds2nis directory that is used by the driver to capture the password.

Post-Installation

Extending the Schema

Before executing the nis-drv-config script, ensure that the Require TLS for Simple Binds with Password option is disabled in eDirectory. For more information, refer to the *Novell eDirectory Administration Guide* (http://www.novell.com/documentation/lg/edir873/index.html).

To run the script, execute the following command:

```
nis-drv-config [-h hostname] [-D adminContext] [-w adminPassword]
```

The nis-drv-config script extends the eDirectory schema for the Nsure Identity Manager driver for Linux and UNIX. The eDirectory schema needs to be extended only once for a particular eDirectory tree.

On a Linux machine that uses native LDAP tools, extend the schema using the following:

```
nis-drv-config [-h hostname] [-D adminContext] [-w adminPassword] <-x>
```

If the hostname or adminContext are not provided as command line parameters, you are prompted to input them. The adminContext should be given in LDAP format cn=admin, o=context.

NOTE: If you want to manually extend the schema that is used by the NIS driver using the ndssch utility, the schema is contained in the nis.sch file in the /usr/lib/nds-schema directory where the driver is installed.

Configuring the PAM Module

A PAM module is provided to capture passwords and send them to the driver.

For the Files datastore, the driver is installed on the machine where the files are, and the PAM module must be installed on the same machine.

For NIS and NIS+, the driver needs to be installed on only one UNIX machine, and the PAM module (the password filter) needs to be installed where the driver is installed as well as on all machines where passwords can possibly be changed. A utility is provided which installs the PAM

module on a remote machine, which requires SSH to be configured so that the remote machine trusts the machine that the utility is run from.

To configure the PAM module:

1. Execute the following command:

   ```
   nis-drv-config -pam
   ```

2. You are now prompted to select the appropriate PAM module configuration option:

   - **1:** if you want to configure PAM on a local machine.

     This will copy the PAM module to the local machine.

   - **2:** if you want to configure PAM on a remote machine (requires SSH).

     To configure PAM on a remote machine, you must have already configured SSH. For more information on configuring SSH on a remote machine, refer to "Completing the SSH Configuration So the PAM Module Can Be Installed on a Remote Machine" on page 25.

   - **3:** if you want to remove the PAM configuration from a local machine.

   - **4:** if you want to remove the PAM configuration from a remote machine (requires SSH).

3. (Conditional) If you selected 2 or 4 in Step 2, specify the IP address or the name of the remote machine where PAM is to be configured.

4. Specify the name and the type of the UNIX datastore that the driver is synchronizing with, whether Files, NIS or NIS+.

   The default is NIS.

5. Specify the hostname of the machine where the driver is running.

6. If you selected NIS in Step 4, specify the directory where the NIS map files are located.

   The default is /var/yp/*domain name*.

7. Specify yes if the machine uses shadow passwords.

8. Type **y** to confirm the inputs provided for the PAM configuration

   The necessary PAM configuration is now completed.

For more information about the PAM configuration files, refer to "PAM Configuration" on page 60.

Completing the SSH Configuration So Passwords Can Be Sent to the Driver

IMPORTANT: This configuration is not required if the PAM module is configured on the machine where the driver is running.

For the PAM module on the remote machine to transfer the password to the Driver, the machine where the Driver is running must trust the remote machine. To enable that, SSH configuration must be set up between the two machines.

1. Make sure you meet the prerequisites for setting up SSH:

   - You must have root privileges on both machines
   - ssh server must be running on the machine the Driver is running on
   - ssh client must be available on the remote machine

2. Generate a public/private key pair on the remote machine.

2a Generate a key pair using the following command:

```
ssh-keygen -t dsa
```

2b Accept the default name (for example, .ssh/id_dsa) or specify a different name for the key pair generated.

2c When prompted for a passphrase, press Enter without typing a passphrase.

It is necessary to have an empty passphrase; the utility will not work otherwise.

2d Press Enter when prompted again to verify the passphrase.

3 Copy the public key (.pub extension) to the machine where the Driver is running.

For example:

```
scp root-user-home-dir/.ssh/id_dsa.pub target-machine:/
id_dsa.pub
```

4 On the machine where the Driver is running, add the contents of this public key to the list of trusted keys.

The list of trusted keys is the authorized_keys file in the .ssh directory in the root user's home directory. If the id_dsa.pub key has been copied to the machine, this command can be executed on the machine where the Driver is running:

```
cat /id_dsa.pub >> root-user-home-dir/.ssh/authorized_keys
```

IMPORTANT: The angle bracket (>>) or greater-than symbol is repeated twice, in order to append. A single angle bracket overwrites instead of appending.

5 Repeat this procedure for every remote machine that should send password changes to the Nsure Identity Manager driver for Linux and UNIX.

To ensure that the SSH configuration is complete, execute the following command at the root user's prompt:

```
ssh target-machine hostname
```

This will return the *target-machine* of the SSH configuration.

Completing the SSH Configuration So the PAM Module Can Be Installed on a Remote Machine

The remote machine must trust the machine where the Driver is installed. This is necessary so that the PAM module can be installed on the remote machine using SSH.

1 Make sure you meet the prerequisites for setting up SSH:

- You must have root privileges on both machines
- ssh server must be running on the remote machine
- ssh client must be available on the machine the driver is running on

2 Generate a public/private key pair on the machine where the driver is installed.

2a Generate a key pair using the following command:

```
ssh-keygen -t dsa
```

2b Accept the default name (for example, .ssh/id_dsa) or specify a different name for the key pair generated

2c When prompted for a passphrase, press Enter without typing a passphrase.

It is necessary to have an empty passphrase; the utility will not work otherwise.

2d Press Enter when prompted again to verify the passphrase.

3 Copy the public key (.pub extension) to the remote machine.

For example:

```
scp root-user-home-dir/.ssh/id_dsa.pub target-machine:/
id_dsa.pub
```

4 On the remote machine, add the contents of this public key to the list of trusted keys.

The list of trusted keys is the authorized_keys file in the .ssh directory in the root user's home directory. If the id_dsa.pub key has been copied to the remote machine, this command can be executed on the remote machine:

```
cat /id_dsa.pub >> root-user-home-dir/.ssh/authorized_keys
```

IMPORTANT: The angle bracket (>>) or greater-than symbol is repeated twice, in order to append. A single angle bracket overwrites instead of appending.

5 Repeat this procedure for every remote machine that you want to configure the PAM utility on.

To ensure that the SSH configuration is complete, execute the following command at the root user's prompt:

```
ssh target-machine hostname
```

This will return the *target-machine* of the SSH configuration.

Uninstallation

To uninstall the driver, execute the following command:

```
nis-drv-uninstall
```

Upgrade

You can upgrade all existing DirXML 1.0 drivers to 2.0.

Prerequisites

- The NDS2NIS.jar must be replaced with the latest version. The native binary Dxnis should also be replaced with the latest version. To upgrade, run the NIS 2.0 installation script. This will over write all the existing binaries.
- Additional NIS PAM module must be installed on all machines of the network to participate in bidirectional password synchronization. To install the PAM module, refer "Installation" on page 22 and "Post-Installation" on page 23.

Procedure:

1 Convert all NIS 1.0 rules to Identity Manager 2.0 format.

1a In iManager, click DirXML Management > Overview and then select the driver set that contains the driver you want to convert.

1b Click the icon for the driver you want to convert.

You are prompted to convert the driver to Identity Manager 2.0 format.

1c Follow the steps in the wizard to complete the conversion.

2 Use the Password Synchronization 2.0 Additional policies overlay template and upgrade the existing object.

3 Add the nspmPassword distribution attribute to the filter for the user class:

```
<filter-attr attr-name="nspmDistributionPassword" merge-authority="none"
publisher="ignore" publisher-optimize-modify="false" subscriber="not
```

4 Make changes according to the table below:

Location	Change Description	Remarks
<*driver-options*>	Add this new init parameter: `<hash-mode display-name="Hashing mode used:">Crypt</hash-mode>` Values can be either CRYTP or MD5.	This is a mandatory input and is valid for all three database types.
<*publisher-options*>	Add this new init parameter: `<pub-heartbeat-interval display-name="Heartbeat interval (minutes):">0</pub-heartbeat-interval>` Ensure that the values have been modified.	Valid for all three database types.
<*driver-options*>	Add this new init parameter: `<map-files-directory display-name="Directory of files corresponding to NIS maps:">/etc/</map-files-directory>`	This is a mandatory input if the database type is NIS.

Location	Change Description	Remarks
New Rule in the subscriber channel and its chaining	Create a new DirXML rule object called Account Management Rules using the policy builder. Click Edit XML and add the following rules to the policy and save the rules. After it is saved, check if you are able to view these rules through the policy builder. 1.<rule> <description>NIS Account Entitlements: Re-enable</description> <conditions> <and> <if-operation op="equal">modify</if-operation> <if-entitlement name="NISAccount" op="changing"/> <if-entitlement name="NISAccount" op="available"/> <if-global-variable name="sp.account.add" op="equal">enable</if-global-variable> </and> </conditions> <actions> <do-set-dest-attr-value name="authPassword"> <arg-value> <token-text>*!!*</token-text> </arg-value> </do-set-dest-attr-value> <do-break/> </actions> </rule>	The contents of the Entitlement rule can be obtained from the Entitlement Rule in the new import file.

Location	Change Description	Remarks
	2.<rule> <description>NIS Account Entitlement: Re Disable</description> <conditions> <and> <if-operation op="equal">modify</if-operation> <if-entitlement name="NISAccount" op="changing"/> <if-entitlement name="NISAccount" op="available"/> <if-global-variable name="sp.account.add" op="equal">disable</if-global-variable> </and> </conditions> <actions> <do-set-dest-attr-value name="authPassword"> <arg-value> <token-text>!!</token-text> </arg-value> </do-set-dest-attr-value> <do-break/> </actions> </rule>	

Location	Change Description	Remarks
	3.<rule> <description>NIS Account Entitlement: Disable</ description> <conditions> <and> <if-entitlement name="NISAccount" op="changing"/> <if-entitlement name="NISAccount" op="not-available"/ > <if-global-variable name="sp.account.remove" op="equal">disable</if-global-variable> </and> </conditions> <actions> <do-set-dest-attr-value name="authPassword"> <arg-value> <token-text>!!</token-text> </arg-value> </do-set-dest-attr-value> </actions> </rule>	

Location	Change Description	Remarks
	4.<rule> <description>NIS Account Entitlement: Delete</description> <conditions> <and> <if-entitlement name="NISAccount" op="changing"/> <if-entitlement name="NISAccount" op="not-available"/> <if-global-variable mode="nocase" name="sp.account.remove" op="equal">delete</if-global-variable> </and> </conditions> <actions> <do-delete-dest-object/> <do-remove-association direct="true"> <arg-association> <token-association/> </arg-association> </do-remove-association> <do-break/> </actions> </rule> Next Transform/ Rule chaining: Ensure that the polices are chained correctly. Set the Next Transform of Command Transform to Account Management Rules. Also, chain the new password polices to Account Management Rules.	
Subscriber channel	On the Subscriber channel, delete the Event Transform object. This is no longer necessary for NIS 2.0.	

5 (Conditional) Perform the following operations if you need NIS 2.0 to support Role-Based Entitlements.

NIS 2.0 supports Account Entitlements. For more information, refer to "Role-Based Entitlements in NIS" on page 55.

Location	Change Description	Remarks
<*filter-class*>For classname="User"	<filter-attr attr-name="DirXML-SPEntitlements" merge-authority="none" publisher="ignore" publisher-optimize-modify="false" subscriber="notify"/>	Typically, NIS 2.0 adds or deletes this entry in the filter depending upon the need for Role-Based Entitlements during import.
Subscriber channel, Create Rule transforms.	Because the existing transform is a style sheet, create a new policy using the Policy Builder and link it to the existing Create Rule Transform using the Next-Transform. Include the following in the new policy that you create: <rule> <description>NIS Account Entitlement: Disable Account</description> <conditions> <and> <if-class-name op="equal">User</if-class-name> <if-entitlement name="NISAccount" op="changing"/> <if-entitlement name="NISAccount" op="available"/> <if-global-variable name="sp.account.add" op="equal">disable</if-global-variable> </and> </conditions> <actions> <do-set-dest-password> <arg-string> <token-text>!!</token-text> <token-password/> </arg-string> </do-set-dest-password> <do-break/> </actions> </rule>	

Location	Change Description	Remarks
Subscriber channel, Matching Rule	Include the following in the policy and save it: <rule> <description>Account Entitlement: Veto</description> <conditions> <and> <if-class-name op="equal">User</if-class-name> <if-entitlement name="NISAccount" op="not-available"/> </and> </conditions> <actions> <do-veto/> <do-break/> </actions> </rule>	

Location	Change Description	Remarks
Subscriber channel, Account management rules	Include the following in the policy and save it: 1. <rule> <description>Disable NIS Account when UNIX Profile is removed for a user</description> <conditions> <and> <if-class-name op="equal">user</if-class-name> <if-operation op="equal">modify</if-operation> <if-op-attr name="uidNumber" op="changing"/> <if-op-attr name="uidNumber" op="not-available"/> </and> </conditions> <actions> <do-strip-op-attr name="uidNumber"/> <do-set-dest-attr-value name="authPassword"> <arg-value type="string"> <token-text xml:space="preserve">!!</token-text> </arg-value> </do-set-dest-attr-value> </actions> </rule>	

Location	Change Description	Remarks
	2. <rule> <description>Re-enable NIS Account when UNIX Profile added again</description> <conditions> <and> <if-operation op="equal">modify</if-operation> <if-class-name op="equal">user</if-class-name> <if-op-attr name="uidNumber" op="changing"/> <if-op-attr name="uidNumber" op="available"/> <if-op-attr name="authPassword" op="changing"/> <if-op-attr name="authPassword" op="not-available"/> </and> </conditions> <actions> <do-set-dest-attr-value name="authPassword"> <arg-value type="string"> <token-text xml:space="preserve">*!!*</token-text> </arg-value> </do-set-dest-attr-value> </actions> </rule>	

Location	Change Description	Remarks

<*configuration-manifest*>	The entry below has to be made in the manifest.
	`<capability name="entitlements">……..`
	`<entitlement conflict-resolution="union" description="User account in Files or NIS or NIS+" display-name="NIS User Account" name="NISAccount">`
	`<interpretive-variables>`
	`<add-variable lossy="false" name="sp.account.add"/>`
	`<remove-variable lossy="true" name="sp.account.remove"/>`
	`</interpretive-variables>`
	`</entitlement>`
	`</capability>`	

<*configuration-values*>	Define two new global configuration variables.
	`1.`
	`<definition display-name="Action On Applying NIS Account Entitlement:" name="sp.account.add" type="enum">`
	`<value>enable</value>`
	`<description>When a user is created in eDirectory with a NIS Account entitlement, specify the action you want the driver to take on an associated NIS account.</description>`
	`<enum-choice display-name="Enable the NIS account">enable</enum-choice>`
	`<enum-choice display-name="Disable the NIS account">disable</enum-choice>`
	`</definition>`	

Location	Change Description	Remarks
	2. <definition display-name="Action On Removing NIS Account Entitlement:" name="sp.account.remove" type="enum"> <value>disable</value> <description>When a user's NIS account entitlement is removed in eDirectory, specify the action you want the driver to take on an associated NIS account.</description> <enum-choice display-name="Disable the NIS account">disable</enum-choice> <enum-choice display-name="Delete the NIS account">delete</enum-choice> </definition>	

Activating the Driver

DirXML and DirXML drivers must be activated within 90 days of installation, or they will shut down. At any time during the 90 days, or afterward, you can choose to activate DirXML products to a fully licensed state.

To activate your driver, you should:

1. Purchase DirXML licenses
2. Generate a Product Activation Request
3. Submit the Product Activation Request
4. Install the Product Activation Credential received from Novell

For more information about completing these tasks, refer to the DirXML Documentation Web site (http://www.novell.com/documentation/beta/dirxml20/index.html).

3 Configuring the Nsure Identity Manager Driver for Linux and UNIX

This sections tells you how to configure the DirXML® driver for Linux and UNIX. It covers the following:

Setting Up the Driver

This section explains the following:

Before You Set Up the Driver

- Ensure that you have configured Novell® eDirectory™ and the DirXML Engine before configuring the Nsure Identity Manager driver for Linux and UNIX.
- Ensure that the iManager plug-in for DirXML is installed.
- Users and groups are placed in a specific container in eDirectory. So, ensure that you have the DN or FDN for user and group containers to be synchronized in eDirectory.
- The eDirectory schema for the Nsure Identity Manager driver for Linux and UNIX needs to be extended.

Setting Up the Driver

1. In iManager, click DirXML Utilities > Create Driver.
2. Do one of the following:
   - Select In an Existing Driver Set, then specify the path where you want the name of the object to be created or use the Object Selector icon to select it.
   - Select In a New Driver Set, then click Next.
     - Specify the name of the driver set.
     - Specify the context for the new driver set or use the Object Selector icon to select it.

3 Click Next.

4 Do one of the following:

- Click Import a pre-configured driver from the server (.XML file), then select the appropriate .xml file from the drop-down list.
- Click Import a pre-configured driver from the client (.XML file), then specify or browse to the appropriate .xml file.

The preconfigured XML files NIS.xml and NIS_en.xlf are available in the /usr/lib/dirxml/rules/nds2nis directory of the machine where the driver is installed. Copy these files to the webapps/nps/DirXML.Drivers directory of the server where iManager is installed.

5 Click Next.

6 Specify the name of the driver.

If you are updating an existing driver, select a driver from the Existing drivers drop-down list.

7 Select the database in use for your network-wide information storage.

Select Files for local file-based storage, NIS for map-based storage, or NISPlus for hierarchical, domain-based storage.

8 If you want this driver to use entitlements granted through shared profiles, select Yes from the drop-down list.

9 Select the algorithm that is used to hash the passwords.

This is the hashing algorithm that is used on the UNIX server for hashing passwords. The default is Crypt.

10 (Conditional) If you selected Files or NIS in Step 8, refer to "Driver Settings" on page 44 to set the merge-password option based on your system's current settings.

The default is No.

11 (Conditional) If you selected NIS in Step 8, specify the path of the directory where the NIS maps are to be found.

Typically, this is /var/yp/*domain name*. Run the domainname command to get the domain name.

The default path is /var/yp/org.domain.com

12 (Conditional) If you selected NIS in Step 8, specify the path of the directory where files corresponding to the NIS maps are to be found.

The default path is /etc/.

13 (Optional) Select Yes from the drop-down menu, if you want to create a home directory when the user is created.

The default is No.

14 (Optional) Select Yes from the drop-down menu, if you want to remove the home directory when the user is deleted.

The default is No.

WARNING: If this option is set to Yes, the user's home directory and its contents will be completely deleted and cannot be recovered.

15 (Optional) Select Yes from the drop-down menu, if you want to allow a duplicate uidNumber for a user or gidNumber for a group.

The default is No.

16 (Optional) Select Yes from the drop-down menu, if you want the driver to automatically generate user IDs.

The default is No.

17 Specify the minimum value for generating user IDs.

ID generation will use this value as the first user ID. The default is 500.

18 Specify the maximum value for generating user IDs.

ID generation will use this value as the last user ID. The default is 60000.

19 Specify the default primary group ID for the user.

Ensure that the corresponding group exists and is synchronized through this driver. You can create this group after the driver is configured and the group is synchronized.

20 Specify the default home directory prefix for the user:

The home directory is set as the user's common name prefixed with the string that is provided.

21 (Optional) If you want to set a default password for users, select Yes from the drop-down menu.

The password is set to the user's common name. The default is No.

22 (Optional) If you want the driver to generate group IDs, select Yes from the drop-down menu..

The default is No.

23 Specify the minimum value for generating group IDs.

ID generation will use this value as the first group id. The default is 500.

24 Specify the maximum value for generating group IDs.

ID generation will use this value as the last group ID. The default is 60000.

25 Select one of the following for data flow:

- **Bi-directional:** Both NIS and eDirectory are authoritative sources of the data synchronized between them.
- **NIS to eDirectory:** NIS is the authoritative source.
- **eDirectory to NIS:** eDirectory is the authoritative source.

26 Specify the interval (in seconds) for Publisher polling.

The polling interval is used before changes in the NIS datastores are checked for.

27 Specify in dot format or browse to select the DN of the container from or to where users should be synchronized to the application.

28 Specify in dot format or browse to select the DN of the container from or to where groups should be synchronized to the application.

29 Select the option for configuring the driver:

- **Local:** Driver is running locally on a DirXML server.
- **Remote:** Driver is running with the Remote Loader Service on a non-DirXML server.

30 (Conditional) If you selected Remote in Step 31, do the following:

30a Specify the hostname or IP address and the port number of the machine where the Remote Loader Service has been installed and is running for this driver.

The default port is 8090.

30b Specify the driver password.

The Driver Object Password is used by the Remote Loader to authenticate itself to the DirXML server. It must be the same as specified for the Driver Object Password on the DirXML Remote Loader.

30c Specify the password to control access to the Remote Loader instance.

This password must be the same as specified for the Remote Loader password on the DirXML Remote Loader.

31 Click Next.

32 Click Define Security Equivalences.

33 To add the name of the object (such as Admin) whose privileges are granted to the driver, then click Add > OK.

34 (Optional) Click Exclude Administrative Roles and specify the objects to be excluded from synchronization.

35 Click Next.

36 To view the overview of the newly created driver, click Finish with Overview.

Configuring Driver Startup

The driver can be started using any of the startup options provided. However, if eDirectory is not installed on the application platform, you must use the Remote Loader to start it. For more information, refer to the DirXML Administration guide (http://www.novell.com/documentation/beta/dirxml20/index.html).

You can set driver startup to any of the following three options:

- **Automatic:** Any time the DirXML engine is started the driver is started automatically. After you have the driver configured, you should use this option.
- **Manual:** The driver can be started manually. This option is often used during driver modification and testing cycles. The engine will buffer the changes to be processed when driver is started.
- **Disabled:** If the driver is disabled, data changes made in eDirectory during the time a driver is disabled will be automatically synchronized upon driver startup.

To configure the driver startup:

1 In iManager, select DirXML Management > Overview.

2 Select the driver set containing the driver, click the driver icon to see the driver overview, then click the driver icon again to get the Modify Object page.

3 Click Driver Configuration at the top of the page, then select one of the three options listed under Startup Option.

4 Click OK.

NOTE: The Nsure Identity Manager driver for Linux and UNIX can be run only on the application platform, which is the machine with the Files, NIS, or NIS+ databases.

Configuring the Remote Loader

You can use the Java Remote Loader or the native Remote Loader available with Identity Manager 2.0. To configure the remote loaders, refer:

- "Configuring the Native Remote Loader" on page 43
- "Configuring the Java Remote Loader" on page 43

To use the remote loader, ensure that the driver is already installed on the machine that you are using.

The Remote Loader and Driver passwords are the same as the ones specified in the Authentication and the Driver Object Password tabs.

IMPORTANT: During the Publisher channel invocation for FILES/NIS/NIS+, several files are created in the driver directory (for example, in the Remote Loader directory for a Remote Loader setup).

If the driver is running on the machine hosting eDirectory, the files are created in /var/nds/dib directory. These are temporary files and will contain information about the processed/synchronized users and groups by the driver.

These are large files, so ensure that you have enough disk space.

Configuring the Native Remote Loader

1. Install the Identity Manager 2.0 Remote Loader on the application platform.

   This installs the binary /usr/bin/rdxml (native Remote Loader). The application platform is the machine with the Files, NIS, or NIS+ databases.
2. Create a directory on the application platform from where you want to execute the native Remote Loader.
3. Create a configuration file with the class name com.novell.nds.dirxml.driver.nisdriver.NISDriverShim.
4. Set the Driver Object and Remote Loader passwords with the following command:

   ```
   rdxml -config <file-name> -sp <remote-loader-password> <driver password>
   ```
5. Start the native Remote Loader with the following command:

   ```
   rdxml -config <file-name>
   ```

NOTE: Ensure that there is only a single space between the string -class and the class name in the config file.

For more information on configuring the Native Remote Loader, refer to the DirXML Administration guide (http://www.novell.com/documentation/beta/dirxml20/index.html).

Configuring the Java Remote Loader

If a Java Remote Loader is used, ensure that a java 1.4 JDK/JRE is available on the disk.

1. Extract the files from the RemoteLoader.tar file (for example, tar xvf RemoteLoader.tar).
2. Create a configuration file with the class name com.novell.nds.dirxml.driver.nisdriver.NISDriverShim.
3. Copy the NDS2NIS.jar file from the /usr/lib/dirxml/classes directory to the RemoteLoader/lib directory.
4. Set the Driver Object and Remote Loader passwords with the following command:

```
./dirxml_jremote -config <file-name> -sp <remote-loader- password>
<driver-password>
```

5 Start the Remote Driver with the following command:

```
./dirxml_jremote -config <file-name>
```

NOTE: Ensure that there is only a single space between the string *-class* and the class name in the config file.

Configuring Driver Parameters

The driver parameters can be configured using iManager.

- "Configuring Driver Parameters" on page 44
- "Driver Parameters" on page 44

Configuring Driver Parameters

1 In iManager, click DirXML Management > Overview.

2 Select the driver set containing the driver, click the driver icon to see the driver overview, then click the driver icon again to get the Modify Object page.

3 Click Driver Configuration at the top of the page, then select Driver Parameters.

4 Specify the desired information.

5 Click OK.

See "Driver Parameters" on page 44 for information about the specific parameters and their values.

Driver Parameters

Driver parameters are divided into the following settings:

- "Driver Settings" on page 44
- "Subscriber Settings" on page 46
- "Publisher Settings" on page 47

Driver Settings

The following table lists the driver settings and their default values in the sample configuration:

Parameter	Sample Configuration Value
nistype	files, nis, or nisplus
map-directory	/var/yp/domain_name
merge-password	No
map-files-directory	/etc/
hash-mode	Crypt

nistype

Specifies the database type for NIS. Its valid values are files, nis, nisplus.

map-directory

Specifies the directory for NIS map files. It is valid only for NIS(YP).

merge-password

Specifies whether the shadow and password files are merged on the system. Values can be either Yes or No. The default is No. This parameter is valid only for Files and NIS(YP).

While importing a driver, you are prompted with a `Password and shadow information merged message`. Specify the correct value as per the following table:

Files	Value	Remarks
User information is available only in /etc/passwd file	Yes	Absence of the /etc/shadow file is also sufficient to indicate that Password and shadow information merged option is Yes. For example, on AIX, the password is not stored in /etc/passwd file. But, because there is no /etc/shadow file, the correct value is Yes.
User information is split between the /etc/passwd and /etc/shadow file	No	

NIS (YP)	Value	Remarks
User information is available only in one passwd map	Yes	This value is not dependent on /etc/passwd and /etc/shadow files. Maps are considered only if NIS (YP) is used as the database.
User information is split between passwd and shadow maps.	No	

IMPORTANT: This information is not relevant if NIS+ is used as the database.

The following table specifies the database and the values for merge-password:

Database	Values
NIS(YP)	False: If password and shadow maps are present True: If there is only a password map
Files	False: If password and shadow files are present True: If there is only a password file

map-files-directory

Specifies the directory where the files corresponding to NIS maps are to be found.

hash-mode

Specifies the hashing algorithm used on the UNIX server (the machine that hosts the NIS driver) to hash passwords.

Subscriber Settings

The following table lists the Subscriber settings and their default values in the sample configuration:

Parameter	Sample Configuration Value
create-homedirectory	No
remove-homedirectory	No
allow-duplicate	No
userid-generate	No
default-groupid	500
min-userid	500
max-userid	60000
groupid-generate	No
min-groupid	500
max-groupid	60000

create-homedirectory

Indicates whether to create the home directory when a user is added. Values can be either Yes or No. The default is No.

remove-homedirectory

Indicates whether to remove the home directory upon user deletion. Values can be either Yes or No. The default is No.

allow-duplicate

Lets you add the duplicate UIDs and GIDs in the Files database upon user creation or modification on the Subscriber channel. Values can be either Yes or No. The default is No.

This option is not supported for AIX.

IMPORTANT: Do not change the default value for NIS(YP).

userid-generate

Indicates whether a uidNumber is to be generated for a user. Values can be either Yes or No. The default is No.

default-groupid

Indicates the default group to which the user belongs.

min-userid

Specifies the minimum value for the UID generated for the user. The default value is 500.

max-userid

Specifies the maximum value for the UID generated for the user. The default value is 60000.

groupid-generate

Indicates whether a gidNumber is to be generated for a group. Values can be either Yes or No. The default is No.

min-groupid

Specifies the minimum value for the GID generated for the group. The default value is 500.

max-groupid

Specifies the maximum value for the GID generated for the group. The default value is 60000.

Publisher Settings

The following table lists the Publisher settings and their default values in the sample configuration:

Parameter	Value
publisher-disable	No
polling-interval	
pub-heartbeat-interval	2

publisher-disable

Specifies whether the Publisher is to be enabled or disabled. Values can be either Yes or No. The default is No.

NOTE: The publisher-disable option should not be set to Yes if the ID Generation is enabled.

polling-interval

Specifies the time (in seconds) as the polling interval before checking for new source files to process.

pub-heartbeat-interval

Specifies the time (in minutes) after which the driver sends a status document. The default is 0.

User and Group Containers

This section describes about placing, matching, and synchronizing user and group containers in eDirectory.

- “Placing New Users and Groups” on page 48
- “Matching User and Group Containers” on page 48

Placing New Users and Groups

You can specify the DN of the container for new users and groups.

To place new users and groups:

1. In iManager, click DirXML Management > Overview.
2. Locate the driver in its driver set.
3. Click the driver to open the Driver Overview Page.
4. Click the Publisher channel to edit the Placement Policies.
5. Replace *USERS_O.ORG_O* with the required DN of the container in slash format where new users are to be placed in the following line:

   ```
   <token-text xml:space="preserve">USERS_O.ORG_O</token-text>
   ```

6. Replace *GROUPS_O.ORG_O* with the required DN of the container in slash format where new groups are to be placed in the following line:

   ```
   <token-text xml:space="preserve">GROUPS_O.ORG_O</token-text>
   ```

NOTE: Ensure that the DN of containers for users and groups in Placement and Matching policies is the same as the FDN of containers for users and groups in the Event Restrictions policy.

Matching User and Group Containers

You can specify the DN of the container whose users and groups are to be matched.

To match user and group containers:

1. In iManager, click DirXML Management > Overview.
2. Locate the driver in its driver set.
3. Click the driver to open the Driver Overview Page.
4. Click the Publisher channel to edit Event Restrictions from the Matching Policies.
5. Replace *USERS_O.ORG_0* with the required DN of the container in slash format whose users are to be matched in the following line:

   ```
   <if-src-dn op="not-in-container">USERS_O.ORG_O</if-src-dn>
   ```

6. Replace *GROUPS_O.ORG_O* with the required DN of the container in slash format whose groups are to be matched in the following line:

   ```
   <if-src-dn op="not-in-container">GROUPS_O.ORG_O</if-src-dn>
   ```

   NOTE: Ensure that the DN of containers for users and groups in Placement and Matching policies is the same as the FDN of containers for users and groups in the Event Restrictions policy.

4 Guidelines for Configuring Policies

You can modify the Subscriber Create Rule Transform policy to implement your specific business rules. This policy modifies the <add> event; for example, providing default values for attributes. In the preconfigured driver file, this policy in Subscriber channel provides default values for homeDirectory, loginShell, and gidNumber for Users.

This section discusses the guidelines for configuring DirXML scripts. It covers the following:

Adding Defaults for Users

The Create Rule Transform policy can be edited to provide default values for password, homeDirectory, loginShell, and gidNumber for users as follows:

To edit the Create Rule Transform policy from the Subscriber channel:

1. In iManager, click DirXML Management > Overview.
2. Locate the driver in its driver set.
3. Click the driver to open the Driver Overview Page.
4. Click the Creation Rule on the Subscriber channel.
5. Click the Create Rule Transform policy to edit the policy.
6. To provide a default home directory for user creation, replace */home* with the desired home directory prefix for user in the last line of the following section:

   ```
   <do-add-dest-attr-value name="homeDirectory">
     <arg-value>
       <token-text>/home</token-text>
   ```

7. To provide a default value for loginShell for the user:

   Replace */bin/sh* with the desired login shell for user in the last line of the following section:

   ```
   <do-add-dest-attr-value name="loginShell">
     <arg-value>
       <token-text>/bin/sh</token-text>
   ```

8. To provide a default gidNumber for the user:

   Replace 500 with the desired primary group ID for the user in the last line of the following section:

```
<do-add-dest-attr-value name="gidNumber">
  <arg-value>
    <token-text>500</token-text>
```

9 To provide default password for user:

Replace <*token-xpath...*> to the desired default password in the following line:

```
<do-set-dest-password>
  <arg-string>
   <token-text>pass</token-text>
```

The clear-text password must be provided in the policy in the <password> tag. The driver will then set this as the initial driver password for the User.

10 If default password is set to No during configuration, add the default password template by adding the following If clause below the homeDirectory template:

```
<rule>
  <description>Adds username as the default password</description>
  <conditions>
    <and>
      <if-operation op="equal">add</if-operation>
      <if-class-name op="equal">User</if-class-name>
      <if-op-attr name="CN" op="available" />
      <if-op-attr name="authPassword" op="not-available" />
      <if-password op="not-available" />
    </and>
  </conditions>
  <actions>
    <do-set-dest-password>
      <arg-string>
        <token-xpath expression="string(./add-attr[@attr-name='CN']/
value)" />
      </arg-string>
    </do-set-dest-password>
  </actions>
</rule>
```

NOTE: If multiple drivers are running, only one driver should have a default password enabled for users, and only one driver should have ID generation enabled for a particular user or group.

Sample Scripts

The following sample scripts describes including additional functionalities in Create Rule Transform of Subscriber channel:

- “Uppercase and Lowercase for the User’s CN Attribute” on page 51
- “Lowercase for the User’s CN Attribute” on page 52

Uppercase and Lowercase for the User’s CN Attribute

The following is a sample script for transforming the user’s CN attribute value to having the first letter in uppercase and the rest in lowercase:

```
<?xml version="1.0" encoding="UTF-8"?>

<xsl:transform version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/
Transform">

     <xsl:variable name="ucase" select="'ABCDEFGHIJKLMNOPQRSTUVWXYZ'"/>

     <xsl:variable name="lcase" select="'abcdefghijklmnopqrstuvwxyz'"/>

    <xsl:template match="add[@class-name='User']/add-attr[@attr-name='CN']">

         <!--The following lines convert CN attribute value of User to first
upper and rest lower case-->

          <xsl:variable name="orig-cn" select="./value"/>

        <xsl:variable name="first-string" select="substring($orig-cn,1,1)"/>

          <xsl:variable name="last-string" select="substring($orig-cn,2)"/>

          <xsl:variable name="new-cn" select="concat($first-
string,translate($last-string,$ucase,$lcase))"/>

          <add-attr attr-name="CN">

               <value>

                    <xsl:value-of select="$new-cn"/>

               </value>

          </add-attr>

     </xsl:template>

     <xsl:template match="@*|node()">

          <xsl:copy>

               <xsl:apply-templates select="@*|node()"/>

          </xsl:copy>

     </xsl:template>

</xsl:transform>
```

To implement specific business rules for groups, modify this script appropriately.

Lowercase for the User's CN Attribute

The following is a sample script for transforming the user's CN attribute value to all lowercase letters:

```
<?xml version="1.0" encoding="UTF-8"?>

<xsl:transform version="1.0" xmlns:xsl="http://www.w3.org/1999/XSL/
Transform">

     <xsl:variable name="ucase" select="'ABCDEFGHIJKLMNOPQRSTUVWXYZ'"/>

     <xsl:variable name="lcase" select="'abcdefghijklmnopqrstuvwxyz'"/>

    <xsl:template match="add[@class-name='User']/add-attr[@attr-name='CN']">

         <!-- The following two lines converts the CN attribute value of the
User to lower case -->

          <xsl:variable name="orig-cn" select="./value"/>

    <xsl:variable name="new-cn" select="translate($orig-cn,$ucase,$lcase)"/>

      <add-attr attr-name="CN">

           <value>

                <xsl:value-of select="$new-cn"/>

           </value>

      </add-attr>

   </xsl:template>

   <xsl:template match="@*|node()">

      <xsl:copy>

        <xsl:apply-templates select="@*|node()"/>

      </xsl:copy>

   </xsl:template>

</xsl:transform>
```

To implement specific business rules for groups, modify this script appropriately.

Synchronizing User and Group Containers

You can specify the DN of the container whose new Users and Groups are to be synchronized with the application.

Refer "Event Restrictions" on page 20 to set this parameter.

Synchronizing large number of users or groups from eDirectory to NIS databases takes a long time on the Subscriber channel.

Disabling the publisher channel helps in preventing loopback in the driver level during synchronization. In a normal scenario, the DirXML engine prevents loopback. But, this is done after receiving changes back from NIS. Removing the Matching Rule will increase the synchronization speed by disabling query for add operations.

To improve the synchronization speed:

1. Disable the Publisher channel. If the ID generation is enabled, then Publisher channel should not be disabled.
2. Detach the Matching Policy from the Account Restrictions policy on the Subscriber channel of the driver.
3. Create indexes for uidNumber, gidNumber, and Group Membership on eDirectory.

   Synchronizing large number of users and groups will result in large number of searches in eDirectory. Indexing will improve the search operation in eDirectory. For more information, refer to the *Novell eDirectory Administration Guide* (http://www.novell.com/documentation/lg/edir873/index.html).

5 Using the Nsure Identity Manager Driver for Linux and UNIX

This section describes using the DirXML® driver for Linux and UNIX. It covers the following:

Role-Based Entitlements in NIS

The Nsure Identity Manager driver for Linux and UNIX supports Accounts Entitlements.

The following table lists the configuration values and actions for entitlements:

Event	Configuration Value	Action
Add Entitlement	enable	Creates an enabled account in NIS
Add Entitlement	disable	Disables an account in NIS
Remove Entitlement	disable	Disables an account in NIS
Remove Entitlement	delete	Deletes an account in NIS

Synchronizing the AuthPassword Attribute

The UNIX passwords of users can be stored in the Authpassword attribute in Novell® eDirectory™ for that user. The Authpassword attribute is a multivalued attribute that can store the MD5 and CRYPT hash of the password for that user. For the NIS Driver to update the Authpassword attribute of the user, the PAM module must be installed and configured to capture any password change of the user. It is essential for the NIS driver to obtain the password in clear-text so that the NIS Driver can generate both MD5 and CRYPT hash and update the Authpassword attribute. Hence, the Authpassword attribute will be updated during password change operation only, not during user add operation.

In a multi-platform scenario, when few machines have MD5 and few have CRYPT form of the password, ensure that the correct hash mode is specified during import. If there is a password change in one of the machines, the Authpassword attribute is updated with MD5 and CRYPT. These changes are appropriately synchronized to the rest of the machines through the NIS driver as the driver picks the correct hash and sets it on the target machines.

It is recommended that when Universal password is set up, Authpassword sync option should not be turned on. However, when the AuthPassword sych option is turned on and the universal password is set up, the following occurs:

- On the Subscriber channel, the distribution password is set as the UNIX password. However, if there are no changes in the distribution password and there are changes only in the Authpassword attribute for the user, the correct hash MD5/CRYPT is picked up and set as the password on UNIX.
- On the publisher side, the distribution password is always updated during password change. The Authpassword attribute is also updated MD5 and CRYPT hash in the same sequence as the distribution password.

To enable AuthPassword synchronization to eDirectory:

1. In iManager, click DirXML Management > Overview.
2. Locate the driver in its driver set.
3. Click the driver to open the Driver Overview Page.
4. Click the icon for the driver.

   A page opens where you can edit various driver parameters.
5. Under Driver Parameters, click Edit XML to add the following line in the <driver-options> tag:

   <sync-AuthPass display-name="Synch AuthPassword">yes</sync-AuthPass>

   If you want to disable this feature, specify No instead of Yes in the above line.
6. Click OK.

IMPORTANT: When you change the universal password of a user through iManager, the universal password is set in UNIX for that user. However, if the AuthPassword attribute synch option is turned on, the Authpassword value is not updated with the new password. This is updated only when the password is changed in UNIX.

When you change the universal password of a user through iManager, the distribution password is set in UNIX for that user. However, even though the AuthPassword attribute synch option is turned on, the Authpassword value is not updated with the new password. This is updated only when the password is changed in UNIX as mentioned above.

Migrating and Resynchronizing Data

After you start the driver, you can migrate users and groups to and from eDirectory and resynchronize the application and eDirectory.

- “Migrating into eDirectory” on page 57
- “Migrating from eDirectory” on page 57
- “Resynchronizing” on page 57

IMPORTANT: Migration to and from eDirectory should be performed in three steps: migrating the groups; migrating the users; and migrating the groups again to complete the migration of the desired accounts into eDirectory. The driver should be running to migrate and resynchronize data.

Migrating into eDirectory

All the users or groups can be selectively migrated by using the Migrate into eDirectory option.

1. In iManager, select DirXML Management > Overview.
2. Locate the driver set containing the NIS driver, then double-click the driver icon.
3. Click Migrate into eDirectory.
4. Click Edit List to add a list of user or group classes and attributes.
5. Select the User or Group class to migrate all existing users or groups.

   or

   Select the User class and the appropriate attribute.
6. Specify the value for the attribute.

   This value is used to determine the objects that are migrated into eDirectory. The valid pattern for attribute is .* for matching all users or groups.
7. Click OK.

Migrating from eDirectory

All the users or groups having a UNIX profile can be selectively migrated by using the Migrate from eDirectory option.

1. In iManager, select DirXML Management > Overview.
2. Locate the driver set containing the NIS driver and then double-click the driver icon.
3. Click Migrate from eDirectory, then click Add to add the objects to be migrated.
4. Click OK.

Resynchronizing

If you want to have an immediate synchronization of all managed object classes, you can use the synchronization function of DirXML.

1. In iManager, select DirXML Management > Overview.
2. Locate the driver set containing the NIS driver, then double-click the driver icon.
3. Select the driver that you want to resynchronize.
4. Click Synchronize.

Synchronizing and Setting Passwords

The NIS driver supports bidirectional synchronization of distribution passwords. The password synchronization for the driver must be set up using iManager. For more information, refer to the DirXML Administration guide (http://www.novell.com/documentation/beta/dirxml20/index.html).

On the Subscriber channel, the Add User event in eDirectory sets the default password in UNIX. Also, it sets a default distribution password for that user. There are two DirXML script rules which govern this, they can be changed to have any default password in UNIX or distribution password. Further, if you set the universal password for a user using the set the universal password task in

iManager, the password for that user will change in UNIX (this overwrites the earlier UNIX password). Therefore any change in the distribution password will change the password in UNIX. If the Authpassword synchronization option is set to on and the Universal password is not configured, the appropriate Authpassword value is set in UNIX when the Authpassword attribute in eDirectory changes for the user.

On the Publisher channel, when users are created in UNIX, the password is not captured by the driver until the password is set/changed for the first time. The default distribution password can be configured in DirXML scripts rules so that they can be set as distribution password when password in clear-text is not available from UNIX. Every modify password event in UNIX results in the change of distribution password of that user. If the Authpassword synchronization is enabled and a password is changed in UNIX, the Authpassword attribute will be updated with MD5 and Crypt hash of the password.

ID Generation

The ID Generation feature enables you to automatically generate user or group IDs for new users or groups on the Subscriber channel. The user or group ID is a unique number that identifies the user or group to the host UNIX system.

A range for ID generation can be configured in the driver parameter. The driver generates IDs based on the minimum and maximum value provided in the range for add events only. If the driver fails and is restarted, the ID generated will be an increment of the previous value. During subsequent driver startups, if there is a change in the specified range, the driver generates IDs based on the new range.

NOTE: Only a single driver must be configured for ID generation of a UID or GID for a particular user or group.

To configure ID Generation for users or groups during the driver startup:

1. Use the steps in "Setting Up the Driver" on page 39. Select Yes for Steps 17 and 23 while setting up the driver.

To configure ID generation for users or groups while a driver is running:

1. Select the driver in the driver set.
2. Select the Driver Parameters tab.
3. Specify Yes for Allow UID Generation.
4. Specify Yes for Allow GID Generation.
5. Edit the Create Rule policy of the Subscriber channel to replace the following line for user ID generation:

   ```
   <do-veto-if-op-attr-not-available name="uidNumber"/>
   ```

   with

   ```
   <!--<do-veto-if-op-attr-not-available name="uidNumber"/>-->
   ```

6. Replace the following line in the class-name=group for group ID generation:

   ```
   <do-veto-if-op-attr-not-available name="gidNumber"/>
   ```

   with

   ```
   <!--<do-veto-if-op-attr-not-available name="gidNumber"/>-->
   ```

   NOTE: This makes the uidNumber and gidNumber non-mandatory attributes in the Create Rule.

7. Click Apply and Close.
8. Attach the Account Restrictions policy as the Next Transformation of Matching Rule.

To remove the configuration settings for user or group ID generation:

1. Select the driver in the driver set.
2. Select the Driver Parameters tab.
3. Specify No for Allow UID Generation.
4. Specify No for Allow GID Generation.
5. Replace the following line for user ID generation:

   ```
   <!--<do-veto-if-op-attr-not-available name="uidNumber"/>-->
   ```

   with

   ```
   <do-veto-if-op-attr-not-available name="uidNumber"/>
   ```

6. Replace the following line for group id generation:

   ```
   <!--<do-veto-if-op-attr-not-available name="gidNumber"/>-->
   ```

   with

   ```
   <do-veto-if-op-attr-not-available name="gidNumber"/>
   ```

7. Click Apply and Close.
8. Attach the Account Restrictions policy as the Next Transformation of Event Restrictions.

Administering Users and Groups

Users and Groups in eDirectory can be administered through iManager.

POSIX attributes of User: authPassword, gidNumber, gecos, homeDirectory, shadowMin, shadowMax, shadowWarning, shadowLastChange, shadowInactive, shadowExpire, and shadowFlag.

POSIX attributes of Group: gidNumber.

Administering POSIX Attributes for a User and Group

All POSIX attributes of the User and Group can be administered using iManager.

1. Click the Roles and Tasks button.
2. Click eDirectory Administration > Modify Object.

   or

   Click Users > Modify User to modify attributes for a user.

   Click Groups > Modify Group to modify attributes for a group.
3. Using the Object Selector icon, select the object you want to extend and then click OK.
4. Click the UNIX profile tab.

PAM Configuration

If you have a basic setup with default configuration, the nis-drv-config copies the NIS password management PAM module to the PAM modules directory and updates the PAM configuration file. If the basic configuration is not found, the PAM configuration is not done. We strongly recommend that you manually update and verify the PAM configuration file to ensure that the custom configuration is not disturbed and the existing PAM configuration file satisfies the NIS PAM module requirements.

The PAM configuration involves copying the PAM module from the /usr/lib/dirxml/rules/nds2nis directory to the corresponding location on each of the following platforms:

- On Linux: /lib/security/pam_dxml.so
- On Solaris: /usr/lib/security/pam_dxml.so.1
- On HP-UX: /lib/security/libpam_dxml.1

Ensure that you modify the PAM configuration file in one of the following ways:

On Linux AS v2.4.9-e.3 (uname -r)

The /etc/pam.d/passwd file can have the following password management modules:

- password required /lib/security/pam_pwdb.so retry=3
- password required /lib/security/pam_dxml.so use_first_pass use_authtok host=164.99.155.241 db=nis mapfilesdir=/var/yp/nisdomain shadowmerged=true

On Solaris 8 (5.8 Generic_108528-13)

The /etc/pam.conf file can have the following password management modules:

- other password requisite pam_authtok_get.so.1
- other password requisite pam_authtok_check.so.1
- other password required pam_authtok_store.so.1 use_first_pass
- other password required pam_dxml.so.1 use_first_pass use_authtok host=164.99.155.241 db=nis mapfilesdir=/var/yp/nisdomain shadowmerged=true

NOTE: On Solaris you need to create a symbolic link, pam_dxml.so in /usr/lib/security, that points to /usr/lib/security/pam_dxml.so.1. The command is `ln -s /usr/lib/security/pam_dxml.so.1 /usr/lib/security/pam_dxml.so`

On HP-UX 11i

The /etc/pam.conf file can have the following password management modules:

- passwd password required /usr/lib/security/libpam_unix.1
- passwd password required /usr/lib/security/libpam_dxml.1 use_first_pass use_authtok host=164.99.155.241 db=nis mapfilesdir=/var/yp/nisdomain shadowmerged=true

Ensure that you have the following parameters with the correct values for the NIS driver's PAM module pam_dxml.so:

- **host=hostname:** Specifies the name or IP address of the machine where NIS driver is running. This parameter will be empty if the PAM module and driver are installed on the same machine. If the IP address is of a remote machine, ensure that SSH is set up and it is possible to execute commands on a remote machine using SSH.

- **mapfilesdir=/var/yp/domainname**: This is the path to the NIS maps.
- **db=files:** Specifies the datastore. Values can be Files, NIS, or NIS+.
- **shadowmerged=false:** Specifies whether the NIS database is configured to support shadow files or not. If a shadow file is present, the value of this parameter is false; otherwise, it is True.
- **use_first_pass:** This tag is used to instruct the NIS PAM module not to prompt for a password and to get it from the previous module.

Files Created by the Driver

During driver execution, some temporary files are also created; however, these files are deleted by the driver itself.

The following files are created when a driver runs:

- "Files Driver" on page 61
- "NIS Driver" on page 61
- "NIS+ Driver" on page 61

Files Driver

- dxnisfiles.stamp
- passwd.log files
- passwd.log.tmp files
- group.log files
- group.log.tmp files
- shadow.log files (these files are created only if the shadow file is present)
- shadow.log.tmp files (these files are created only if the shadow file is present)

NOTE: Ensure that you manually delete the above files after removing the driver from the driver set.

NIS Driver

- dxnisyp.stamp
- passwd.byname.log files
- passwd.byname.log.tmp files
- group.byname.log files
- group.byname.log.tmp files
- shadow.byname.log files (these files are created only if the shadow file is present)
- shadow.byname.log.tmp files (these files are created only if the shadow file is present)

NOTE: Ensure that you manually delete the above files after removing the driver from the driver set.

NIS+ Driver

- dxnisplus.stamp

NOTE: Ensure that you manually delete the above file after removing the driver from the driver set.

6 Troubleshooting the Nsure Identity Manager Driver for Linux and UNIX

This section explains how to troubleshoot the DirXML® driver for Linux and UNIX.

NDSTrace Utility and Error Codes

In case of an error, use the NDSTrace utility available in the /usr/bin/ndstrace directory on the machine where Novell® eDirectory™ is installed to diagnose the cause of the error. The error generated by the driver for an add/modify/delete/query operation of a User or Group in the Publisher Channel is logged in the DIRXML.LOG file (or the log files in rdxml side).

For more information on using the NDSTrace utility, refer to the DirXML Administration guide (http://www.novell.com/documentation/beta/dirxml20/index.html).

Following are explanations of some possible error messages:

ERR_ENTRY_EXISTS

Possible Cause: The User or Group being added already exists in the NIS database, or the uidNumber/gidNumber already exists.

Action: Change the name, uidNumber, or gidNumber of the object so that it is unique in the NIS database.

ERR_INVALID_VALUE

Possible Cause: The User or Group to be modified does not exist or a user's primary group gidNumber does not exist.

ERR_ENTRY_INUSE

Possible Cause: The user to be modified is currently in use.

Action: Try again after logging out the user.

ERR_PASSWD_FAILURE

Possible Cause: Some other program has locked the password or shadow file so the password was not updated.

Action: Ensure that there is no other program editing the password or shadow file, when a User password is added or modified.

ERR_ID_INUSE

Possible Cause: The specified range for ID generation has already been assigned and is in use.

Explanation: The range specified for ID generation might be in use. The driver retries after every 30 seconds to generate ID within the specified range.

Action: Modify the ID generation range to an unused ID.

ERR_INSUFFICIENT_ACCESS

Possible Cause: The object specified in the Security Equivalences for the driver does not have enough privileges.

Action: Ensure that the object specified in the Security Equivalences for the driver has enough privileges for the requested operation.

ERR:-299 - Unable to bind DirXML Driver

Possible Cause: The LD_LIBRARY_PATH is not set.

Action: Ensure that the LD_LIBRARY_PATH is set to /usr/lib/nds-modules/jre/lib/i386.

Set the LD_LIBRARY_PATH at the command prompt using the following command:

LD_LIBRARY_PATH=/usr/lib/nds-modules/jre/lib/i386:$LD_LIBRARY_PATH

export LD_LIBRARY_PATH

NOTE: This is required only on Linux.

ERR_NO_SUCH_ATTRIBUTE

Possible Cause: The schema has not been extended for the NIS driver.

Action: Ensure that the schema has been extended for NIS driver using the nisdrvconfig script.

ldap_simple_bind_s: Confidentiality required

Possible Cause: The server does not accept clear-text passwords for nisdrvconfig.

Action: Ensure that the LDAP Allow Clear Text Password option is enabled in eDirectory version 8.6.2.x or the Require TLS for Simple Binds with Password option is disabled in eDirectory version 8.7.x.

ERR_DATABASE_FAILURE

Possible Cause: Improper configuration of the driver parameters.

Action: 1. Ensure that the value of the merge-shadow option provided in the driver configuration parameters is correct. For more information, refer to “Driver Settings” on page 44.

2. Ensure that the paths provided to the maps and files during driver configuration are correct.

Users created in eDirectory are not getting synchronized to UNIX

Action: Ensure that the password policy is associated to the user that is created/modified.

Additional Troubleshooting Information

- Use the passwd command to change passwords for Files/NIS/NIS+ users. You must make appropriate changes to the nsswitch.conf file for the passwd command to work. Do not use

the yppasswd and passwd -r commands because they will bypass PAM and, consequently the NIS PAM module will not be able to capture passwords.

If a local user has the same name as the NIS user, make sure that the nsswitch.conf is configured properly so that the NIS password also changes in addition to the local user password.

- In a setup where NIS drivers are installed on AIX, we do not recommend modifying the GID of a group that has members in it. If you change the GID of a group, the members of that group will continue to have references to the previous GID; when the user record changes. AIX will not allow changes to the user GID because the GID that exists in the user record does not exist in the system.
- If you add a user using the useradd command and specify the password during useradd, the NIS PAM module will not be able to capture the password and hence the password synchronization to eDirectory fails.
- Password sync from UNIX to eDirectory fails if the earlier Unix and eDirectory passwords are different.
- If the YP files are placed in a directory other than /etc/, ensure that the yppasswdd daemon is started with the yppasswdd /var/yp/etc/ -m option. This will enable the yppasswdd daemon to locate the updated password files from a specified directory for building maps after the password changes.
- If the NIS+ Publisher takes a long time to process events: The NIS+ Publisher picks events from the NIS+ transaction log. After all the events have been processed by the Nsure Identity Manager driver for Linux and UNIX, checkpoint the log to speed up the Publisher channel. Ensure that the transaction log is checkpointed by verifying the drivers' log files only after the Nsure Identity Manager driver for Linux and UNIX has processed all the events.

  Checkpoint the transaction log using the following command at the prompt:

  ```
  /usr/lib/nis/nisping -Ca
  ```

- When a User is deleted in NIS and NIS+ on the application platform, the name is not removed from the Group's member list of its secondary groups. Ensure that you manually update the groups member list on the application platform.
- While adding or modifying a Group with a user list in Files, ensure that all the users in the user list are present in the /etc/passwd file and none of the users are currently logged in.
- In AIX, renaming the User or Group and the shadow attributes for the user are not supported; moreover, the Create/Remove Home Directory option cannot be configured for Files. The home directory for a User is created by default; however it is not removed for deletion. This setting is governed by the mkuser.default file from /usr/lib/security/ directory and login.cfg file from /etc/security directory.
- Addition of a User or Group to Files fails if the same name exists for User or Group in NIS or NIS+ and the /etc/nsswitch.conf file contains an entry for NIS or NIS+.
- We strongly recommend that the User or Group record size should not exceed 1024 bytes in any of the databases.
- The default User or Group attributes should be consistent across all platforms. Ensure that these attributes are acceptable in all the platforms. For example: In Linux, a default value of 99999 for shadowMax will not synchronize to AIX.
- The nistbladm command should be used instead of the nisaddent or nispopulate command to modify indexed attributes such as name and gid for groups, and name and UID for users on NIS(+).

- Avoid running any database administration utility when the driver is running.
- Ensure that the appropriate locale is set before running the DirXML Remote Loader or the Novell eDirectory server while synchronizing non-English accounts.
- If the create-homeDirectory is set for users, ensure that you have enough privileges to create the home directory on the application platform.
- The client machines should have access to the home directories created by the driver for NIS(YP) and NIS(+). The access can be set by using the NFS appropriately.
- Ensure that you set the merge-password option based on you system's current settings. For information on recommended values, refer to "Driver Settings" on page 44.
- Ensure that there is only a single space between the string *-class* and the class name in the config file.
- If a user login to NIS database fails, check the default password, homeDirectory, and Login shell.
- If a large number of users (more than 10,000) are to be migrated to eDirectory, the DHOST_JVM_OPTIONS environment variable should be set to -Xmx256m before starting the Remote Loader and eDirectory. This increases the memory available for the JVM.

  To set the above environment variable, use the following command at the shell prompt:

  ```
  DHOST_JVM_OPTIONS=Xmx256m

  export DHOST_JVM_OPTIONS
  ```
- If multiple drivers are running, only a single driver should have a default password enabled for a particular user.
- If multiple drivers are running, only a single driver should be configured for ID generation of the UID or GID for a particular user or group.
- The NIS(YP) driver caches map entries. Because of this, some events are not reflected immediately. Use the makedbm -c command to refresh the ypserv.
- Synchronizing passwords is not supported for groups. The group password will be reset if a group is modified in the eDirectory.
- On Solaris, if the Remove Directory option is selected, users will not be deleted if their home directory is not removable.
- The asterisk character (*) cannot be given in the gecos field. If given, it will remove the already existing value.
- Users or Groups added to eDirectory using the ICE Forward Referencing feature will not be synchronized by the NIS driver. You can use the Migrate from eDirectory option in iManager to synchronize such users or groups.
- In case of a fatal error:
  - Ensure that all the mandatory configuration parameters during driver import/creation are correct.
  - Ensure that NIS YP database is set up correctly and there are no errors while building password and group maps by running make on /var/yp/Makefile.