Novell
IDM Driver for Schools Interoperability Framework

1.5

www.novell.com

IMPLEMENTATION GUIDE

August 24, 2006

Novell®

Legal Notices

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

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

Novell Trademarks

ConsoleOne is a registered trademark of Novell, Inc., in the United States and other countries.
DirXML is a registered trademark of Novell, Inc., in the United States and other countries.
eDirectory is a trademark of Novell, Inc.,
NetWare is a registered trademark of Novell, Inc., in the United States and other countries.
Novell is a registered trademark of Novell, Inc., in the United States and other countries.

Third-Party Materials

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

Contents

About This Guide

The driver for SIF lets you automatically provision users in the Identity Vault and synchronize user accounts the Identity Vault with user data from a SIF-enabled student information system.

This configurable solution gives you the ability to increase productivity, streamline school processes, and reduce errors by automating the transfer of user data to the Identity Vault.

The guide contains the following sections:

SIF is an open standard created to allow K-12 education applications to exchange data effectively. The driver for SIF works as a SIF Agent.

The 1.5.0 release of the driver conforms to SIF Implementation Specifications 1.1 and 1.5r1. For information about the SIF specifications, see the Schools Interoperability Framework Web site (http://www.sifinfo.org).

This release supports only English versions of NetWare® and Windows*.

Audience

This manual is for school administrators, Novell® eDirectory™ administrators, and others who implement the Identity Manager Driver for Schools Interoperability Framework (SIF) in a K-12 school environment.

Feedback

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

Documentation Updates

For the most recent version of this document, see the Drivers Documentation Web site (http://www.novell.com/documentation/lg/dirxmldrivers).

Additional Documentation

For documentation on using Identity Manager and the other drivers, see the Identity Manager Documentation Web site (http://www.novell.com/documentation/lg/dirxml20).

Documentation Conventions

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 Linux or UNIX, should use forward slashes as required by your software.

Introducing the Identity Manager Driver for SIF

1

Managing student and staff accounts manually in a K-12 school system can be a time-consuming job for a Novell® eDirectory™ administrator. Support time and opportunities for human error are multiplied during the influx of students at the beginning of the year, the changes in student enrollment or staff employment throughout the school year, and the end-of-year issues such as disabling accounts or moving students to reflect a school or grade change.

The Identity Manager Driver for Schools Interoperability Framework (SIF) lets you automatically synchronize student, faculty, and staff data in K-12, SIF-enabled applications with user objects in the Identity Vault. Using the driver for managing user accounts provides a great return on investment.

A configuration file is provided for provisioning students and staff, using the Student Information System as the authoritative data source. You can also customize the configuration.

In this section:

1.1 New Features

In this section:

1.1.1 Driver Features

- The Identity Manager Driver 1.5.0 for SIF conforms to SIF Implementation Specifications 1.1 and 1.5r1 and is certified by the SIF organization.
- The driver configuration provided has the following enhancements:
  - Receives information from multiple Zones using a single driver object. You can receive information from up to 10 Zones with one driver object.
  - Can send or receive user passwords. Sending passwords allows other SIF-enabled applications to use a common password provided by the Identity Vault. Receiving passwords allows another SIF-enabled application to be the authoritative source for passwords.
  - Manages both students and staff using a single driver object.
  - Allows configuration data to be edited more easily (such as school names and codes, and student groups), through the use of global configuration values (GCVs).
  - Provides more flexibility for creating the pattern for user IDs.

- Places user objects that have login disabled in a container you specify. For example, students whose login has been disabled because the student has withdrawn from school can be automatically placed in a Disabled container.

- The driver supports bidirectional data flow. This new feature allows for the following options:
  - You can specify that the Identity Vault is the authoritative source for some SIF attributes, meaning that changes made to those attributes in the Identity Vault are published to other SIF-enabled applications.
  - If your Student Information System is not SIF-enabled, you can use the Identity Manager Driver for SIF to provide student information to other SIF-enabled applications.
- The driver requires Identity Manager, which supports iManager as the management utility. ConsoleOne® is no longer supported.
- The driver now optionally supports the SIF EmployeePersonal object on the Publisher channel. You can provision Users provided by a SIF-enabled HR system. (EmployeePersonal objects cannot be sent from the Identity Vault to SIF.)
- Duplicate user IDs are resolved by appending a digit to the user ID, or you can configure e-mail notifications to inform administrators of the duplicate user ID.

1.1.2 Identity Manager Features

For information about the new features in Identity Manager, see "What's New in Identity Manager?" in the *Identity Manager 3.0.1 Installation Guide*.

1.2 About the Identity Manager Driver for SIF

Schools use many applications to organize data for a K-12 education environment, such as systems for student administration, network access, food services, and library automation. These diverse systems often contain duplicate information. If the applications do not communicate with each other to share information, school administrators and information technology personnel must deal with the challenges of manually provisioning students and using redundant data entry to keep the systems synchronized.

For example, when new students enroll at a school, they need network access and a home directory for their files. If the Student Information System (SIS) does not communicate with the Identity Vault, the network administrator must manually create a user account and assign network resources for each new student, one at a time. Without interoperability between the systems, each subsequent change to student data also requires manual intervention to keep the Identity Vault users updated.

To create interoperability between the Student Information System and the Identity Vault, Novell provides the Identity Manager Driver for Schools Interoperability Framework (SIF).

SIF is an open standard created to allow K-12 education applications to exchange data effectively. The Identity Manager Driver for SIF works as a SIF Agent. The 1.5 release of the driver conforms to SIF Implementation Specifications 1.1 and 1.5r1. For information about the specifications, see the Schools Interoperability Framework Web site (http://www.sifinfo.org).

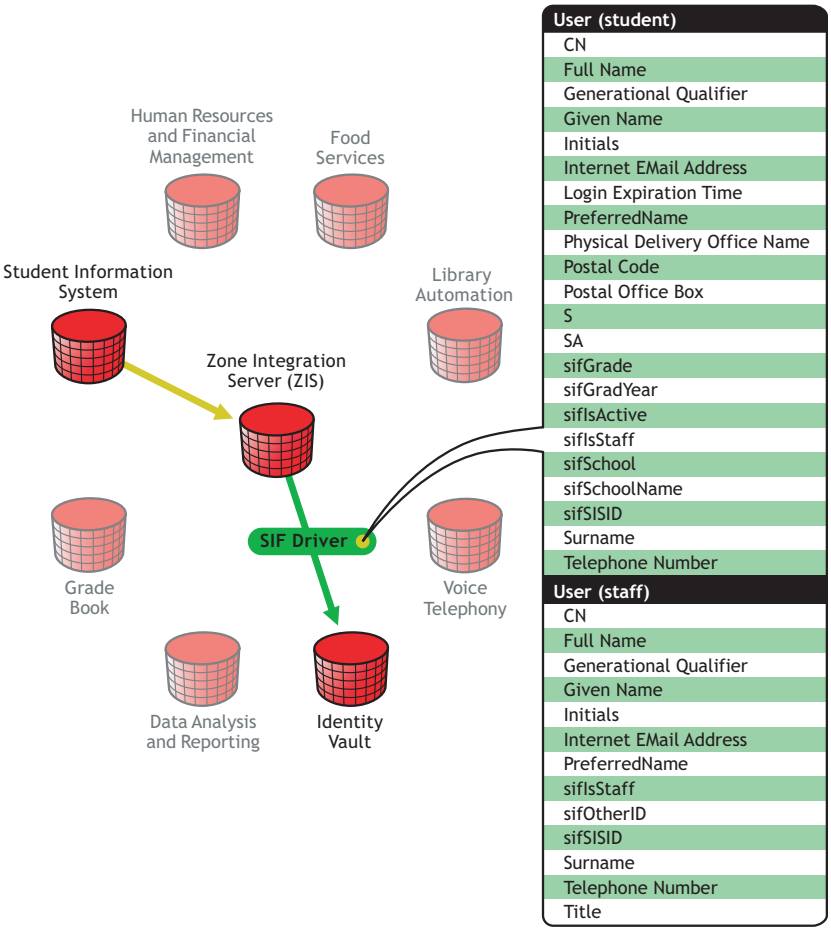
The driver eliminates the need to manually provision, change, or delete User objects for a school system in the Identity Vault. Instead, the changes in the Identity Vault are made automatically, mirroring the data from the Student Information System. When a student is entered in the Student Information System, he or she is automatically given a User object in the Identity Vault, in the correct container, with network resources. If the student's status changes, such as a grade-level

change or a move to a different school, the change is reflected in the Identity Vault and the User object is moved to a different container, if appropriate. If a student leaves the school system, the user object's login is disabled. The same kind of synchronization is done for staff and faculty users.

In a school network that uses the SIF standards, the Student Information System publishes information to the Zone Integration Server (ZIS).

The driver, like other SIF Agents, registers with the ZIS so it can receive information. The driver receives the StudentPersonal, StudentSchoolEnrollment, and SchoolInfo objects for students, and the StaffPersonal object for faculty and staff. The driver uses that information to create User objects for students and staff, give them appropriate attributes, and automatically place them in the correct container in the Identity Vault. This flow of information and the list of the attributes that are populated in the Identity Vault are shown in the following diagram.

Figure 1-1 *The Role of the Identity Manager Driver for SIF*



In the driver configuration provided, the Identity Vault receives information from the Student Information System. You can customize the configuration to change how students and staff are provisioned, and cause the Identity Vault to send information to the ZIS.

1.3 Understanding the Driver Configuration

After you install Identity Manager and the driver, you create a Driver object. A Driver object represents an instance of the Identity Manager Driver for SIF.

A driver configuration file, SIFAgent.xml, is provided to get you up and running with a minimum of customization. This section explains what the driver configuration does.

- "How the Identity Vault Is Updated When Data Changes in the Student Information System" on page 12
- "Data Mapping" on page 14
- "Sending Data from the Identity Vault to SIF" on page 15

For information about Identity Manager in general, see "Overview" in the *Identity Manager 3.0.1 Installation Guide*.

1.3.1 How the Identity Vault Is Updated When Data Changes in the Student Information System

The following tables describe what the configuration does to provision user accounts and keep the Identity Vault updated when changes occur in the Student Information System.

In this section:

- "Student Provisioning" on page 12
- "Staff Provisioning" on page 13

Student Provisioning

Change in Student Data	Synchronization in the Identity Vault
A student is added	◆ Creates an the Identity Vault User object with a unique user ID. ◆ Populates the User object attributes with data from the Student Information System. The attributes are listed in "Data Mapping" on page 14. ◆ Places the user in the correct container as determined by the student's school and grade level or graduation year. ◆ Uses a template (if you specify one) to set default properties for the user, group membership, login restrictions, and password restrictions. ◆ (NetWare® only) Creates a home directory in the file system. (You must use a template to specify this.)

Change in Student Data	Synchronization in the Identity Vault
A student's information is modified	◆ Modifies the Identity Vault User object attributes accordingly. The attributes are listed in "Data Mapping" on page 14. ◆ If appropriate, moves the User object to a different container in the tree. For example, a school or grade level/graduation year change could trigger moving the user to a different container. ◆ (Optional) If any of the attributes creates a User ID change, the user account is renamed. ◆ The home directory is not moved.
A student withdraws from school or graduates	◆ On the Exit Date, disables the login of the User object in the Identity Vault. ◆ (Optional) On the Exit Date, moves the user account to the Disabled directory. ◆ The home directory is not deleted.
A student returns to the school system (an Entry Date that is newer than the Exit Date is entered in the Student Information System)	◆ Enables the login of the User object in the Identity Vault. ◆ Moves the user account from the Disabled directory to the correct student container. ◆ The User object still has rights to the home directory.
A student is removed from the Student Information System	◆ On the Exit Date, disables the login of the User object in the Identity Vault. ◆ (Optional) Moves the user account to the Disabled directory. ◆ The home directory is not deleted.

Staff Provisioning

Change in Staff Data	Synchronization in the Identity Vault
Staff is added	◆ Creates an the Identity Vault User object with a unique User ID. ◆ Populates the User object attributes with data from the Student Information System. The attributes affected are listed in "Data Mapping" on page 14. ◆ Places the user in the correct container, as determined by the Zone. ◆ Uses a template (if you specify one) to set default properties for the user, including group membership, login restrictions, and password restrictions. ◆ (NetWare only) Creates a home directory in the file system. (You must use a template to specify this.)
Staff information is modified	◆ Modifies the Identity Vault user accordingly. The attributes maintained are listed in "Data Mapping" on page 14. ◆ (Optional) If any of the attributes creates a User ID change, the user account is renamed.

Change in Staff Data	Synchronization in the Identity Vault
Staff removed from the Student Information System	◆ Disables the User object in the Identity Vault. ◆ (Optional) Moves the user account to the Disabled directory. ◆ The home directory is not removed from the file system.

1.3.2 Data Mapping

The Identity Manager Driver for SIF uses data from the Student Information System to synchronize the following User class attributes in the Identity Vault:

eDirectory Attribute	SIF Object	SIF Attribute
CN	StudentPersonal or StaffPersonal	CN is formed from the combination of several SIF attributes.
Full Name	StudentPersonal or StaffPersonal	Name/FullName
Generational Qualifier	StudentPersonal or StaffPersonal	Name/Suffix
Given Name	StudentPersonal or StaffPersonal	Name/FirstName
Initials	StudentPersonal or StaffPersonal	Name/MiddleName
Internet EMail Address	StudentPersonal or StaffPersonal	Email
Login Expiration Time	StudentSchoolEntrollment	EntryDate and ExitDate When ExitDate is newer than EntryDate, the login is set to expire on the ExitDate. When the EntryDate is newer than the ExitDate, the expiration date is removed.
personalTitle	StudentPersonal or StaffPersonal	Name/Prefix
preferredName	StudentPersonal or StaffPersonal	Name/PreferredName
Physical Delivery Office Name	StudentPersonal or StaffPersonal	Address/City
Postal Code	StudentPersonal or StaffPersonal	Address/PostalCode
Postal Office Box	StudentPersonal or StaffPersonal	Address/Street/Line2
S	StudentPersonal or StaffPersonal	Address/StatePr

eDirectory Attribute	SIF Object	SIF Attribute
SA	StudentPersonal or StaffPersonal	Address/Street/Line1
Surname	StudentPersonal or StaffPersonal	Name/LastName
Telephone Number	StudentPersonal or StaffPersonal	PhoneNumber
Title	StaffPersonal	Name/Title
DirXML-sifGrade	StudentSchoolEnrollment	GradeLevel
DirXML-sifGradYear	StudentPersonal	GradYear
DirXML-sifIsStaff	StudentPersonal or StaffPersonal	Not set from a particular attribute. Set to True if the SIF object is StaffPersonal. Otherwise, it is set to False.
DirXML-sifSchool	SchoolInfo	IdentificationInfo
DirXML-sifSchoolName	SchoolInfo	SchoolName
DirXML-sifSISID	SchoolInfo	RefId
DirXML-sifSSEGUID	StudentSchoolEnrollment	RefId

1.3.3 Sending Data from the Identity Vault to SIF

The SIF Driver is generally used to provision users from a SIF-enabled Student Information System to the Identity Vault. The driver is configured, by default, to send no data from the Identity Vault to the Zone Integration Server (ZIS) and the Student Information System. The Student Information System is considered to be the authoritative data source.

However, the driver is capable of bidirectional synchronization and can send data to the ZIS and SIF. There are two ways you might choose to use this bidirectional capability:

- Configure the driver as the authoritative source for some user attributes or for new users.

  If you want the Identity Vault to be the authoritative source for some user attributes, you could configure the driver to send certain attributes from the Identity Vault to SIF.

  If your business practices allow users to be entered manually in the Identity Vault who are not entered in the Student Information System first, you could also configure the driver to send new users from the Identity Vault to SIF.

- Configure the driver to be the SIF provider for all student and staff data.

  If your Student Information System is not SIF-enabled, but you have other SIF-enabled applications, you might choose to configure the SIF Driver to function as the authoritative source for students and staff.

  In this role, the SIF Driver is the SIF provider for StudentPersonal, StudentSchoolEnrollment, SchoolInfo, StaffPersonal, and SIF Authorization objects. Being the provider means this driver responds when other SIF-enabled applications send SIF queries for information about students and staff.

For example, you could export student and staff information from your Student Information System and import it into the Identity Vault, using a database import. At the start of the school year, the other SIF Agents in the Zone would populate their databases by querying for all students. If you register the SIF Driver as the provider for the Zone, the queries would be routed to the SIF Driver. During the school year, as student and staff information in the Identity Vault is updated, either by database import or by updating manually, the SIF Driver would send those updates to SIF, thereby keeping the other SIF-enabled applications current.

You would not enable this option if you have a SIF-enabled Student Information System. Only one Agent in a Zone can be the provider. If you have a SIF-enabled Student Information System, we recommend that the Student Information System be the provider.

If you configure the Novell SIF Driver to send new users or to be the provider of all student and staff information, at a minimum you must provide the following user attributes when creating a user object in the Identity Vault. A new user object is not sent from the Identity Vault to SIF unless these attributes have values.

Type of User Account	Attribute
Student	Given Name
	Surname
	DirXML-sifGrade
	DirXML-sifGradYear
	DirXML-sifSchool
	DirXML-sifSISID
Staff	Given Name
	Surname
	DirXML-sifSISID

Planning

2

Installing Identity Manager and the driver is a simple process. However, you need to do some planning to make sure that you prepare your tree structure, know where to place your partition replicas and the driver, consider some of the choices you make when configuring the driver, and gather additional configuration information.

In this section:

2.1 Outlining Your Groups Of Students

Outlining the groups of students that you want the Identity Manager Driver for SIF to manage provides the following benefits:

- It helps you prepare for creating the tree structure you want to use for the containers that hold student users, described in the next section, Section 2.2, “Creating Your Tree Structure,” on page 19.
- It helps you configure the driver more quickly. In the driver configuration, you must specify each group of students, their location, and the Template object to use.

As a planning tool, we recommend that you create a table to represent the groups of students. This table will help you when you are configuring the driver, to make sure you have all the containers and templates you need.

When identifying the groups, use the identifiers used by your student information system for school code and for grade or graduation year. To configure the driver correctly, you need to know the codes your student information system uses.

You can choose to group students by grade level, graduation year, school, or in a single container. (Example tree structures are shown in “Creating Containers for Students” on page 19.)

For example, consider a school district named Alpine District, with one Zone and three schools: Canyon Elementary, Sunset Middle School, and Highland High School. To group the students by grade level, you would create a table like the one below.

School Code	Grade or Graduation Year	Container DN	Template DN
CElem	KG		

School Code	Grade or Graduation Year	Container DN	Template DN
	01		
	02		
	03		
	04		
	05		
	06		
SMiddle	07		
	08		
HHS	09		
	10		
	11		
	12		

After completing the planning section Section 2.2, “Creating Your Tree Structure,” on page 19, you would fill in the rest of the table with the container DN and template for each student group.

For example, if you were using one container per grade level, and decided to use one template per school with the templates placed in the Alpine container, your table would now look like this.

School Code	Grade or Graduation Year	Container DN	Template DN
CElem	KG	Alpine\District\Canyon Elem\K	Alpine\Elementary
	01	Alpine\District\Canyon Elem\01	Alpine\Elementary
	02	Alpine\District\Canyon Elem\02	Alpine\Elementary
	03	Alpine\District\Canyon Elem\03	Alpine\Elementary
	04	Alpine\District\Canyon Elem\04	Alpine\Elementary
	05	Alpine\District\Canyon Elem\05	Alpine\Elementary
	06	Alpine\District\Canyon Elem\06	Alpine\Elementary
SMiddle	07	Alpine\District\Sunset Middle\07	Alpine\Middle
	08	Alpine\District\Sunset Middle\08	Alpine\Middle
HHS	09	Alpine\District\Highland High\09	Alpine\HighSchool
	10	Alpine\District\Highland High\10	Alpine\HighSchool
	11	Alpine\District\Highland High\11	Alpine\HighSchool
	12	Alpine\District\Highland High\12	Alpine\HighSchool

Use the table as a reference when you configure the driver, as described in Section 5.1, “Creating and Configuring the Driver,” on page 39.

2.2 Creating Your Tree Structure

In this planning step, you review your tree and add or update the containers you want to use to hold student and users, add containers for incomplete or disabled user objects, and make sure you have the eDirectory™ template objects you need.

- “Creating the Hierarchy of Containers for Students and Staff” on page 19
- “Identifying “Incomplete” Containers” on page 23
- Section 2.2.4, “Identifying “Disabled” Containers (Optional),” on page 24
- “Identifying eDirectory Templates” on page 24

2.2.1 Creating the Hierarchy of Containers for Students and Staff

We recommend that your eDirectory tree have a hierarchal structure for holding User objects.

This part of the tree should begin at least one level down from the root container, so that the root container can contain the Admin user and other objects you don’t want the driver to manage. We recommend that students and staff be kept in separate eDirectory containers.

As part of your planning, you need to decide how you want to group your student users.

The container names don’t need to be identical to the school code or grade code used in the student information system.

In this section:

- “Creating Containers for Students” on page 19
- “Creating One or More Containers for Staff Users” on page 21

Creating Containers for Students

The tree structure can be created according to your needs; the only thing that’s required by the driver is that you specify which containers students and staff are placed in. In the examples in this manual, separate school containers are shown, and sometimes grade or graduation year containers as well, but this is not required.

One example tree structure would be to create a single district container below the root container. Below the district container you could create containers representing each school. Below each school container could be containers representing the grade levels or graduation years in the school.

Figure 2-1 illustrates this example hierarchy, with the District container, the Highland High school container, and the 12th grade container.

Figure 2-1 *Example Tree Structure, with Grade Level Containers*

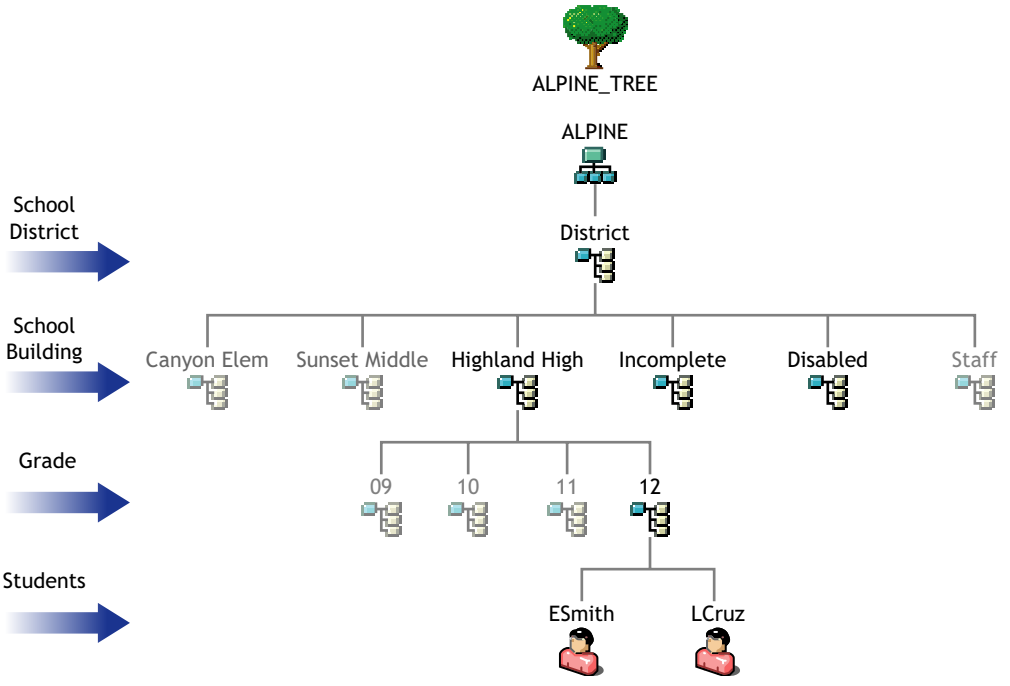
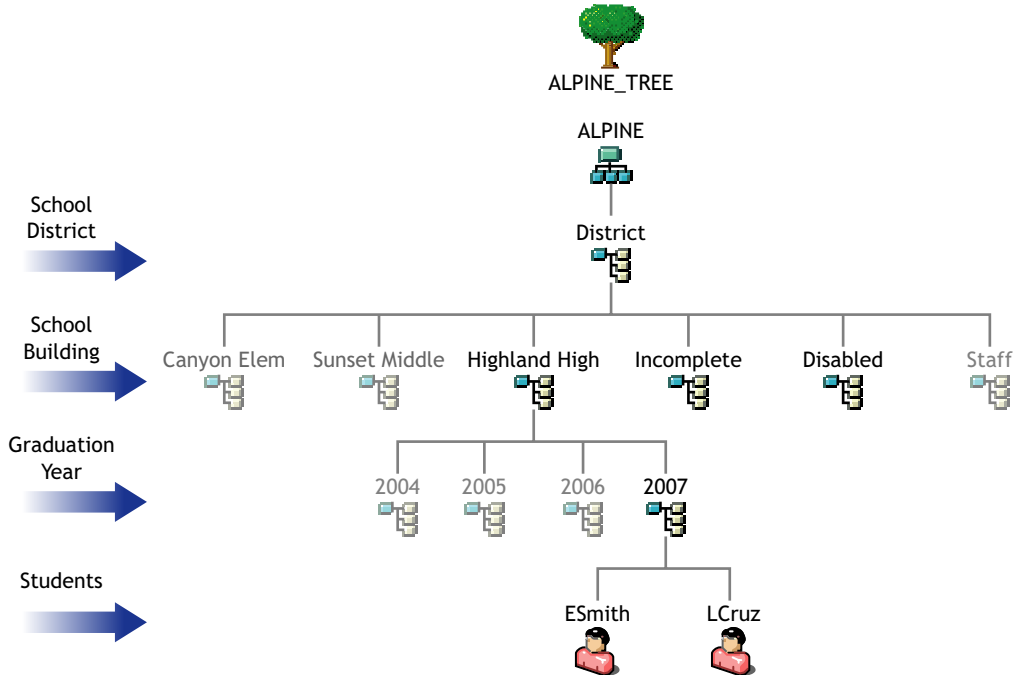


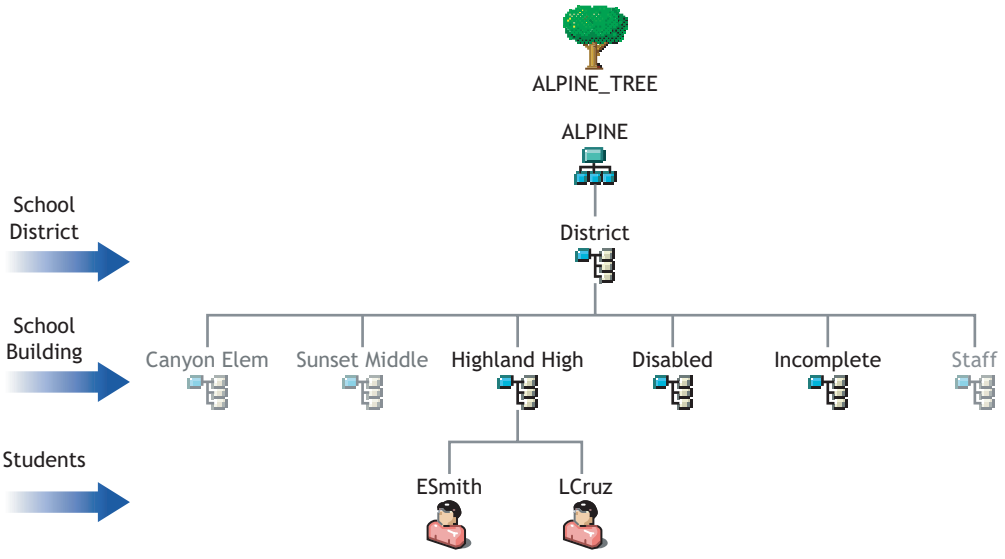
Figure 2-2 illustrates using the same kind of structure with graduation year containers instead of grade level containers.

Figure 2-2 *Example Tree Structure, with Graduation Year Containers*



Another way you could organize the tree is to eliminate the optional grade or graduation year level, and use only school containers, as shown in Figure 2-3.

Figure 2-3 *Example Tree Structure, without Grade Level Containers*



Creating One or More Containers for Staff Users

In this planning step, you review your tree and identify or create the container you want to use to hold staff users.

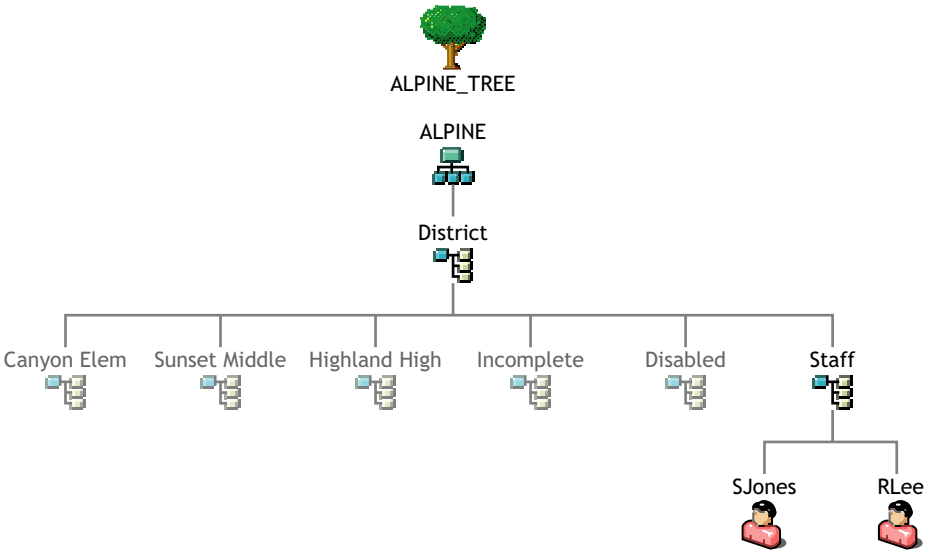
This container should be at least one level down from the root container, so that the root container can contain the Admin user and other objects you don't want the driver to change.

Each Zone that you configure specifies a Staff container.

For this part of your planning, it's helpful to know how many Zones you have, as discussed in Section 2.3, "Planning Driver and Replica Placement on Your Servers," on page 24.

If you have a single Zone, you could place your staff users in a container below the district-level container, as illustrated in the following figure.

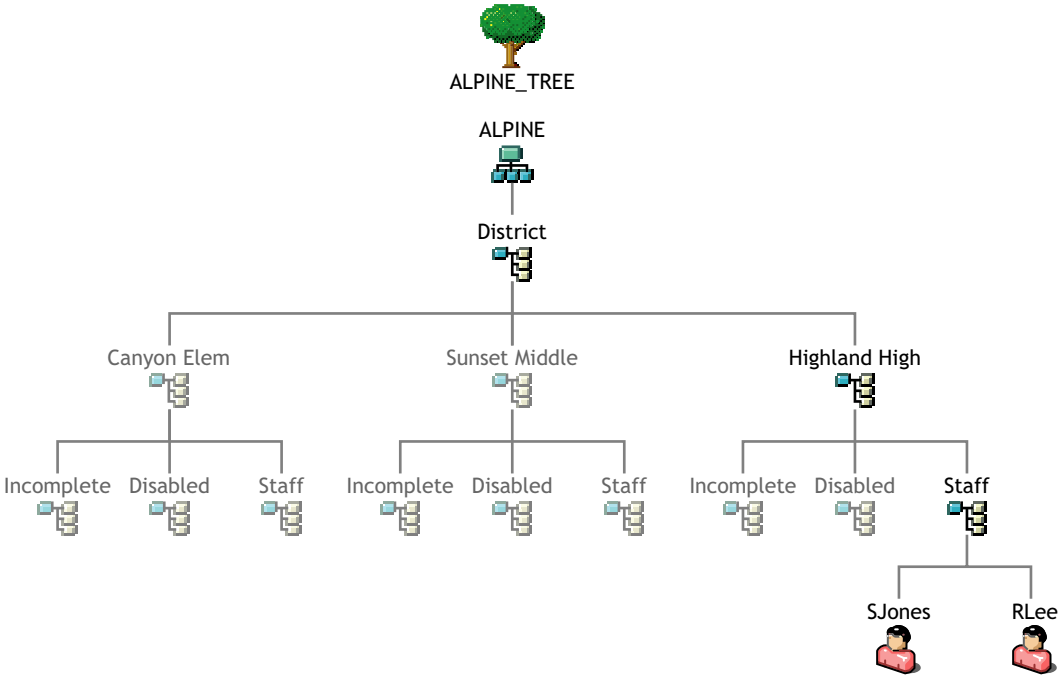
Figure 2-4 *Example Tree Structure for Staff for Single Zone*



If you have multiple zones, you have two choices for placing staff users:

- You could specify the same container for all your staff Driver objects, so all staff users are created in the same container regardless of which Zone they are represented in. This would be like the scenario illustrated in the previous figure.
- You could create one container for staff for each Zone, as illustrated in the following figure.

Figure 2-5 *Example Tree Structure for Staff for Multiple Zones*



2.2.2 Identifying “Incomplete” Containers

You need to identify a container to be used as the Incomplete container, so the driver has a place to hold information for students that it can’t place correctly in the tree. This container is needed when a student’s information is incomplete. If desired, you can specify an existing container to be used for this purpose instead of creating a new one.

If you have only one Zone, we recommend that you create one Incomplete container below the district container, as illustrated in Figure 2-6 on page 26.

If you have multiple Zones, we recommend that you create an Incomplete container below each school container, as illustrated in Figure 2-8 on page 28. This way, the users who are not yet placed correctly or who require administrator intervention are grouped by school.

Here are two examples of situations in which the driver would place students in the Incomplete container:

- A student has been entered into the student information system but the grade level or graduation year has not yet been entered.

  When the grade level or graduation year is entered into the student information system, Identity Manager automatically creates the user in the correct container, using the correct template.

- A student has a school and grade level for which no container has been specified in the rules, the container specified does not exist, or there is a syntax problem with a rule.

  For example, if the driver were set up for students in grades K-6 at Canyon Elementary, but the eDirectory administrator setting up the driver mistakenly left out a rule for the 5th grade, then Identity Manager would not know where to place students with the school of Canyon Elementary and the grade level of 05. Identity Manager would place them in the Incomplete container awaiting intervention by the eDirectory administrator.

  The administrator needs to fix the rules and then place the students in the right container using the right template. If no template is desired, the User objects could simply be manually moved to the correct container. If the User objects need to be created using a template, first the administrator needs to delete them from the Incomplete container. Then, they need to be re-created with the correct template in the correct container either manually or by using the Migrate into the Identity Vault command to cause the driver to re-create them. (See “Using Migrate into Identity Vault to Populate or Update the Identity Vault” on page 49.)

  You need to specify the DN of the Incomplete container when you configure the Driver object.

2.2.3 Identifying “Search” Container

The search container is the point in the Identity Vault below which User IDs must be unique. When creating a new User object, the driver searches the Identity Vault to verify that the new User ID is not already in use. The search container and all subcontainers are searched. Choose the district container or a container that is high enough in the tree that user IDs are unique for all students and staff. For example, for the environment shown in Figure 2-6, “Example Tree for One Zone, Showing Partitioning,” on page 26, you would specify the District container. A single search container is used for all zones.

If you specify Yes in the *Send New Users to SIF field,* only users created in this container and its subcontainers are sent to SIF.

2.2.4 Identifying “Disabled” Containers (Optional)

The driver configuration gives you the option to automatically move a student user to a different container if the user’s login is disabled. This option makes it easy for the administrator to identify all disabled accounts.

If you want to use this option, you must specify which container or containers you want the user objects to be placed in. If desired, you can use an existing container for this purpose instead of creating a new one.

If you have only one Zone, we recommend that you create one Disabled container below the district container, as illustrated in Figure 2-6 on page 26.

If you have multiple Zones, we recommend that you create a Disabled container below each school container, as illustrated in Figure 2-7 on page 27. This way, the users who have login disabled are grouped by school.

A student account is disabled when an exit date is set in the student information system. For example, this could happen when a student withdraws from school. If the student returns to school, a new entry date is set in the student information system. The student’s account is then enabled and moved to the appropriate student container.

2.2.5 Identifying eDirectory Templates

Decide which eDirectory User Template objects you want the Identity Manager Driver for SIF to use when creating new users. An eDirectory User Template object is not required for the driver, but it helps automate User object creation by allowing you to specify standard properties that can then be applied to new User objects.

For example, you might decide to have one Template object corresponding with each container where student users are grouped, such as one per school or grade, and a different Template object for staff users.

To prepare for configuring the driver, review the Template objects you have and update or add new ones if necessary. The Template objects that the driver needs access to must be on the server where the driver is running.

2.3 Planning Driver and Replica Placement on Your Servers

In this section:

2.3.1 Determining How Many Zones You Have

Consult with your student information systems administrator to find out how many Zones your environment is using and what they are managing.

Some SIF-enabled student information systems use one Zone for a whole district; some use multiple Zones, such as one per school.

A single instance of the Identity Manager Driver for SIF supports up to 10 Zones. If you have more than 10 Zones we recommend that you install Identity Manager and the SIF driver on more than one server. Each server with Identity Manager and the SIF Driver can service up to 10 Zones.

If you have multiple Zones, compare what the Zone manages to the containers in your eDirectory tree, to see which containers hold objects that are managed by each Zone.

For additional information about planning your containers for managing students, see "Creating the Hierarchy of Containers for Students and Staff" on page 19.

2.3.2 Planning Replica Placement

This information is based on "Replicating the Objects that Identity Manager Needs on the Server" in the *Identity Manager 3.0.1 Installation Guide*.

For each Driver object, the server where it runs must hold full master or read/write replicas of the following objects:

- The User objects that you want this instance of the driver to synchronize.

  The driver can't synchronize objects unless a replica of those objects is on the same server as the driver. This might necessitate some changes, for example, aggregating replicas onto a single server if the driver needs a tree-wide view of eDirectory data.

- The Driver Set object for that server.

  You should have one Driver Set object for each server that is running Identity Manager. Inside this Driver Set object is the Driver object that represents the driver that is running on that server. Unless you have specific needs, don't associate more than one server with the same Driver Set object.

- The Template objects you want the driver to use when creating users, if you choose to use templates.

  The driver does not require you to specify templates for use when creating users. But if you want the driver to use templates, the Template objects must be on the server where the driver is running.

- The Server object for that server.

  The Server object is necessary because it allows the driver to generate key pairs for objects. It also is important for Remote Loader authentication.

- Containers

  All containers specified in the configuration must be visible on the server, such as the Incomplete container and the Disabled container.

2.3.3 Examples of Driver and Replica Placement

In this section:

Example: Placing Drivers and Replicas for One Zone

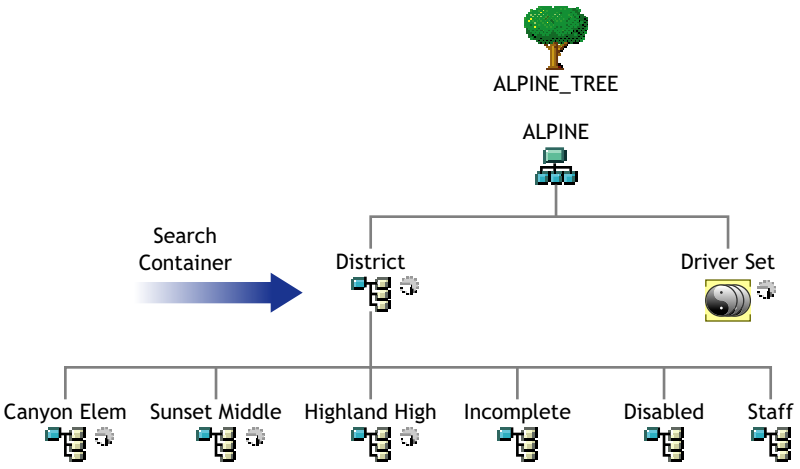
The following figures show an example of how to place the driver and partition replicas based on an example tree, for an environment with only one Zone that manages the whole district.

Figure 2-6 shows how the example tree is partitioned, and Figure 2-7 shows which replicas are needed on the server.

In this example tree, each school container is in a separate partition. The Driver Set object is also in a separate partition.

In this case, you should specify the District container as the search container. (In the driver configuration, you specify which container is the search container, meaning the container and subcontainers that should be searched to find out if there are duplicate User IDs.)

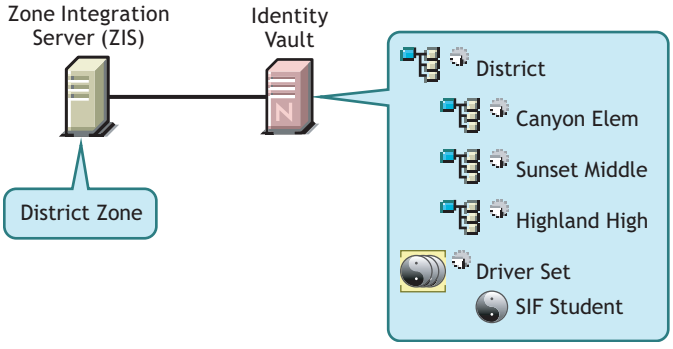
Figure 2-6 *Example Tree for One Zone, Showing Partitioning*



In this example, a single Identity Vault server is used for the district. Identity Manager and the driver software must be installed on the server so the server can run the driver.

The partitions that are needed on the Identity Vault server with the driver are shown in Figure 2-7.

Figure 2-7 *Partitions Containing Users Must Be Replicated on the Same Server as the Driver*



Example: Placing Drivers and Replicas for Multiple Zones

This section gives an example of how to place drivers and replicas on servers, based on an example tree, for an environment with multiple Zones. There are three Zones, one for each school.

Figure 2-8 shows how the example tree is partitioned, and Figure 2-9 shows that all replicas must be on the Identity Vault server.

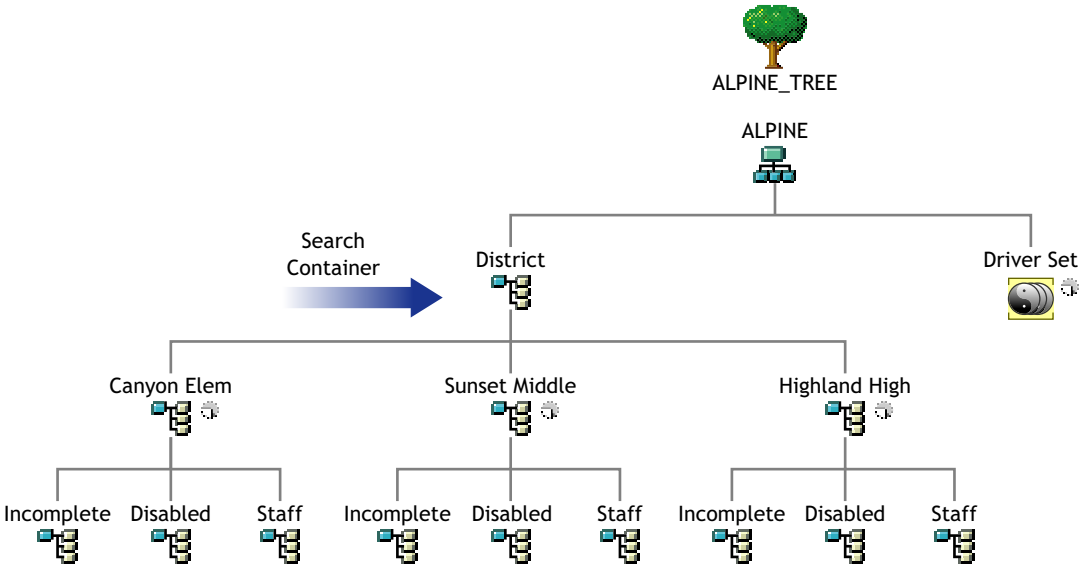
In this example tree, each school container is in a separate partition, as shown in Figure 2-8. The Driver Set object is also in a separate partition.

For this example, the District container is the search container. The search container should be high enough in the tree to include all students and staff.

In this example, each school contains its own Incomplete container and Disabled container.

NOTE: This is not required; you could use a single Incomplete container. However, we recommend this implementation for school systems with multiple Zones because it makes it easier to see which Zone needs attention if a student account is “stuck” in the Incomplete container, and because it reduces the number of partitions you might need on each server. If you use a single Incomplete container for all Zones, you need to keep a master or read/write replica of it on every server.

Figure 2-8 *Example Tree for Multiple Zones, Showing Partitioning*

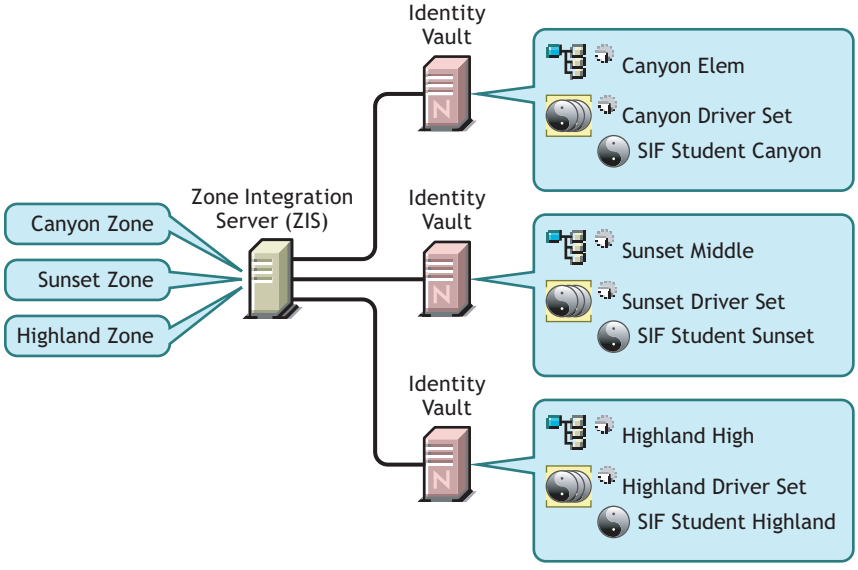


In this example there are three Zones, one per school. Identity Manager and the Identity Manager Driver for SIF are installed on a server that holds replicas of the partitions from each school. One driver is configured to connect to all three Zones.

NOTE: Unlike the example for a single Zone, in this example it's not necessary to replicate the District container on each server in order to get a replica of the Incomplete container, because separate Incomplete containers for each Zone are inside each individual school container.

Figure 2-9 illustrates the driver and the partitions that are replicated on the server.

Figure 2-9 *Multiple Zones*



2.4 Specifying the Pattern for User IDs

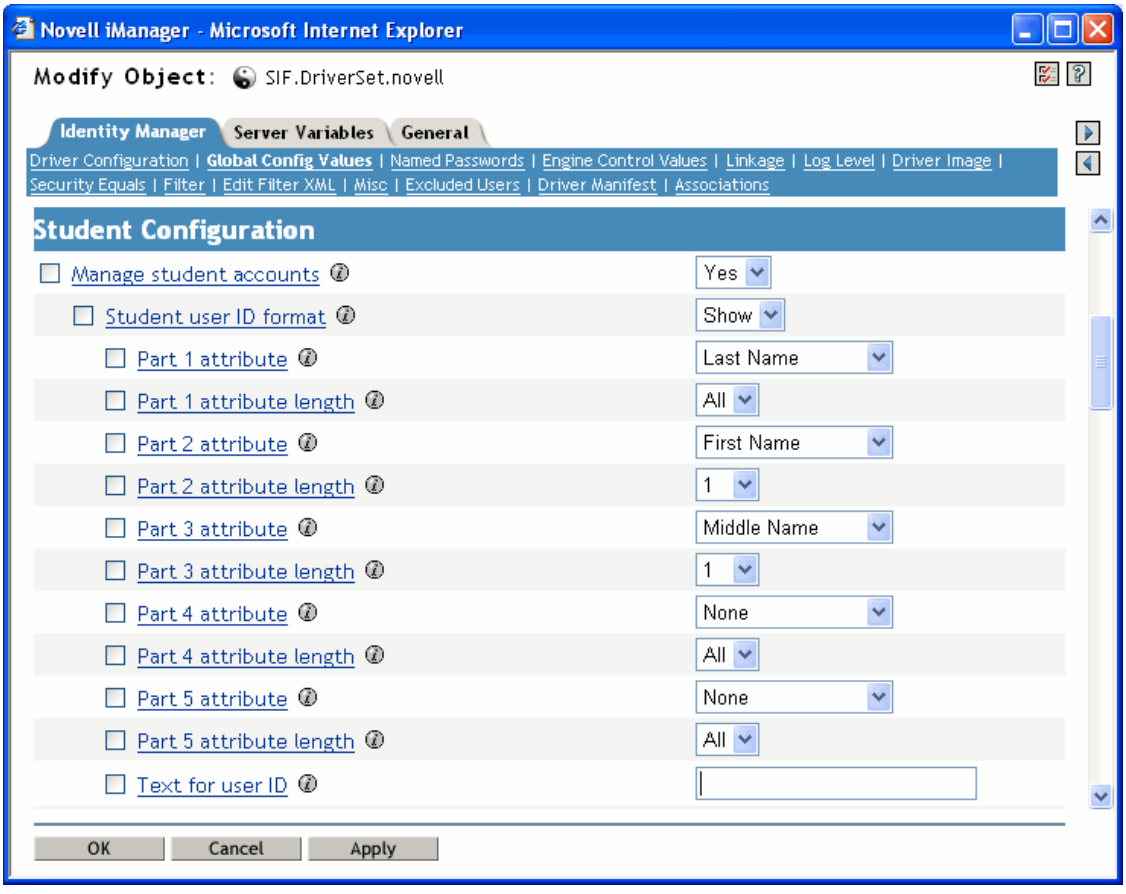
Using Identity Manager for provisioning ensures that eDirectory User IDs follow a consistent pattern, and it eliminates human error in creating User IDs. Consistently following a good pattern reduces support time because you don't need to go in to the Identity Vault to look up User IDs; instead, the student can predict the ID by knowing the pattern (such as last name, first initial, and student ID) and applying it to his or her own information.

You need to plan the pattern you want the driver to follow when creating an eDirectory User ID.

The driver configuration gives you a lot of flexibility in specifying the pattern for creating User IDs. You specify one pattern for student User IDs and a separate pattern for creating staff User IDs. You can create User IDs that are a combination of up to 5 parts.

The following figure shows an example of the options that are provided for User IDs in the driver configuration.

Figure 2-10 *Five Parts You Can Use to Create a Pattern for User IDs*



You can use the following attributes from the student information system:

- Last Name
- First Name
- Middle Name

- Student ID number

  TIP: Formats that include part of the student ID number are more likely to produce unique User IDs.

- Graduation Year

In addition to using attributes, you also have the option to specify one of the following values:

- Text

  You could incorporate a text string you specify. The text field where you enter the string is the last field shown in the figure above.

- None

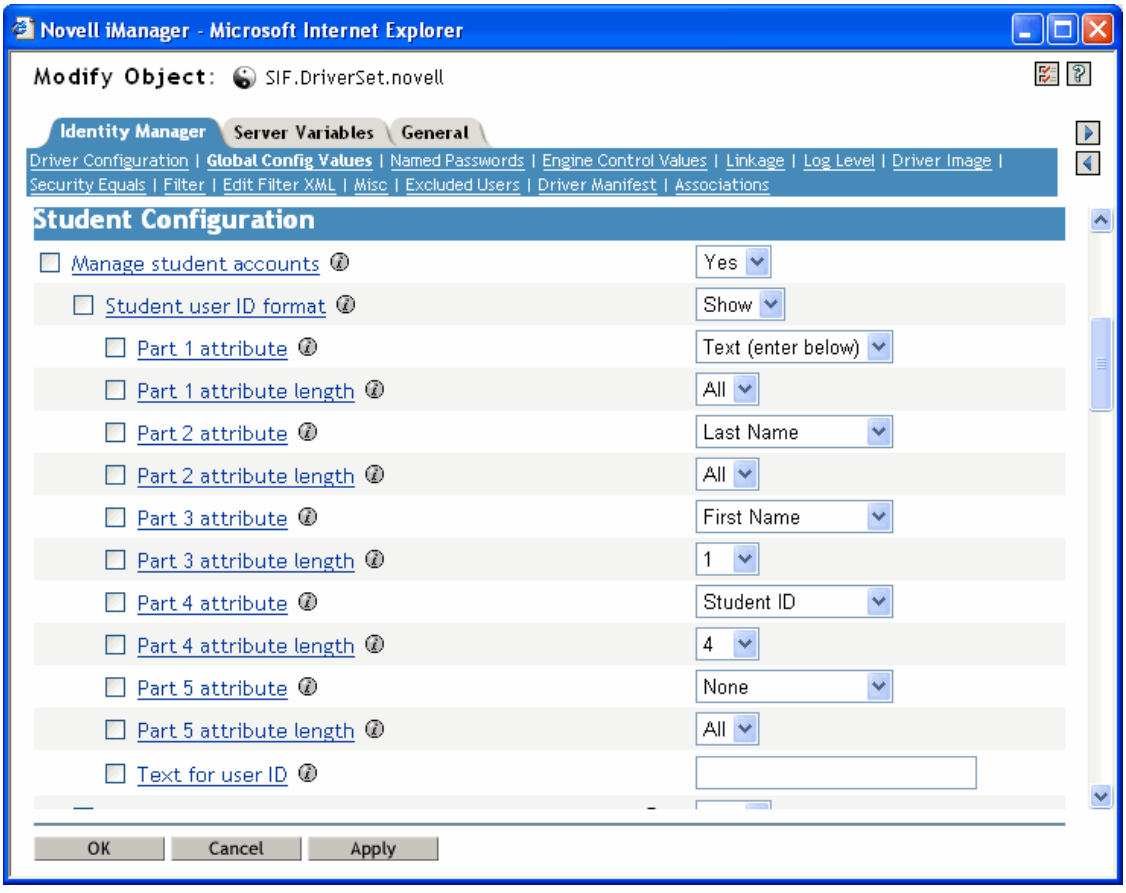
  Using this option for one of the parts of the User ID indicates that the part has no value and is not being used. For example, if you wanted the User ID to be made up of only three parts, you could specify None as the value for parts 4 and 5.

For each part, you specify a length. The length indicates the number of characters or digits to use from the attribute. For Last Name, First Name, Middle Name, and Text, the left-most characters are used. For Student ID and Graduation Year, the right-most digits are used.

Example

In this figure showing the User ID section of the driver configuration, the administrator has chosen to use 4 parts for the User ID. Because the 5th part is not needed, it is set to None.

Figure 2-11 *Sample User ID Pattern*



The table below represents the same choices, and what the resulting parts of the User ID would be for an example user, Michelle Jones. For this example, the resulting User ID would be "S-JonesM3842."

Part	Value Specified	Length Specified	Attribute Value	Resultant Value
1	Text	All	S-	S-
2	Last Name	All	Jones	Jones
3	First Name	1	Michelle	M
4	Student ID	4	7683842	3842
5	None	All		

2.5 Deciding Whether You Want the Driver to Manage Existing User Accounts

During your planning, decide whether you want the driver to manage existing Identity Vault user accounts. This decision lets you know whether to specify Yes or No for the Manage Existing eDirectory Users field when configuring the driver. This field is on the Global Config Variables page for the driver.

The driver gives you the following options for how to handle existing accounts. You can choose one to start with, and later switch to another option as needed.

- **Yes.** Use this option if you have one of the following scenarios:
  - The Identity Vault has no users, and you want to populate the Identity Vault by migrating all students from the student information system into the Identity Vault.
  - You want to remove all existing users in the Identity Vault and home directories, then populate the Identity Vault by migrating all students from the student information system into the Identity Vault.
  - You want to manage all existing Identity Vault User objects and new students, without deleting any existing user accounts.

    Add the student ID from the student information system to the DirXML-sifSISID attribute for existing accounts in the Identity Vault, so the driver can manage them.
- **No.** Use this option if you don't want to manage existing Identity Vault users; you want to use the driver only to provision new students.

For more information on these options, the reasons why you might choose them, and how to set them up, see Section 5.4, "Synchronizing the Identity Vault the First Time," on page 46.

2.6 Password Synchronization

The SIF driver can synchronize passwords between the Identity Vault and the Zone if the SIF driver and the Zone are using SIF Specification 1.5r1 or later. In order to properly synchronize passwords with the Identity Vault, you must be familiar with "Password Synchronization across Connected Systems"in *Novell Identity Manager 3.0.1 Administration Guide*. There are two prompts in the SIF driver's Global Configuration Variables (GCVs) that control password sharing with SIF. Set these two prompts to True if you want to synchronize or share passwords.

- SIF Driver sends user passwords to the Zone

  If set to True, the SIF driver sends user passwords in the Identity Vault to the Zone. Passwords are sent as SIF Authorization objects. Other SIF-enabled applications can subscribe to the Zone to receive the passwords.

  You would set this parameter to True when other SIF-enabled applications want to use the user's network password. When a Distribution Password is set for a new user or when a Distribution Password is changed in the Identity Vault, the Novell SIF driver sends a SIF Authorization object containing the password to the Zone.
- SIF Driver accepts user passwords from the Zone

  If set to True, the SIF Driver sets user passwords in the Identity Vault to the passwords received from the Zone. The passwords are received as SIF Authorization objects. The passwords are published to the Zone by other SIF-enabled applications.

You would set this parameter to True if you want the network password to be generated by another SIF-enabled application. For example, you have a SIF-enabled application in the Zone that generates a password for each user. When the Novell SIF driver receives the password in a SIF Authorization object, the corresponding user's the Identity Vault password is set to this value.

If this parameter is set to True, we recommend that the Novell SIF driver also be configured to set an initial password for each new user. There might be a delay between the creation of the user account and when the password is received, and it is best to make sure the account is protected by a password at all times.

2.7 Gathering Information for the Driver Configuration

After you create a Driver object with the SIFAgent.xml configuration, you need to configure driver settings on the Global Configuration Values page.

As part of your planning, review the table in Section 5.1, "Creating and Configuring the Driver," on page 39, which lists the settings in the driver configuration that you need to complete.

In the previous planning sections, you have already gathered some of the information you need.

Upgrading the Driver

3

If you have been using a previous version of the driver, follow these instructions instead of the ones in Chapter 4, “Installing the Driver,” on page 37.

The Identity Manager 3.0.1 engine is backward compatible with the Identity Manager 2.0.1 and DirXML 1.1a SIF driver shim and driver configuration. We recommend that you upgrade Identity Manager and the SIF driver at the same time. The SIF driver and configuration are tightly coupled. Both must be used together.

1. Review and record the Driver Parameters for the existing Driver object so you can use the same settings when configuring the new driver.

   Review and record the Global Config Values for the existing driver so you can use the same setting when configuring the new driver.
2. Stop your existing SIF driver as explained in “Starting, Stopping, or Restarting a Driver”in the *Novell Identity Manager 3.0.1 Administration Guide*.
3. Set the driver Startup Option to *Manual*.
4. As a backup, export the existing driver configuration to a file.
5. Upgrade to Identity Manager, as described in the “Upgrading” section in the *Identity Manager 3.0.1 Installation Guide*.
6. Install the driver shim for the Identity Manager Driver for SIF 1.5.
7. Import the new sample driver configuration onto your existing driver using the Import Driver Wizard in iManager.

   IMPORTANT: It’s important to import the configuration onto your existing driver object, to preserve associations.

   ---
8. Configure the driver using the *Global Config Values* page, as explained in Section 5.1, “Creating and Configuring the Driver,” on page 39.

   Refer to the values you were using for the driver previously, as noted in Step 1.
9. Test the driver.

   For testing, specify the *Poll rate in seconds* field to a short period, such as 15 seconds.
10. In the driver properties, set the driver Startup Option to *Auto start*, and set the *Poll rate in seconds* to 900 seconds (default value).

Installing the Driver

4

If you are upgrading from a previous version of the SIF driver, follow the instructions in Chapter 3, “Upgrading the Driver,” on page 35.

This section gives the prerequisites and the steps for a new installation of the driver.

After completing these tasks, follow the instructions in Chapter 5, “Deploying the Driver,” on page 39 to create and test a Driver object.

4.1 Prerequisites

This section lists the software and hardware requirements you must meet to run the driver.

4.1.1 Software Requirements

- ❑ Identity Manager with the latest patches and product updates

  For patches and product updates for Novell® products, see Product Updates (http://support.novell.com/filefinder/5069/index.html).

- ❑ The software requirements for Identity Manager listed, in the “ Installing Identity Manager” section found in the *Identity Manager 3.0.1 Installation Guide*.

- ❑ A Zone Integration Server and student information environment that complies with SIF standard 1.1 or 1.5r1.

  NOTE: If necessary, the driver can be used with a Student Information System that is not SIF-enabled, as described in “Sending Data from the Identity Vault to SIF” on page 15.

- ❑ One of the following server operating systems:
  - Novell NetWare® 6 or 6.5 with the latest Support Pack (you must obtain and install JVM 1.4.2 on NetWare)
  - Windows NT*, 2000, or 2003 with the latest Service Pack

  The Identity Manager Driver for SIF supports only English versions of NetWare and Windows.

- ❑ One of the following eDirectory™ versions:
  - eDirectory 8.7.3 with the latest Support Pack
  - eDirectory 8.8

4.1.2 Hardware Considerations

- Identity Manager and the Identity Manager Driver for SIF use approximately 5% of the system's memory and CPU for each Zone they connect to.
- An Identity Manager-dedicated NetWare system with a 1 gHz processor and 1 GB memory can support connecting to 10 Zones.
- In production, the driver's poll rate should be set at 900 seconds or higher.

4.2 Installing the Identity Manager Driver for SIF

Installing Identity Manager and the driver software is a simple process.

For a new installation, install Identity Manager and the SIF driver shim on either NetWare or Windows, as described in the " Installing Identity Manager" section found in the *Identity Manager 3.0.1 Installation Guide*.

If you are upgrading from a previous version of Identity Manager and the SIF driver, see "Upgrading the Driver" on page 35.

NOTE: Install Identity Manager and the SIF driver shim only once per server, even if a server is running multiple instances of the driver. Multiple instances of the driver are not necessary unless you have more than 10 Zones.

Keep in mind that installing the driver software lets you get the driver up and running, but it does not install the product license. Without the license and activation, the driver will not run after 90 days.

4.3 What's Next

To begin using the driver, create a new Driver object, as explained in Chapter 5, "Deploying the Driver," on page 39.

4.4 Activating the Driver

For activation information, refer to "Activating Novell Identity Manager Products"in the *Identity Manager 3.0.1 Installation Guide*.

Deploying the Driver

5

You can use the Identity Manager Driver for SIF to manage Identity Vault accounts for students, staff, and faculty. This automation allows new users to have network access and a home directory right away, without manual intervention by the Identity Vault administrator. When changes occur to student, staff, and faculty information, the Identity Vault is automatically updated.

This section contains the information you need to set up the driver object and configure it, after it is installed (as explained in Chapter 4, "Installing the Driver," on page 37).

After you complete these tasks, decide how you want to synchronize student data from the Student Information System into the Identity Vault.

5.1 Creating and Configuring the Driver

The Identity Manager Driver for SIF comes with a driver configuration file named SIFAgent.xml.

You use a wizard to create a new Driver object based on this configuration file. When you import the configuration file to create or upgrade a driver object, only a few prompts are presented. Most of the driver configuration is done after you import, on the Global Configuration Values page for the driver.

Prerequisites

- ❑ You have installed Identity Manager and the Identity Manager Driver for SIF on the Identity Vault server, and installed the Identity Manager plug-ins and the driver configuration files on the iManager Web server, as explained in Section 4.2, "Installing the Identity Manager Driver for SIF," on page 38.
- ❑ You restarted NetWare® (for a NetWare server) or eDirectory™ (for a Windows server) after installing the driver.
- ❑ You have followed the instructions in "Planning" on page 17 to complete the following tasks:
  - Identify or create the Identity Vault objects you need: the necessary containers for your students and staff, the Incomplete and Disabled containers, and the Template objects.

    In the driver configuration, you need to specify the DN for these objects.
  - Gather the other information you need for setting up the driver configuration Section 2.7, "Gathering Information for the Driver Configuration," on page 33.

Importing the Driver Configuration File in Designer

Designer allows you to import the basic driver configuration file for SIF. This file creates and configures the objects and policies needed to make the driver work properly. The following instructions explain how to create the driver and import the driver's configuration.

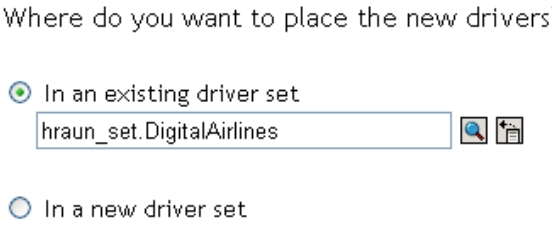
There are many different ways of importing the driver configuration file. This procedure only documents one way.

1. Open a project in Designer and in the modeler, right-click on the Driver Set object and select *Add Connected Application*.
2. From the drop-down list, select *SIFAgent.xml*, then click *Run*.
3. Click *Yes*, in the Perform Prompt Validation window. It has you fill in all of the fields to correctly configure the SIF driver.
4. Configure the driver by filling in the fields. Specify information specific to your environment. For information on the settings, see Table 5-1 on page 41 for more information.
5. After specifying parameters, click *OK* to import the driver.
6. After the driver is imported, customize and test the driver.
7. Once the driver is fully tested, deploy the driver into the Identity Vault. See "Deploying a Driver to an Identity Vault" in the *Designer for Identity Manager 3: Administration Guide*.

Importing the Driver Configuration File in iManager

The Active Directory preconfiguration file is an example configuration file. You installed this file when you installed the Identity Manager Web components on an iManager server. Think of the preconfiguration file as a template that you import and customize or configure for your environment.

1. In iManager, select *Identity Manager Utilities* > *Import Drivers*.
2. Select a driver set, then click *Next*.



If you place this driver in a new driver set, you must specify a driver set name, context, and associated server.

3. Select the *SIF* driver, then click *Next*.

4. Configure the driver by filling in the configuration parameters. For information on the settings, see Table 5-1 on page 41.

5 Define security equivalences using a user object that has the rights that the driver needs to have on the server

   The tendency is to use the Admin user object for this task. However, you might want to create a DriversUser (for example) and assign security equivalence to that user. Whatever rights that the driver needs to have on the server, the DriversUser object must have the same security rights.

6 Identify all objects that represent administrative roles and exclude them from replication.

   Exclude the security-equivalence object (for example, DriversUser) that you specified in Step 2. If you delete the security-equivalence object, you have removed the rights from the driver. Therefore, the driver can't make changes to Identity Manager.

7 Click Finish.

Configuration Parameters

The following table explains the parameters you must provide during initial driver configuration.

Table 5-1 *Configuration Parameters for the SIF Driver*

Field Name	Description
Driver name	Specify the name you want to use for the driver object in the Identity Vault.
Sif Agent Name	Specify the name this driver uses to register as a SIF Agent with the Zone Integration Server (ZIS). The driver must have a Zone-unique, case-sensitive name. We recommend that you use the default name, Novell Identity Manager. You need to coordinate with the ZIS administrator to make sure that the same name is used when configuring the ZIS, as described in "Configuring the ZIS to Recognize the Driver" on page 43.
Sif Specification version	Specify the SIF Specification version you want this driver to use, either SIF Specification 1.1, or SIF Specification 1.5r1.

Field Name	Description
Manage preexisting eDirectory users	The SIF Driver can match students and staff in the Student Information System (SIS) with preexisting Identity Vault users only if the eDirectory user attribute DirXML-sifSISID contains the student's or staff's ID number. Specify *Yes* if one of the following is true: ◆ You want to manage preexisting Identity Vault users, and the DirXML-sifSISID is set on all users. ◆ No users currently exist in the Identity Vault. Otherwise, specify *No*. If Yes is specified, the *Migrate into Identity Vault* command can be used to add or update all SIF users into the Identity Vault. If No is specified, the *Migrate into Identity Vault* command is ignored to prevent duplicate users from being created in the Identity Vault. This field does not apply to users added to the Identity Vault by this driver. Identity Manager can always match these Identity Vault users with Student Information System users, and these Identity Vault users are always kept current with changes from the Student Information System. For more information on how to make this decision, see Section 5.4, "Synchronizing the Identity Vault the First Time," on page 46.
Driver is Local/ Remote	Specify whether to run the driver locally or using Remote Loader. If you specify *Remote*, and click Next, another page presents a few more items for you to specify regarding Remote Loader configuration. For information about running the driver remotely, see "Setting Up Remote Loaders"in the *Novell Identity Manager 3.0.1 Administration Guide*.

Post Configuration Tasks

1. After you create the Driver object, configure settings such as the containers to use for students and staff.
   - **1a** In iManager, click *Identity Manager > Identity Manager Overview*. Search for and select the driver set.
   - **1b** Browse to and click the driver icon, then in the next page, click the driver icon again.
2. Click the *Global Config Values* tab, then specify the following settings. Some of them were specified when creating the driver object; for those items you can simply review the settings to make sure they are correct. See Appendix B, "Global Configuration Values," on page 69 for a detailed list of all of the fields.
3. Follow the instructions in Section 5.2, "Preparing the ZIS and the Student Information System," on page 43 to configure the ZIS to recognize the driver as a SIF Agent.

5.2 Preparing the ZIS and the Student Information System

The Zone Integration Server (ZIS) must be configured to recognize the driver as a SIF Agent, just as you would do for other SIF Agents. The driver works with data from the Student Information System without changes to the Student Information System, but you can optimize the data if desired.

You can complete these steps either before or after you create a Driver object in the Identity Vault for the Identity Manager Driver for SIF, but you must complete them for the driver to receive information.

5.2.1 Configuring the ZIS to Recognize the Driver

The Zone Integration Server (ZIS) must be configured to recognize the Novell Identity Manager Driver for SIF as a SIF Agent. The driver can't receive any information about students or staff until this has been done.

The ZIS administrator should configure the ZIS to recognize the driver by doing the following tasks. Refer to your ZIS documentation for instructions.

- Specify the SIF Agent name for the driver, such as Novell Identity Manager.

  This is the name the driver uses to register with the ZIS. It must be the same name you specify in the *SIF Agent Name* field when you create the Driver object, as described in Section 5.1, "Creating and Configuring the Driver," on page 39.

  The default name is Novell Identity Manager. If you want to use a different name, keep in mind that it must be unique within each Zone, and it is case sensitive.
- Specify the SIF objects the driver has access to:
  - StudentPersonal
  - StudentSchoolEnrollment
  - SchoolInfo
  - StaffPersonal
  - EmployeePersonal
  - Authorization

  For these SIF objects, the driver should have Add, Change, Delete, Subscribe, and Request rights.

  If the driver is also the SIF Provider, it should have Publish and Response rights.
- Specify that the driver is a pull agent.
- Give the driver permission to request the ZoneStatus object.
- Set up security, if desired. This is explained in Section 6.2, "Setting Up Security," on page 56.

5.2.2 Optimizing Data in the Student Information System

The Identity Manager Driver for SIF is designed to work as a SIF Agent without requiring any change in the Student Information System, but there is one aspect of the Student Information System that can be optimized.

According to the SIF implementation specification, the StudentPersonal object provides the student's name, the StudentSchoolEnrollment object provides the grade, and the SchoolInfo object provides the school code. However, some Student Information Systems can be configured to also provide school and grade information with the StudentPersonal object, in the OtherID attribute.

Student placement is done most efficiently when the Student Information System provides the school and grade to the driver using the OtherId attribute of the StudentPersonal object. If possible, have the Student Information System administrator configure it this way.

No corresponding change to the driver configuration is necessary. These values are handled in the Input Transformation, which is configured to accept the school and grade information from either the StudentSchoolEnrollment object or the OtherID attribute.

5.3 Starting and Testing the Driver

After creating the Driver object and completing the rules for placing groups of students, you can start the driver and test it.

The default polling rate on a new Driver object is 900 seconds. This is appropriate for a production environment, but you should make it shorter for testing purposes.

Prerequisites

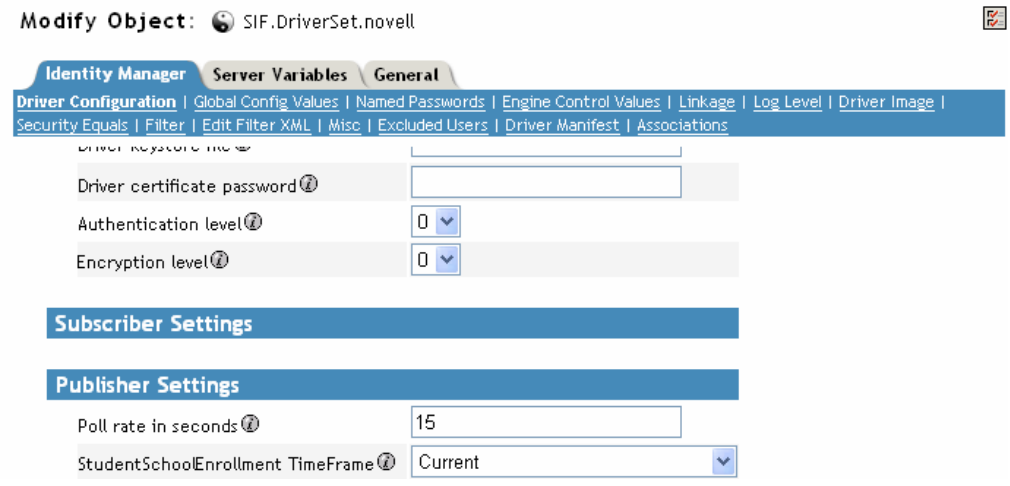
- ❑ You have configured the ZIS to recognize the driver as a SIF Agent, as described in "Configuring the ZIS to Recognize the Driver" on page 43.

  If you don't complete this step, you will get errors in the status log when you start the driver.
- ❑ If you have existing users in the Identity Vault, and the *Manage preexisting eDirectory users* parameter for the driver is set to *Yes*, review your options before starting the driver to avoid duplicate users being created. See Section 5.4, "Synchronizing the Identity Vault the First Time," on page 46. If you select *Yes* for *Manage preexisting eDirectory users*, you should follow the steps given and fill in the DirXML-sifSISID attribute for existing user objects before starting the driver.

Procedure

1. For testing purposes, set the polling rate for the Driver object to 15 seconds.
   - **1a** In iManager, click *Identity Manager >Identity Manager Overview*. Search for the driver set.
   - **1b** In the driver set, click the icon for the driver. On the Identity Manager Driver Overview page that appears, click the driver icon again.
   - **1c** Click the *Identity Manager* tab, then click *Driver Configuration*. On the Driver Configuration page, find the *Publisher Settings* and *Poll rate in seconds*.

1d Change the poll rate to 15 seconds, then click *OK*.



2 Set the startup option for the driver. On the same Driver Configuration page, scroll to *Startup Option*. Select how you want the driver to be started, then click *OK*.

3 Start the driver. On the Identity Manager Driver Overview page, click the icon in the upper-right corner of the driver icon, then click *Start Driver*.

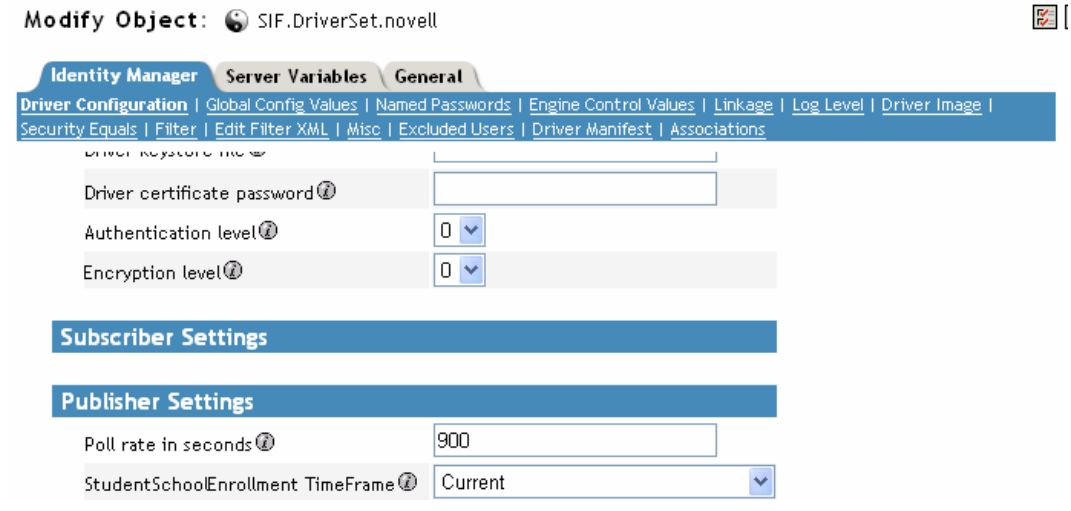
4 Check for errors.

If you see errors you need to fix, you might want to clear the log before you make changes so you can see which errors are new.

See Section A.1, “Viewing Status Messages for the Identity Manager Driver for SIF,” on page 61 and Section A.2, “Error Messages,” on page 62.

Disregard the error message “No object name provided.” It does not indicate a problem.

5 After you test the driver, set the polling rate to a longer period that’s appropriate for your environment, such as 900 seconds.



5.4 Synchronizing the Identity Vault the First Time

After you have imported the driver and tested it, you need to decide how to handle synchronizing the Identity Vault user accounts with user data in the Student Information System the first time.

When you configure the driver, you specify either *Yes* or *No* for the *Manage preexisting eDirectory users* field as described in Section 5.1, "Creating and Configuring the Driver," on page 39. This setting determines whether the driver tries to synchronize existing users in the Identity Vault, or ignores them and only manages new students and staff. You specify this setting on the Global ConfigValues page for the driver.

The Identity Manager Driver for SIF gives you three options for synchronizing existing accounts. Regardless of which option you choose for existing accounts, the driver provisions and manages any new accounts entered into the Student Information System in the future.

This section describes the three options, the reasons why you might choose one, and how to set them up.

To help you set up these options, this section also provides instructions for the following task:

5.4.1 Option 1: Populate the Identity Vault Using Migrate into Identity Vault

For this option, you remove all existing accounts and home directories, and re-create them "from scratch" using the *Migrate into Identity Vault* command to populate the Identity Vault.

Why Would You Use This Option?

- You want the driver to manage all accounts.
- You have decided you want to "start from scratch" by removing existing users from the Identity Vault, or you have not yet put any users into the Identity Vault.
- You don't need to preserve the files that are currently in the home directories.

For example, if you were implementing the driver before the beginning of the school year, and you didn't need to keep home directories from the previous year, you could get a fresh start in the Identity Vault using this option.

How To Set It Up

1. Remove existing user accounts (User objects) from the Identity Vault.
2. Remove the home directories from the server.

   IMPORTANT: If existing home directories are not deleted along with existing user accounts, the users who are migrated won't have a home directory. Identity Manager must create the

home directory at the same time it creates a user. It can't grant the newly created user rights to an existing home directory; instead, it gives an error.

If you had existing user accounts with home directories and you didn't delete them before using Migrate into Identity Vault, you need to delete them and repeat the migration.

3 *Set Manage preexisting eDirectory users* to *Yes*.

You set this on the Global Config Values page for the driver.

4 Populate the Identity Vault by using the *Migrate into Identity Vault* command to request all user data from the Student Information System.

See "Using Migrate into Identity Vault to Populate or Update the Identity Vault" on page 49.

NOTE: You should use *Migrate into Identity Vault* when demand for the server is low, such as on a weekend. If you have more than one Zone configured, we recommend you perform the migration one Zone at a time. The migration can take approximately 20 seconds per user and places a load on the server.

Identity Manager creates all students and staff in the Student Information System as User objects in the Identity Vault. As they are created, the objects are automatically associated with the ID in the Student Information System, so Identity Manager can manage them.

5.4.2 Option 2: Manage Existing Identity Vault User Accounts

For this option, you leave existing accounts in the Identity Vault. You manually put the student or staff ID from the Student Information System into the DirXML-sifSISID attribute of each existing Identity Vault user object, so the driver can match it with the corresponding individual in the Student Information System. After you put in the Student Information System ID, the driver can manage existing user accounts, so any new changes to those individuals in the Student Information System are reflected in the Identity Vault.

If you want current data from the Student Information System to be synchronized to the Identity Vault (for example, because you are concerned that existing user account data doesn't currently match the Student Information System), use the *Migrate into Identity Vault* command after you add the Student Information System ID to the DirXML-sifSISID attribute.

If you choose this option, you need to fill in the DirXML-sifSISID immediately. If you don't, and a change comes through for an account, the driver cannot to find the matching User object and a duplicate is created.

Why Would You Use This Option?

- You already have User objects in the Identity Vault, and you don't want to delete them, but you do want the driver to manage them.
- You want to preserve the files that are currently in the home directories.

For example, if you were implementing the driver during the school year, and you wanted to keep home directories intact and minimize the risk of any problems with accounts, you might decide to keep existing accounts in place. With this option, you could keep accounts that are currently working and take the time to manually add the Student Information System ID to each of them, so the driver can recognize and manage them.

How To Set It Up

1. For all existing Identity Vault User objects, manually enter the Student Information System ID into the DirXML-sifSISID attribute. Make sure it is correct.

   This is a one-time effort.

   IMPORTANT: If the ID is not entered or is not correct, *Migrate into Identity Vault* creates duplicate User objects instead of updating existing User objects. There is no command to "undo" *Migrate into Identity Vault*, so you would need to remove the duplicates manually.

   ---

2. Set *Manage preexisting eDirectory users* to *Yes*.

   You set this on the Global Config Values page for the driver.

3. (Optional) If you want to synchronize existing accounts in the Identity Vault with all data from the Student Information System, you can use *Migrate into Identity Vault*.

   See "Using Migrate into Identity Vault to Populate or Update the Identity Vault" on page 49.

   If you are only concerned about synchronizing new changes that occur, you don't need to do this step.

   NOTE: You should use *Migrate into Identity Vault* when demand for the server is low, such as on a weekend. If you have more than one Zone configured, we recommend you perform the migration one Zone at a time. The migration can take approximately 20 seconds per user and places a load on the server.

After following these steps, Identity Manager can manage existing Identity Vault user accounts because you have manually made the association with the Student Information System ID. New users are also managed because Identity Manager automatically creates the association when it creates a new user.

5.4.3 Option 3: Don't Manage Existing Identity Vault User Accounts

For this option, you set the driver to ignore existing accounts and manage only new students who are entered in the Student Information System. You don't use the *Migrate into Identity Vault* command as part of setting up this option.

Existing student accounts in the Identity Vault are not affected by the driver; changes that occur for these accounts in the Student Information System are ignored by the driver.

New students added to the Student Information System after the driver is started are provisioned in the Identity Vault and are thereafter managed by the driver. The Identity Vault users created by the driver are always kept current with changes from the Student Information System.

Don't run the *Migrate into Identity Vault* command if you are using this option.

Why Would You Use This Option?

- You don't want the driver to affect existing student accounts.
- You only want the driver to provision and manage new students who are added to the Student Information System.
- You need to preserve the files that are currently in home directories.

For example, you could use this option if you were deploying the driver during the middle of the school year, and you wanted to eliminate risk to any existing accounts. Perhaps you don't have time to manually create the association with the Student Information System for each existing object. With this option, you can keep existing accounts as they are but take advantage of the driver's functionality to provision any new students.

How To Set It Up

1. Set *Manage preexisting eDirectory users* to *No*.

   You set this on the Global Config Values page.

2. Don't use *Migrate into Identity Vault*.

   If *Manage preexisting eDirectory users* is set to *No*, the *Migrate into Identity Vault* command is ignored.

Should I use the Migrate into Identity Vault or Synchronize Options?

The *Migrate into Identity Vault* command requests all student and staff records from the Student Information System and tries to match each record with an user account in the Identity Vault. If a match is found, the Identity Vault user account is updated with the information from the Student Information System. If a match is not found, a new user account is created in the Identity Vault.

For each user account in the Identity Vault, the *Synchronize* command queries the Student Information System for its attribute values and updates the Identity Vault user account with the received information.

The *Migrate into Identity Vault* command is more efficient. Only one query is sent to the SIS. The *Synchronize* command sends a separate query for each user account in the Identity Vault. The *Migrate into Identity Vault* command updates existing the Identity Vault user accounts and creates new Identity Vault user accounts. The *Synchronize* command only updates existing Identity Vault user accounts.

5.4.4 Using Migrate into Identity Vault to Populate or Update the Identity Vault

This section describes how to use the *Migrate into Identity Vault* command. This command lets you request records for all individuals from the Student Information System. If a matching user is not found in the Identity Vault, a new account is created. If an account already exists in the Identity Vault for the student, and the DirXML-sifSISID attribute contains the correct Student Information System ID, the driver updates the account to match the information in the Student Information System.

You can run *Migrate into Identity Vault* at the start of a school year to initially populate the Identity Vault. You can also run it any time you want to ensure the Identity Vault is synchronized with the Student Information System.

You should use this option only if the following two conditions are met:

- If you have any users in the Identity Vault, they must either have been created by the driver (which means they have an Identity Manager association created by the driver), or they must have the correct ID manually entered in the DirXML-sifSISID attribute.

This allows the driver to match an individual in the Student Information System with an existing User object.

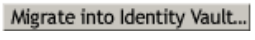
IMPORTANT: If this condition is not met, *Migrate into Identity Vault* creates duplicate User objects instead of updating existing User objects. There is no command to "undo" *Migrate into Identity Vault*, so you would need to remove the duplicates manually.

- ❑ The Driver object's *Manage preexisting eDirectory users* parameter is set to *Yes*.

  If it is set to *No*, the *Migrate into Identity Vault* command is ignored.

You should use *Migrate into Identity Vault* when demand for the server is low, such as on a weekend. If you have more than one Zone configured, we recommend you perform the migration one Zone at a time. The migration can take approximately 20 seconds per user and places a load on the server.

1. In iManager, click *Identity Manager* > *Identity Manager Overview*, and search for the driver set.
2. Click the driver icon for the driver.
3. If the driver is not running, click the icon in the upper-right corner of the driver icon, then select *Start Driver*.
4. Click the *Migrate into Identity Vault* button.

5. In the Migrate Data into the Identity Vault dialog box, click *Edit List*.

   The Edit Migration Criteria dialog box appears.
6. In the left column, select *User*, then click *OK*.
7. On the Migrate Data into the Identity Vault page, click *OK*.

   The driver continues to run the migration, even if you close iManager.

5.5 Synchronizing the Identity Vault Each School Year

You can synchronize student data in the Identity Vault so that it matches the Student Information System at the beginning of the school year. To accomplish this, you have options similar to the ones outlined in Section 5.4, "Synchronizing the Identity Vault the First Time," on page 46. Consult with your Student Information System administrator; the way your application works might influence your choice, and your application vendor might have a recommended approach.

This section describes the options and issues you should consider.

5.5.1 New Year Options for Students in School or Grade Containers

In this section:

Option 1 for a New Year: Repopulate the Identity Vault Using Migrate into Identity Vault

For this option, you delete existing student accounts and home directories in the Identity Vault and use *Migrate into Identity Vault* to repopulate the Identity Vault "from scratch" at the beginning of the year.

Why Would You Use This Option?

- Your Student Information System application recommends this kind of approach.

  We recommend this approach; however, you should consult with the administrator of the your Student Information System.
- You don't need to preserve the files that are currently in the home directories.
- You have students who are moving to new schools, their home directories need to be moved to a new server, and you don't want to move them manually.
- You have specified different eDirectory templates for different containers or schools, and you need accounts to be updated to match a new eDirectory template when users move to a new container or school.

How to Set It Up

1. Stop the driver at the beginning of the summer.
2. Remove the eDirectory accounts and the home directories.

   IMPORTANT: If existing home directories are not deleted along with existing user accounts, the users who are migrated won't have a home directory. Identity Manager must create the home directory at the same time it creates a user. It can't grant the newly created user rights to an existing home directory; instead, it gives an error.

   If you had existing user accounts with home directories and you didn't delete the home directories before using *Migrate into Identity Vault*, you need to delete them and repeat the migration.

   ---

3. At the end of the summer when the Student Information System is up-to-date for the next school year, start the driver again and use *Migrate into Identity Vault* to repopulate the Identity Vault.

   See "Using Migrate into Identity Vault to Populate or Update the Identity Vault" on page 49.

   You should use *Migrate into Identity Vault* when demand for the server is low, such as on a weekend. If you have more than one Zone configured, we recommend you perform the

migration one Zone at a time. The migration can take approximately 20 seconds per user and places a load on the server.

Option 2 for a New Year: Update Existing Accounts Using Migrate into Identity Vault

For this option, you keep your existing Identity Vault student accounts and update them all at once using *Migrate into Identity Vault* at the beginning of the year.

This option involves stopping the driver at the beginning of summer. At the end of the summer when the Student Information System data is ready for the new year, you start the driver again and use *Migrate into Identity Vault* to update existing accounts all at once.

To use this option, the driver must be able to associate existing user accounts with a record in the Student Information System. Therefore, all existing user accounts must have either the Student Information System ID entered in the DirXML-sifSISID attribute (you need to do this manually for users who were originally created by hand), or an Identity Manager association created (the driver does this for user accounts it creates).

IMPORTANT: If the ID is not entered or is not correct, *Migrate into Identity Vault* creates duplicate User objects instead of updating existing User objects. There is no command to "undo" *Migrate into Identity Vault*, so you would need to remove the duplicates manually.

Using *Migrate into Identity Vault* moves student accounts to new containers if necessary. However, the driver does not move home directories, so if the student account moves to a container on a new server and you want the home directory to be on the same server, you must move the home directories manually or with third-party software.

Why Would You Use This Option?

- Your Student Information System application recommends this kind of approach.
- You don't need student accounts to be re-created based on a new eDirectory template when they move to a new grade or school.
- You want to preserve the files in the home directories.

How To Set It Up

1. Stop the driver at the beginning of the summer.
2. When the Student Information System is up-to-date for the next school year, start the driver again and use *Migrate into Identity Vault* to synchronize the Identity Vault.

   See "Using Migrate into Identity Vault to Populate or Update the Identity Vault" on page 49.

   You should use *Migrate into Identity Vault* when demand for the server is low, such as on a weekend. If you have more than one Zone configured, we recommend you perform the migration one Zone at a time. The migration can take approximately 20 seconds per user and places a load on the server.
3. Move home directories as necessary, such as for students who are moving to a new school and whose accounts need to be on a different server.

   You can do this manually. Third-party software is also available to move home directories.

Option 3 for a New Year: Maintain Existing Accounts All Summer

For this option, you keep your existing Identity Vault student accounts, and keep them up-to-date by receiving changes as they are entered in the Student Information System over the summer.

You leave the driver running all summer to receive incremental changes from the Student Information System.

The driver moves students from one container to another as their schools and grades are updated in the Student Information System. However, the driver does not move home directories, so if the student account moves to a container on a new server and you want the home directory to be on the same server, you must move the home directories manually or with third-party software.

Migrate into Identity Vault is not required for this option.

Why Would You Use This Option?

- Your Student Information System application recommends this kind of approach.
- You want to preserve the files in the home directories.
- You don't need student accounts to be re-created based on a new eDirectory template when they move to a new grade or school.
- You need student accounts to be up-to-date all summer, such as for year-round schedules or summer school.

How to Set It Up

1. Keep the driver running all summer.
2. Move home directories as necessary, such as for students who are moving to a new school and whose accounts need to be on a different server.

   You can do this manually. Third-party software is also available to move home directories.

5.5.2 New Year Tasks for Students in Graduation Year Containers

If you put students in graduation year containers (see the example in Figure 2-2 on page 20), you need to update your tree structure each year to accommodate groups of students moving to new schools.

1. Manually create new graduation year containers under the school containers they are moving to.
2. In the Global Configuration Values for the driver, update the container DN and template assignments for all groups of students that are moving to a new school.

   See Section 5.1, "Creating and Configuring the Driver," on page 39.
3. Make sure the students are placed in the new container. You have three options for doing this, based on how you want to handle student accounts for each new school year.
   - "Option 1 for a New Year: Repopulate the Identity Vault Using Migrate into Identity Vault" on page 51
   - "Option 2 for a New Year: Update Existing Accounts Using Migrate into Identity Vault" on page 52

- "Option 3 for a New Year: Maintain Existing Accounts All Summer" on page 53

  For this option, if you create the new graduation year containers and update the Global Config Values for the driver *after* the school changes for students have been made in the Student Information System, then you still need to move students manually to the correct container.

4. After you have tested the change, and all the students have been moved to the new graduation year containers, delete the old containers.
5. Move home directories as necessary.

   You can do this manually. Third-party software is also available to move home directories.

Customizing the Driver

6

In this section:

6.1 Driver Parameters

The parameters in this table are in the driver properties, on the Identity Manager tab under Driver Configuration.

Table 6-1 *Driver Parameters*

Parameter	Default Value	Description
SIF Agent name	Novell Identity Manager	Specify the name this driver uses to register as a SIF Agent with the Zone Integration Server. The driver must have a Zone-unique, case-sensitive name. You need to coordinate with the ZIS administrator to make sure that the same name is used when configuring the ZIS, as described in “Configuring the ZIS to Recognize the Driver” on page 43.
SIF Specification version	SIF Spec 1.5r1	Specify the SIF Specification version you want this driver to use, either *SIF Spec 1.1*, or *SIF Spec 1.5r1*.
Driver keystore file	Blank	Specify the path and name of the client keystore file used when the ZIS is configured to request client authentication. For example: *java-home*\jre\lib\security\sifagentcert. This keystore file should hold only the client key and certificate. Leave this field blank if client authentication is not used. See Section 6.2, “Setting Up Security,” on page 56.
Driver certificate password	Blank	Specify the key password (not the keystore password) used when the ZIS is configured to request client authentication. Leave this field blank if client authentication is not used. See Section 6.2, “Setting Up Security,” on page 56.

Parameter	Default Value	Description
Authentication level	0	Specifies the security requirements of the communication channel between the ZIS and the recipient agents. Authentication level and encryption level define the minimum level of security a data transport channel must provide. See the SIF Specification (http://www.sifinfo.org) for more information about authentication level.
Encryption level	0	Encryption level specifies the security requirements of the communication channel between the ZIS and the recipient agents. Authentication level and encryption level define the minimum level of security a data transport channel must provide. See the SIF Specification (http://www.sifinfo.org) for more information about encryption level.
Poll rate in seconds	900	Specify the rate at which the driver polls the Zone Integration Server (ZIS) for incoming messages. We recommend 900 seconds when the driver is used in a production environment.
StudentSchoolEnrollment TimeFrame	Current	Specify the StudentSchoolEnrollment TimeFrame attribute values you want the driver to recognize. StudentSchoolEnrollment objects with TimeFrame values not specified here are ignored. Normally, the setting for this parameter should be Current. Specify other combinations only if your Student Information System uses them.

6.2 Setting Up Security

You should initially connect the driver to the ZIS using HTTP. After the connection is shown to be working, switch to using HTTPS. When passing real student information, we recommend that you use secure HTTP (HTTPS) between the driver and the Zone Integration Server (ZIS). Secure HTTP connections use server authentication. The server is the ZIS. In server authentication the client (the driver) authenticates that it is communicating with the expected server. (the ZIS) The ZIS server might also require client authentication. Client authentication occurs after the server authentication is complete. The ZIS server authenticates that it is communicating with a known client (the driver).

6.2.1 Server Authentication

For secure HTTP to work you must import the Certification Authority (CA) certificate used by the ZIS into the jssesacerts keystore file to show you trust the CA. To prove that a server belongs to the organization that it claims to represent, the server presents its public key certificate to the driver. This certificate is validated against the CA certificate so the client can be sure of the identity of the server.

The CA certificate must be added to the *java-home*/lib/security/jssecacerts keystore file. For NetWare® systems, *java-home* is typically sys:/java. For Windows systems, *java-home* is typically Novell\Nds\jre. The CA certificate is added to the keystore using the keytool utility (http://java.sun.com/j2se/1.3/docs/tooldocs/solaris/keytool.html). For example,

```
java-home/jre/bin/keytool -import -alias zisca -file zisca.cer -
keystore
java-home/jre/lib/security/jssecacerts -storepass changeit
```

This sets the initial password of the jssecacerts keystore file to “changeit.” The system administrator should change that password and the default access permission of that file.

6.2.2 Client Authentication

When client authentication (in other words, mutual authentication) is also desired, the client public key and certificate must be stored in a separate keystore file, for example *java-home*/lib/security/sifagentcerts. This keystore file should only hold the one client key. The name of this file is also entered in the driver configuration. You must import the client’s CA certificate into the client’s trusted-certificate store and the ZIS trusted-certificate store. You first need a client key pair, then a CA must sign the key pair.

One way to get the key pair signed is to use the Novell CA.

1. Export the Novell® CA trusted root certificate. In ConsoleOne®, open the Security container > select the Organizational CA > *Properties* > *Certificates tab* > *Self Signed Certificate* > click *Export*.
2. Select *No*, then click *Next*.
3. Save the certificate in Base64 format as NOVELLCASELFSIGNEDCERT.B64.
4. Import this certificate into the client’s trusted-certificate keystore.

   ```
   java-home/jre/bin/keytool -import -alias novellca -file
   NOVELLCASELFSIGNEDCERT.B64 -keypass novell1 -keystore
   java-home/jre/lib/security/cacerts -storepass novell2
   ```
5. This certificate must also be imported into the ZIS trusted-certificate keystore. Consult the ZIS documentation on how this is done.
6. Generate a public and private key pair for the agent in a new keystore file. The -dname parameter must contain the IP address of the client system or SIF Level 3 Authentication will not work. The -keyalg parameter must be RSA.

   ```
   java-home/jre/bin/keytool -genkey -alias sifagent -keyalg RSA -
   dname "CN=137.65.146.24, OU=DirXML, O=Novell, L=Provo, S=Utah,
   C=US" -keypass novell1 -keystore
   java-home/jre/lib/security/sifagentcert -storepass novell2
   ```
7. To guarantee the identity of the client, a certificate is needed to authenticate the key pair ownership. To do this, generate a Certificate Signing Request (CSR) in the novellagent.csr file.

   ```
   java-home/jre/bin/keytool -certreq -alias sifagent -file
   novellagent.csr -keypass novell1 -keystore
   java-home/jre/lib/security/sifagentcert -storepass novell2
   ```
8. Now use the Novell CA to generate a certificate for the client’s key pair. In ConsoleOne, select *Tools* > *Issue Certificate*.
9. In the Filename field, browse to and select the novellagent.csr file, then click *Next*.
10. Select Organizational Certificate Authority, then click *Next*.
11. Specify SSL or TSL as the Type, then click *Next*.
12. Review the certificate parameters, click Next, then click *Finish*.
13. Save the certificate in Base64 format as ISSUEDCERTIFICATE.B64.

14 The certificate now needs to be stored in the sifagentcert keystore with the key pair.

```
java-home/jre/bin/keytool -import -trustcacerts -alias sifagent -
file ISSUEDCERTIFICATE.B64 -keypass novell1 -keystore
java-home/jre/lib/security/sifagentcert -storepass novell2
```

15 At this point, your sifagentcert keystore consists of the client's CA self-signed certificate and your key and a Certificate Authority has signed it. View the sifagent keystore. There should be two entries. Your key entry should show "Certificate chain length: 2." The first certificate is your key; the second certificate is the CA that signed it. When the server (ZIS) asks for a certificate, the signed certificate is returned to the server for authentication.

```
java-home/jre/bin/keytool -list -v -keystore
java-home/jre/lib/security/sifagentcerts -storepass novell2
```

6.3 Identity Manager Association Keys

SIF objects have a GUID assigned to them by the application that creates the object. For example, the Student Information System assigns a GUID to each StudentPersonal object when a new student is created. The GUID uniquely identifies the SIF object. The GUID is part of the SIF object and is called the RefId. The RefId is always sent as part of the object. The driver uses the RefId for the Identity Manager Association Key.

6.4 Mapping SIF XML to the eDirectory Schema

SIF XML uses names that are hierarchical. Element names include the path to the element, relative to the data object. For example, the name of the City element in the StudentPersonal object is StudentAddress/Address/City.

The Identity Manager driver for SIF uses the path name as the element name, for example, Name/FirstName and Name/LastName. SIF element names are case sensitive. SIF application names in the Schema Map must use the path name. An example segment from a Schema Map follows.

```
<attr-name class-name="User">
     <nds-name>Given Name</nds-name>
     <app-name>Name/FirstName</app-name>
</attr-name>
<attr-name class-name="User">
     <nds-name>Surname</nds-name>
     <app-name>Name/LastName</app-name>
</attr-name>
<attr-name class-name="User">
     <nds-name>Telephone Number</nds-name>
     <app-name>PhoneNumber</app-name>
</attr-name>
```

SIF elements can contain attributes. Usually the attribute qualifies the element. For example, the element Name has the attribute Type="02." The value "02" qualifies the name as the legal name. SIF attribute values are enumerated in the SIF Implementation Specification or some other recognized standard. The SIF shim does not filter out these attributes or use schema mapping to change their names. The driver simply passes them through so the style sheets can process them. The attribute names are passed through using the namespace "sif" so they are not confused with Identity Manager reserved words. For example:

```
<add-attr attr-name="OtherId" sif:Type="06">
     <value type="string">360367</value>
```

```
</add-attr>
<add-attr attr-name="Name/LastName" sif:Type="02">
     <value type="string">Appleseed</value>
      </add-attr>
<add-attr attr-name="Name/FirstName" sif:Type="02">
     <value type="string">Johnny</value>
</add-attr>
      <add-attr attr-name="TelephoneNumber" sif:Format="NA"
sif:Type="HP">
     <value type="string">123-456-7890</value>
</add-attr>
```

Some SIF elements use an attribute field to specify the element value. For these special attributes, the driver takes the attribute value and passes it to eDirectory as the element value. Attributes whose values are used as the element value are specified in the sifobjects.conf file. Two examples are:

```
<StatePr Code="PA"/>
<Country Code="US"/>
```

These attributes are changed to:

```
<add-attr attr-name="StudentAddress/Address/StatePr" sif:Code="PA">
            <value type="string">PA</value>
      </add-attr><add-attr attr-name="StudentAddress/Address/Country"
sif:Code="US">
     <value type="string">US</value>
      </add-attr>
```

Troubleshooting the Driver

A

In this section:

A.1 Viewing Status Messages for the Identity Manager Driver for SIF

When configuring the driver, status messages can be viewed in the Driver Set Status Log, Publisher channel status log, Subscriber channel status log, or in the DSTrace screen. The status log contains error messages. The DSTrace screen contains a trace of the SIF Driver activity.

You can also set up logging using Novell® Audit. See “Logging and Reporting Using Novell Audit”in the *Novell Identity Manager 3.0.1 Administration Guide*.

In this section:

A.1.1 Using the Status Logs

To view messages in the Publisher or Subscriber status log:

1. In Novell iManager, click *Identity Manager* > *Identity Manage Overview*. Search for the driver set.
2. Click the driver icon.
3. In the page that appears showing the configuration for the driver, click the status log icon  for either the Publisher or Subscriber channel.

To view messages in the Driver Set status log:

1. In Novell iManager, click *Identity Manager* > *Identity Manager Overview*. Search for the driver set.
2. Click the status log icon  .

If you see errors you need to fix, you might want to clear the log so you can see which errors are new.

For a description of messages, see Section A.2, “Error Messages,” on page 62.

A.1.2 Using the DSTrace Screen

To obtain SIF Driver traces:

1. In the DSTrace window, click *Edit* > *Options* > *Events* > *Clear All* > select *Identity Manager Drivers* > *Save Default* > *OK*.
2. In iManager, click *Identity Manager* > *Identity Manager Overview*. Search for the driver set, then click the driver object icon. On the driver parameters page that appears, click the *Misc* tab. Set the trace level to 3, then click *Apply*.

For information on using DSTrace, see the *eDirectory 8.8 Administration Guide* (http://www.novell.com/documentation/lg/edir88/index.html).

A.1.3 Identity Manager Status Levels

For each event or operation received from the Identity Vault, the driver returns an XML document containing a status report. If the status report does not indicate success, the document also contains a reason.The table in Section A.2, “Error Messages,” on page 62 contains error text returned by the driver to Identity Manager.

Possible values for levels are:

- **Success:** The operation or event was successful.
- **Warning:** The operation was not successful, but can be ignored without consequences.
- **Error:** The operation failed.
- **Fatal:** A fatal error occurred, and the driver will be shut down.
- **Retry:** The ZIS is unavailable. Identity Manager retries the operation every 30 seconds.

Here are examples of return status in the trace screen:

```
<status event-id="0" level="success"/><status event-id="0"
level="warning">SIFdoes not support the Move operation.</status>
```

A.2 Error Messages

The following table contains errors that can be seen in the Status Log or DSTrace screen. The Error Condition column contains the error text returned to Identity Manager. The Level column specifies the status level. The Description column describes situations that might cause the condition and possible actions you can take to fix the problem. The message text and status level are recorded in the Driver Identity Manager log.

Table A-1 *Errors*

Error Condition	Level	Description
A SIF Agent Name must be provided.	Fatal	A SIF Agent Name must be specified in the driver parameters.
A Zone URL must be provided.	Fatal	A Zone URL must be specified in the driver parameters.

Error Condition	Level	Description
Authentication level must be 0-3.	Fatal	An authentication level of 0, 1, 2, or 3 must be specified in the driver parameters.
Connection to ZIS not yet established	Retry	The Metadirectory engine sent a command to the driver Subscriber channel. The driver cannot handle the command at this time because it does not have a connection to the ZIS. The engine retries the operation every 30 seconds.
Encryption level must be 0-4.	Fatal	An encryption level of 0, 1, 2, 3, or 4 must be specified in the driver parameters.
Error connecting to Zone = java.io.FileNotFoundException: http://ZISserver/zone1	Error	The specified ZIS server cannot be located. Use the IP address of the ZIS Server instead of a DNS name.
Error connecting to Zone = java.net.MalformedURLException: no protocol: ...	Error	The URL must begin with http:// or https://. Correct the URL and retry.
Error connecting to Zone = java.net.SocketException: Connection refused: Connection refused	Error	The ZIS server is up but the ZIS is not running. Start the ZIS.
Error connecting to Zone = javax.net.ssl.SSLException: Received fatal alert: handshake_failure (no cipher suites in common)	Error	
Error processing sifobjects.conf, code = xxx	Fatal	The sifobjects.conf file is required. Either the file could not be accessed or the file contains errors and cannot be processed. The Identity Manager trace contains additional information.
Error processing sifschema.xml	Fatal	The sifschema.xml file is required. Either the file could not be accessed or the file contains errors and cannot be processed. The Identity Manager trace contains additional information.
java.io.IOException: HTTPS hostname wrong: should be <x.x.x.x.x>, but cert says <y.y.y.y>	Error	The specified communications protocol is secure HTTP (HTTPS). The ZIS has sent its public key certificate to the driver for authentication. The certificate cannot be authenticated. The keystore file jssecacerts contain the server's CA trusted root certificate but the certificate contains the wrong hostname (cn=).
java.net.SocketException: Connection reset by peer: JVM_recv in socket input stream read	Error	The specified communications protocol is HTTP. The specified URL is a ZIS expecting a secure HTTP (HTTPS) connection. The ZIS URL is specified in Driver object > Properties > Driver Parameters.
javax.net.SocketException: Connection timed out: Connection timed out	Error	The specified ZIS server cannot be reached. Verify the ZIS address. If the ZIS server is on the other side of a firewall, verify that the firewall allows the connection.

Error Condition	Level	Description
java.net.SocketException: Network is unreachable	Error	TCP/IP is not configured properly. Verify that the gateway and subnet mask are correct.
java.net.SocketException: Software caused connection abort:	Error	TCP/IP is not configured properly. Verify that the gateway and subnet mask are correct.
javax.net.ssl.SSLException: Received fatal alert: bad_certificate	Error	The specified communications protocol is secure HTTP (HTTPS) with client authentication. ◆ An incorrect or no driver keystore file is specified, or ◆ An incorrect or no driver certificate password is specified. The agent keystore file and password are specified in the Driver object > Properties > Driver Parameters.
javax.net.ssl.SSLException: Received fatal alert: certificate_unknown	Error	The specified communications protocol is secure HTTP (HTTPS) with client authentication. The server could not authenticate the client's key. There are two possibilities: ◆ The client key in the agent keystore file is incorrect. or ◆ The client's CA trusted root certificate is not contained in the server's (ZIS) trusted keystore.
javax.net.ssl.SSLException: Unrecognized SSL handshake.	Error	The specified communications protocol is secure HTTP (HTTPS). The specified ZIS URL is not correct. The contacted server is not expecting a secure connection. The ZIS URL is specified in *Driver object* > *Properties* > *Driver Parameters*. Try using the IP address of the ZIS Server instead of a DNS name.
javax.net.ssl.SSLException: untrusted server cert chain		The specified communications protocol is secure HTTP (HTTPS). The ZIS has sent its public key certificate to the driver for authentication. The certificate cannot be authenticated. The keystore file jssecacerts does not contain the server's CA trusted root certificate.
Manage existing users must be 'yes' or 'no'.	Fatal	Manage existing users must be set to Yes or No in the driver parameters.
Migrate not supported when Match Existing Users is set to no.	Warning	The Driver will not process a *Migrate into the Identity Vault* command when *Manage Existing eDirectory Users* is set to *No*.

Error Condition	Level	Description
No initialization parameters No publisher initialization parameters No subscriber initialization parameters Publisher filter missing.	Fatal	On driver initialization, the Metadirectory engine provided no parameters. Verify that the Metadirectory engine is properly installed and configured.
No Publisher Option Parameters	Fatal	On Publisher channel initialization, the Metadirectory engine provided no Publisher options. Verify that *Driver Object* > *Properties* > *Driver Parameters* are properly configured.
Poll rate is not defined. Poll rate must be an integer value	Fatal	A valid poll rate must be specified in the Driver Parameters. The poll rate is an integer greater than 5.
SAXException = Missing whitespace before SYSTEM literal URI. null response received	Error	The specified URL is not correct. The contacted server is not a ZIS. The ZIS URL is specified in *Driver object* > *Properties* > *Driver Parameters*.
SIF Category = xxx, SIF Code = xxx, SIF Description = xxx, yyy;	Error	An error has been returned from the ZIS. This error is reported to Identity Manager. Additional information about the category, code, and description can be found in the SIF Implementation Specification (http://www.sifinfo.org).
SIF does not support the Move operation.	Warning	The SIF Implementation Specification does not contain the notion of containers. Therefore it does not provide for moving objects.
SIF does not support the Rename operation	Warning	The SIF Implementation Specification does not provide for renaming objects.
SIF objects to process not provided.	Fatal	The SIF objects to process are not specified in the Driver Parameters. The values are student, staff, or the names of defined SIF objects.
SIF Schema not available, error processing sifobjects.conf, code = xxx	Fatal	The sifschema.xml file is required. Either the file could not be accessed or the file contains errors and cannot be processed. The Identity Manager trace contains additional information.
The Incomplete container must be specified. Incomplete Container does not reference an Organizational Unit.	Fatal	The Incomplete container in the Driver Parameters must contain the DN of an organizational unit (container).
Unable to add home directory: novell.jclient.JCException: licenseConnection -1 DSERR_INSUFFICIENT_SPACE	Error	The NetWare® system must have sufficient user licenses installed. An available license does not exist that can be used for creating the user home directory.
Unsupported Subscriber Channel operation =	Error	The Metadirectory engine has passed the driver a command that it cannot convert to a SIF operation.

Error Condition	Level	Description
xmlDoc is null.	Error	The Metadirectory engine passed a null document to the Subscriber channel. Verify that the Metadirectory engine is properly installed and configured.
ZIS connection operational. (This is not an error.)	Informational	When the driver has established an operational connection with the ZIS this message is logged. If the connection is lost an error is logged. When the connection is reestablished this message is logged. Because only error messages are logged, this message shows in the log file as an error.
Zone is not responding = java.net.ConnectException: Connection refused: connect	Error	The ZIS is not up or is not accepting connections. Verify the ZIS address and port number.
Zone is not responding = java.net.ConnectException: Operation timed out: connect	Error	The specified ZIS server cannot be reached. Verify the ZIS address.
novell.jclient.JCException: modifyEntry -672 ERR_NO_ACCESS	Error	Driver Security Equals is not defined or does not have sufficient rights to perform operation.
provideUsers is not defined. modifyUsers is not defined. addUsers is not defined. Driver parameter <schools> malformed. Driver parameter <schools> parameter not available.	Fatal	The driver Subscriber channel configuration is not set up correctly. Remove the current driver object and add the driver again.
School Information zone n does not reference an enabled zone	Fatal	The Zone number specified in the SUBSCRIBER CHANNEL section of the Global Configuration Values does not reference an enabled Zone.
At least one School Information must be configured when providing users.	Fatal	When *Be the SIF Default Provider for Students and Staff* is set to Yes, one or more School information sets must be configured in the SUBSCRIBER CHANNEL section of Global Config Values.
Connection to ZIS not yet established	Retry	The driver has not yet established a connection the Zone when an event is received from the Metadirectory engine. The driver responds with a retry status.
A Search Container must be provided	Fatal	A search container must be specified in the *Global Config Values*.
Zone n - Enabled zone must have a URL Zone n - Malformed Zone URL = Zone n - URL not http or https =	Fatal	In the *Global Config Values* a Zone is enabled but a URL is not specified or is not correctly formed.

Error Condition	Level	Description
Zone n - Incomplete container must be configured for enabled zone.	Fatal	In the *Global Config Values*, a Zone is enabled but an Incomplete container is not specified.
Zone n - Staff container must be configured for enabled zone.	Fatal	In the *Global Config Values*, a Zone is enabled but a Staff container is not specified.
At least one zone must be enabled.	Fatal	In the *Global Config Values*, at least one Zone must be enabled.
Stopping driver because configured objects were not found in the Identity Vault.	Fatal	One of the DNs specified in the *Global Config Values* does not reference a valid object in the Identity Vault.
Stopping driver because nothing is on sendDocToEngine. Stopping driver because doc = null. Stopping driver because something is on sendDocToEngine.	Fatal	Internal Driver error.
SIF objects to process not provided. SIF objects must include StudentPersonal and/or StaffPersonal. Driver parameter *zone* malformed. *zone* parameter not available. Driver parameter *student* malformed. *student* parameter not available.	Fatal	The driver Publisher channel configuration is not set up correctly. Remove the current driver object and add the driver again.
No object name provided.		Disregard this error message. It does not indicate a problem.

A.3 Common HTTP Status Codes

- 404 indicates that the requested resource is not available.
- 401 indicates that the request requires HTTP authentication.
- 500 indicates an error inside the HTTP server that prevented it from fulfilling the request.
- 503 indicates that the HTTP server is temporarily overloaded and unable to handle the request.

A.4 ZIS Return Status

For each event or operation sent to or received from the ZIS, an XML document containing a SIF_Ack message is returned. A SIF_Ack contains either a SIF_Status element acknowledging a successful result or a SIF_Error element indicating the error. The SIF_Error element contains an error number as well as a description of the error. The error number and descriptions are defined in the SIF Implementation Specification (http://www.sifinfo.org).

Examples

```
<SIF_Status>
    <SIF_Code>0</SIF_Code>
    <SIF_Data>Success</SIF_Data>
</SIF_Status>
```

```
<SIF_Error>
    <SIF_Category>1</SIF_Category>
    <SIF_Code>1</SIF_Code>
    <SIF_Desc>Message is not well-formed</SIF_Desc>
    <SIF_ExtendedDesc>Next character must be ">" terminating element
"Name".</SIF_ExtendedDesc>
</SIF_Error>
```

Global Configuration Values

B

The following table contains the various Global Configuration Values available for the SIF driver on the Global Config Value page. After the driver is created, review these setting to make sure the proper options are set for your environment.

Table B-1 *Global Configuration Values*

Field Name	Description
Driver Configuration	
Search container DN	The container below which User IDs must be unique. When creating a new User object, the driver searches the Identity Vault to verify that the new User ID is not already in use. This container and all subcontainers are searched. Choose the district container or a container that is high enough in the tree that user IDs are unique for all students and staff. For example, for the environment shown in Figure 2-6 on page 26, you would specify the District container. This search container is used for all zones. If you select Yes in the *Send New Users to SIF* field, only users in this container and its subcontainers are sent to SIF.
Manage preexisting eDirectory users	This option lets you decide whether you want the driver to manage accounts that you already have created in the Identity Vault, before using this driver. The SIF Driver can match students and staff in the Student Information System (SIS) with preexisting Identity Vault users only if the Identity Vault user attribute DirXML-sifSISID contains the student's or staff's ID number. Select *Yes* if one of the following is true: ◆ You want to manage preexisting Identity Vault users, and the DirXML-sifSISID is set on all users. ◆ No users currently exist in the Identity Vault, and you plan to let the driver create them all using the Migrate into the Identity Vault command. Otherwise, select *No*. If *Yes* is specified, the *Migrate into the Identity Vault* command can be used to add or update all SIF users into the Identity Vault. If *No* is specified, the *Migrate into the Identity Vault* command is ignored to prevent duplicate users from being created in the Identity Vault. This field does not apply to users added to the Identity Vault by this driver. Identity Manager can always match these Identity Vault users with Student Information System users, and these Identity Vault users are always kept current with changes from the Student Information System. For more information on how to make this decision, see Section 5.4, "Synchronizing the Identity Vault the First Time," on page 46.

Field Name	Description
Send user updates to SIF	Select *Yes* if you want changes made to users in the Identity Vault to be sent to SIF. You might want to do this for the following reasons: ◆ the Identity Vault is the authoritative source for some student information and you want SIF applications notified when it changes. ◆ Your Student Information System is not SIF-enabled and you want the Novell SIF Driver to inform SIF of changes to student and staff information. Otherwise, select *No*.
Send new users to SIF	Select *Yes* if you want new users in the Identity Vault to be sent to SIF. You might want to do this if your Student Information System is not SIF-enabled and you want the Novell SIF Driver to inform SIF of new students and staff. If you select Yes you should also set “Send user updates to SIF” to Yes. Otherwise, select *No*.
Send email notification	Send an e-mail notification when an Identity Vault account’s User ID is renamed or when a new user is created with a non-standard User ID. User IDs must be unique. When the driver receives information for a new student from the Student Information System, it follows the format for creating the User ID that you chose in the User ID Format. Before creating the User object, the driver searches for a duplicate ID starting with the container you specified in the Search container DN. If the driver finds the user ID already exists, the driver creates a unique ID by appending a digit to it. For example, if Dawn Smith had the User ID of DSmith, and a new user named David Smith were added, the driver place him in the appropriate container and would give David the User ID: DSmith1. Also, when an Identity Vault user account is renamed by the driver, an e-mail notification can be sent. Select Yes if you want e-mail notifications sent. You must have a local SMTP server. Otherwise, select No. If you select *Yes*, you are presented with the following four additional prompts: ◆ *Recipient’s email address* Replace the sample e-mail address with the recipient’s e-mail address, for example, admin@school.com ◆ *SMTP server address* Replace the sample address with the address of an SMTP server, for example, mail.school.com. You must have a local SMTP server. ◆ *Optional user account on SMTP server* Optional credential for authentication to the SMTP server. If the SMTP server requires authentication, enter the user account name. Otherwise, leave the field blank. ◆ *Optional password for user account on SMTP server* Optional credential for authentication to the SMTP server. If the SMTP server requires authentication, enter the password for the user account. Otherwise, leave the field blank. For more information, see the following fields below: *Rename student users when naming attributes change* and *Rename staff users when naming attributes change*.

Field Name	Description
Specify the Student Information System you are using	Select the Student Information Management System you are using. ◆ *CSIU Administrative Software* ◆ *Apple PowerSchool* ◆ *NCS Pearson SASIxp* ◆ *SunGard Pentamation eSchoolPlus* ◆ *Visual Software* This information is used to accommodate unique features about each SIS. Select *Other* if the SIS you are using is not listed. Select *Yes* if you want to manage student accounts in the Identity Vault, otherwise select *No*.
Student Configuration	
Manage student accounts	Select *Yes* if you want to manage student accounts in the Identity Vault. Otherwise, select *No.*
Student user ID format	Configure the Student user ID format. The format is composed of five parts. The five parts are concatenated to produce the user ID. See the description and example in Section 2.4, “Specifying the Pattern for User IDs,” on page 29.
Rename student users when naming attributes change	Select *Yes* if you want student user accounts in the Identity Vault renamed when any of the attributes change that are used to build the User CN (the attributes you select in Student user ID format). Otherwise, select *No.* See *Send e-mail notifications* in the Driver Configuration options above.
Student placement is by	Select the criteria used to place students in the Identity Vault tree. ◆ *School and Grade* - Students are placed based on their school and grade level. ◆ *School and Graduation Year* - Students are placed based on their school and graduation year. ◆ *Grade Only* - Students are placed by grade level only. ◆ *Graduation Year Only* - Students are placed by their graduation year only. ◆ *School Only* - Students are placed by their schools only.
Student password format	Select a password format for students. ◆ *Student ID* - Student ID number. ◆ *Preset text* - The password is the text specified in the field below. ◆ *No password* - No password is specified; the user logs in without a password.
Student preset text for password	If you selected *Preset text* in the *Student password format* field above, specify the password you want to be assigned to new student users. Otherwise, leave this field blank.
Staff and Employee Configuration	

Field Name	Description
Manage staff and employee accounts	Select *Yes* if you want to manage staff and employee accounts in the Identity Vault. Otherwise, select *No*. Typically StaffPersonal objects are maintained by the SIS and EmployeePersonal objects are maintained by the HR system. When you select *Yes,* there are additional options. These options are documented below.
SIF Staff and Employee objects to manage	◆ *StaffPersonal* - provisions SIS data into the Identity Vault. ◆ *EmployeePersonal* - provisions HR data in the Identity Vault. ◆ *StaffPersonal and EmployeePersonal* - Provisions both.
Staff user ID format	Configure the *Staff user ID format*. The format is composed of five parts. The five parts are concatenated to produce the user ID. See the description and example in Section 2.4, “Specifying the Pattern for User IDs,” on page 29.
Rename staff users when naming attributes change	Select *Yes* if you want staff user accounts in the Identity Vault renamed when any of the attributes change that are used to build the User CN (the attributes you specify in Staff user ID format). Otherwise, select *No*. See *Send email notification* in the Driver Configuration options above.
Staff password format	Select a password format for staff. ◆ *Staff ID* - Staff ID number. ◆ *Preset text* - Password is the text specified in the prompt below. ◆ *No password* - No password is specified; the user logs in without a password. You can modify the formats in the Publisher Create style sheet.
Staff preset text for password	If you select *Preset text* in the *Staff password format* field above, specify the password you want to be assigned to new staff users. Otherwise, leave this field blank.
Zone Configuration	
Zone 1	Configuration information for each SIF Zone the driver connects to. Select *Show* to use the zone. Select *Hide* if you do not need the zone. The driver can connect up to ten Zones. You can use as many or as few Zones as needed for your environment. The order of the Zones is not important. *Zone 1* through *Zone 10* contain the same fields. You specify the information for each Zone.
Connection to Zone	Select *Enabled* if the driver is to connect to this Zone. Select *Disabled* if the driver is to ignore these parameters. The connection to a configured Zone is disabled, for example, when testing an individual Zone or when a Zone is offline.

Field Name	Description

Zone URL	The URL of the SIF Zone Integration Server (ZIS) this driver connects to. The URL can be obtained from the ZIS administrator. It is case sensitive.
	
	The protocol is HTTP (Hypertext Transfer Protocol) or HTTPS (Secure Hypertext Transfer Protocol).
	
	If you have DNS, you can use the hostname; otherwise, use the IP address.
	
	Example URLs are
	`http://www.myzis.com/Zone1`
	`https://1.2.3.4:123/Zone2`
	
	When https is specified, the CA certificate for the ZIS must be placed in the *java-home*`\jre\lib\security\jssecacerts` keystore file. For more information on how to set this up after importing the driver, see Section 6.2, “Setting Up Security,” on page 56.

Incomplete Container DN	The DN of the Incomplete container. If the grade or school for a student is not provided by the Student Information System, the user is created in the Incomplete container with login disabled. No template is used when creating the user. When the Student Information System provides the missing information, the user is deleted from this container, and created in the correct container. Browse and select the Incomplete container you created for this Zone. This is the Incomplete container that you created during planning, in “Identifying “Incomplete” Containers” on page 23.
Disabled container DN	A student’s login is disabled when he or she withdraws from school. If you want the student moved when the login is disabled, browse and select the Disabled container you created for this Zone. If you do not want the user moved, leave this field blank.
Staff container DN	If you are managing SIF staff users, browse and select the container where you want staff users to be placed for this Zone. Leave this field blank if you are not managing staff users.
Staff template DN	If you are managing SIF staff users, browse and select the eDirectory Template object you want to be used when creating staff users. Leave this field blank if you are not managing staff users or if you are not using a template.
Student Placement	
School 1	Use this field to separate school configurations. Use this section to configure the placement of students in the same school. It places students in an eDirectory container based on their school code, graduation year, or grade level. You need to know the values your Student Information System (SIS) uses for schools, graduation years, and grades. Complete as many Student group placement entries as you need to in order to place all students. Use *Show* to use the *School* fields. Use *Hide* if you do not need all ten options. *School 1* through *School 10* contain the same fields. Use the additional *School* field to define information specific for each school you administer.

Field Name	Description
School code or 'all'	The value of this field is based on your *Student placement is by* criteria. If you specified *School and Grade, School and Graduation Year,* or *School Only* enter the school code for this group of students exactly as it is specified in the Student Information System. Contact the administrator to find out the school code. This code might be alpha, numeric, or a combination. If you specified *Group Only* or *Graduation Year Only* in *Student placement is by*, type `all`. It must be all lowercase.
Student Group 1 Placement	This section lets you configure the placement of a group of students in the Identity Vault. Students are placed in an eDirectory container based on their school code, graduation year, or grade level. You need to know the values your Student Infomration System (SIS) uses for schools, graduation years and grades. Complete as many *Student Group x Placements* entries as you need to place all students. *Student Group 1 Placement* through *Student Group 6 Placement* contain the same fields. Use the additional *Student Group Placement* fields to place additional groups of users. To use a *Student Group Placement* fields set the option to *Show*. If you do not need all six fields, set any fields not in use to *Hide*. If you need more than six *Student Group Placements* for this school, use additional *Student Group Placements* with the same school code.
Grade code, graduation year, or 'all'	Fill in this field based on your choice in the *Student Placement is by field*, in the STUDENT CONFIGURATION section. If you specified *School and Grade or Grade Only* in *Student Placement is by field*, specify the grade level code exactly as it is specified in the SIS. If you specified *School and Graduation Year* or *Graduation Year Only* in Student Placement Is by, specify the graduation year exactly as it is specified in the SIS. If you specified *School Only* in Student Placement Is by, type `all`. It must be all lowercase.
Student container DN	Browse and select the eDirectory container where you want this group of students to be placed.
Student template DN	Browse and select the eDirectory template you want to be used when creating users for this group of students. Leave this field blank if you are not using a template.
SIF Provider Configuration	
Configure this section only when this driver is the SIF provider for student and staff information, as described in "Sending Data from the Identity Vault to SIF" on page 15.	
You might want to do this if your Student Information System is not SIF-enabled, and you want the driver to be the SIF provider of student and staff information. Being the provider means this driver responds to SIF queries for information about students and staff.	

Field Name	Description
Be the SIF default provider for students and staff	Select *Yes* if you want this driver to be the SIF provider for student and staff information. If you select Yes, other settings are displayed. You might want to do this if your Student Information System is not SIF-enabled and you want the Novell SIF Driver to be the SIF provider of student and staff information. Being the provider means this driver responds to SIF queries for information about students and staff. See "Sending Data from the Identity Vault to SIF" on page 15. If you select *Yes*, you must also set *Send User Updates to SIF* to *Yes* and *Send New Users to SIF* to *Yes*, and configure one or more sets of School Information. Otherwise, select *No*.
School information	This field is used to separate school configurations. This prompt and its sub-prompts are only used if you set *Be the SIF Default Provider for Students and Staff* to *Yes*. This information is used so the SIF Driver can provide the SIF SchoolInfo objects. You need to know the value your Student Information System uses for each school. Complete as many School Information entries as you need to define all schools.
School code	Specify the school code exactly as it is specified in the Student Information System.
School name	Specify the school name as it is specified in the Student Information System.
Zone number	Specify the Zone number (1-10) this school belongs to.
Password Configuration **By default, this section has a setting of Hide. It is used only if you want the driver to exchange passwords between the Identity Vault and the SIF zones.**	
Password Configuration Parameters	The only settings you should edit here are the ones listed in this table. The others are GCVs regarding Password Synchronization that are common to all drivers. They should be edited using iManager in *Passwords* > *Password Synchronization*, not here. Some of them have dependencies on each other that are represented only in the iManager interface. They are explained in "Password Synchronization across Connected Systems"in the *Novell Identity Manager 3.0.1 Administration Guide*.
SIF Driver sends user passwords to the Zone	If set to *True*, the SIF driver sends user passwords in the Identity Vault to the Zone. Passwords are sent as SIF Authorization objects. Other SIF-enabled applications can subscribe to the Zone to receive the passwords. You would set this parameter to *True* when other SIF-enabled applications want to use the user's network password. When a Distribution Password is set for a new user or when a Distribution Password is changed in the Identity Vault, the Novell SIF driver sends a SIF Authorization object containing the password to the Zone.

Field Name	Description
SIF Driver accepts user passwords from the Zone	If set to *True*, the SIF Driver sets user passwords in the Identity Vault to the passwords received from the Zone. The passwords are received as SIF Authorization objects. The passwords are published to the Zone by other SIF-enabled applications. You would set this parameter to *True* if you want the network password to be generated by another SIF-enabled application. For example, you have a SIF-enabled application in the Zone that generates a password for each user. When the Novell SIF driver receives the password in a SIF Authorization object, the corresponding user's eDirectory password is set to this value. If this parameter is set to *True*, we recommend that the Novell SIF driver also be configured to set a password for each new user. There might be a delay between the creation of the user account and when the password is received, and it is best to make sure the account is protected by a password at all times.

Glossary

This glossary contains some basic Identity Manager terms and SIF terms used in this driver documentation.

Agent
A SIF term. SIF-enabled software that interfaces with an application on one side and a Zone Integration Server on the other side. The Agent is used to make the application's data available to the Zone or to consume data from the Zone and to make it available to the application. The Identity Manager Driver for SIF is a SIF Agent.

shim
An Identity Manager term. Another word for driver.

Schools Interoperability Framework (SIF)
A SIF term. The Schools Interoperability Framework (SIF) is an industry initiative to develop an open specification for ensuring that K-12 instructional and administrative software applications interact and share data seamlessly. SIF is not a product, but rather an industry-supported technical blueprint for K-12 software. For additional information about SIF, see the Schools Interoperability Framework Web site (http://www.sifinfo.org).

Connecting the applications with a common framework allows you to enter information once in an authoritative information source, such as a Student Information System (SIS), and then publish that information so other systems can be updated automatically.

Student Information System (SIS)
A SIF term. A K-12 application for maintaining student information. Some Student Information Systems also store faculty and staff information.

Publisher channel
An Identity Manager term. The work of provisioning SIF student or staff from the SIS to Novell® eDirectory™ users is done through the Publisher channel of Identity Manager. You can customize the configuration that comes with the driver.

For more information on the channels, see *Novell Identity Manager 3.0.1 Administration Guide*.

Subscriber channel
An Identity Manager term. In the base configuration, the student information system is the authoritative data source for student information, so no data is sent from the Identity Vault to the SIS through the Zone Integration Server (ZIS). The Subscriber channel is fully functional, but in the base configuration it is not used.

You can customize the Subscriber channel to send data changes made in the Identity Vault to SIF, if desired.

For more information on the channels, see the *Novell Identity Manager 3.0.1 Administration Guide*.

Zone

A SIF term. A grouping of SIF-enabled Agents for sharing data. A Zone might be small or large, servicing a school, several schools, or a district. An Agent must register with a Zone. The Zone manages the registered Agents.

Zone Integration Server (ZIS)

A SIF term. A software product that implements the SIF ZIS functionality and can also contain value-added management and configuration tools. A ZIS should be capable of supporting more than one Zone. The term ZIS is often used to mean a Zone.