NetIQ

Identity Manager 4.5 Driver for Ellucian Banner Implementation Guide

Identity Manager 4.5
Driver for Ellucian Banner Implementation Guide

September 20, 2014

www.netiq.com/documentation

Legal Notice

Contents

About this Book and the Library

The *Identity Manager 4.5 Driver for Ellucian Banner Implementation Guide* explains how to install and configure the Novell® Identity Manager Ellucian Banner driver 4.0.1.

Intended Audience

This book provides information for consultants and administrators implementing Novell Identity Manager driver for Ellucian Banner. You should have an understanding of the Ellucian Banner system, SPML, SOAP, and HTML.

Other Information in the Library

The library provides the following information resources:

Installation Guide

Provides detailed planning and installation information.

User Guide

Provides conceptual information about DRA and ExA. This book also provides an overview of the user interfaces and step-by-step guidance for many administration tasks.

Trial Guide

Provides product trial and evaluation instructions and a product tour.

Help

Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for each field on each window.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit http://community.netiq.com.

1 Overview

1.1 Introduction

The Novell Identity Manager driver for Ellucian Banner (Ellucian Banner) integrates with the Ellucian Banner system. The driver synchronizes identity information for people in the higher education environment: students, faculty, and staff. This information is stored in the Identity Vault where it can be synchronized with other applications.

Ellucian Banner provides the Unified Digital Campus to unify people, processes, and technology in an environment that addresses the needs of higher education institutions and the people they serve. The Ellucian Banner solutions involve the Banner Suite*, Luminis Portal* and Workflow and other applications. While the architecture of the Ellucian Banner driver and the Ellucian Banner integration points it ties to is intended to allow a single driver to integrate with any of the Ellucian components, version 4.0.1 of the driver is only supported by the Banner Suite.

Ellucian Banner communicates identity information using the UDCIdentity* Schema in SPML 2.0 formatted documents. The Identity Manager driver for Ellucian Banner converts the UDCIdentity schema from SPML 2.0 format into Novell XDS format and publishes the resulting document to the Identity Vault.

For more information about the UDCIdentity, see the Ellucian Banner Banner Identity Handbook.

For more information on SPML 2.0, see <OpenSMPL.org> (http://www.openspml.org/).

1.2 How the Driver Works

The Identity Vault uses XDS, a specialized form of XML, to represent events in the Identity Vault. The Novell Identity Manager passes the XDS to the driver policy, which can consist of basic policies, DirXML Script, and the XSLT style sheets.

The following diagram illustrates the data flow between the Identity Manager and the Ellucian Web service:

Figure 1-1 *Ellucian Banner Driver Data Flow*

The schema mapping driver policy translates the Identity Vault Schema in XDS to UDCIdentity.

The Subscriber channel of the driver shim receives the XML from the driver policy and converts the UDCIdentity data from XDS format into SPML 2.0 format. The driver then encapsulates the SPML in a SOAP envelope and uses HTTP to communicate with the Web service. The hand-off between the driver shim and the application is serialized XML.

The Web service or application processes the request and returns a SOAP response to the driver shim. The shim receives the response as an array of bytes and converts it to an SPML document before passing it back to the driver policies. The Novell Identity Manager driver for ~~Sungard~~Ellucian Bannerprocesses the response, converting it into XDS that is reported back to the Identity Vault.

The Publisher channel of the driver shim receives a UDCIdentity in SPML from BEIS and converts the UDCIdentity data into XDS format. The driver then passes the XDS to the Identity Manager engine, where the Schema Mapping policy converts the UDCIdentity into the eDirectory schema before committing the object to eDirectory.

Identity Manager processes the change and returns a response formatted in XDS. The driver converts the response into SPML and returns it to BEIS.

1.3 Key Driver Features

The following sections contain a list of the driver's key features.

1.3.1 Local Platforms

A local installation is an installation of the driver on the Metadirectory server. The Ellucian Banner driver can be installed on the operating systems supported for the Metadirectory server.

For information about the operating systems supported for the Metadirectory server, see "Metadirectory Server" in "System Requirements" in the *Identity Manager 4.0 Framework Installation Guide*.

1.3.2 Remote Platforms

The Ellucian Banner driver can use the Remote Loader service to run on a server other than the Metadirectory server. The Ellucian Banner driver can be installed on the operating systems supported for the Remote Loader.

For information about the supported operating systems, see "Remote Loader" in "System Requirements" in the *Identity Manager 4.0 Framework Installation Guide*.

1.3.3 Supported Operations

The Ellucian Banner driver interacts with Banner via the Banner Enterprise Integration Service (BEIS). BEIS publishes data in SPML format. The driver is limited to operations supported by SPML. The basic configuration files for the Ellucian Banner driver are capable of performing the following operations on User objects.

- Add

- Modify
- Delete
- Query
- Modify password

BEIS does not support rename or move operations. It is possible to synthesize these operations in IDM Policy based on attribute data changes in the XML data received from BEIS.

The driver publishes role information from the Ellucian system. Roles are used to grant access to information on the Ellucian Portal in Luminis and other Ellucian applications and resources. Ellucian does not delete identities after they are created. The Ellucian system removes roles from the collection of roles on a given user. Consultants or IDM administrators deploying the driver might implement Role-Based Entitlements on other drivers to react to changes in the list of roles for a given user.

For additional information, see Section 3.1.6, "Understanding Institutional Roles," on page 22.

1.3.4   Password Synchronization Support

By default, the Novell Identity Manager driver for Ellucian Banner policies do not synchronize passwords to or from the Ellucian system. However, when a user is added to the Identity Vault, a password can be created for the user by selecting an attribute to pull the password from, or by generating a random password using a policy on the Publisher Channel Command Transform.

In order to configure this policy, select the behavior of this policy by setting the "Banner Password Settings" attributes on the "Password Settings" tab of the GCV editor.

Select *Random Password* to have a random password generated for the new user. You can specify the number of alphabetic characters and numeric characters which must be used in generating the password.

Select *Attribute Value from User* to have a password value set from the value of an attribute on the user object. BEIS can be configured to publish a password from the Banner system as an extension attribute. The driver will recognize the extension attribute and publish it as an <add-attr> element in the XDS document to be sent to the IDM engine. Map the Banner element name to an eDirectory attribute and set that attribute name as the *eDirectory attribute to use for initial password value* and the driver password policy will use the attribute in the specified eDirectory attribute as the user's new password.

2 Installing the Ellucian Banner Driver

The Ellucian Banner driver can be installed on multiple systems and platforms. To verify the system requirement list, see "System Requirements" in the *Identity Manager 4.0 Framework Installation Guide*.

This section contains the following information:

- "Getting the .iso file from the Novell Download Site" on page 13
- "New Installation by Using a Physical Media or ISO" on page 14

2.1 Getting the .iso file from the Novell Download Site

1 Go to the *Novell Download page* (http://download.novell.com).

2 In the Product or Technology menu, select Identity Manager Integration Modules, then click *Search*. You may wish to narrow your search by entering "Banner" in the *Keyword* field.

3 On the Novell Identity Manager Downloads page, click *Download* next to *Identity Manager Integration Module 4.0.1 for Banner*.

4 Follow the on-screen prompts to download the file to a directory on your computer.

If you haven't already verified that the media you burned is valid, you can check it by using the Media Check option; otherwise, refer to the Getting the .iso file from the Novell Download Site section.

2.2 New Installation by Using a Physical Media or ISO

Insert the disc of the Identity Manager 4.0.1 installation media that you created into the CD-ROM or DVD drive of the computer that you want to be your Identity Manager 4.0.1 server.

1 From the CD root folder \Additional_Drivers\Ellucian Banner, start the installation by executing the correct program for your workstation's platform.

   ◆ **Windows:** If you are installing to the Identity Vault server, Copy `Ellucianbannershim.jar`to the DirXML Drivers directory. The default value is `c:\novell\nds\lib`. If you are using Remote Loader to run the driver, then copy `Ellucianbannershim.jar` to `c:\novell\remoteloader` on the maching running Remote Loader.

   ◆ **Linux:** `rpm -ivh novell-DXMLBanner.rpm`

   ◆ **Solaris:** `pkgadd -d novell-DXMLBanner.pkg`

2 In order to use the pre-config package within Designer, you will need to extend the eDirectory schema using the following steps:

   ◆ **Windows:**

      1. Click Start > Settings > Control Panel > Novell eDirectory Services

      2. Click install.dim, then click Start

      3. Click Install Additional Schema files, then click Next

      4. Log in as a user with administrative rights, then click OK

      5. Specify the schema file path and name (<InstallDirectory>\Novell_Banner_Schema.sch)

      6. Click Finish

   ◆ **Linux/Unix:**

      1. /opt/novell/eDirectory/bin/ndssch -h <localhost:524> -t <MyTreename> <admin_fdn>/ opt/novell/eDirectory/lib/nds-schema/Novell_Banner_Schema.sch

3 It may be necessary to restart eDirecory once the driver binary and schema have been updated.

   ◆ **Windows:**

   Use services to restart your eDirectory Instance.

   ◆ **Linux/Unix:**

   `/etc/init.d/ndsd restart`

3 Creating a Working Driver

After the Ellucian Banner driver files are installed on the server where you want to run the driver (see Chapter 2, "Installing the Ellucian Banner Driver," on page 13), you can create the driver in the Identity Vault. You do so by importing the driver configuration file and then modifying the driver configuration to suit your environment.

The following sections provide instructions to create the driver:

3.1 Creating the Driver in Designer

You create the Ellucian Banner driver by importing the driver's configuration file and then modifying the configuration to suit your environment. After you have created and configured the driver, you need to start it.

3.1.1 Installing the Current Driver Packages

The driver packages contain the items required to create a driver, such as policies, entitlements, filters, and Schema Mapping policies. These packages are only available in Designer and can be updated after they are initially installed. You must have the most current version of the packages in the Package Catalog before you can create a new driver object.

To verify that you have the most recent version of the driver packages in the Package Catalog:

1 Open Designer
2 In the toolbar, Left Click Help > Check for Package Updates
3 Left Click OK to update the packages or Left Click OK if the packages are up-to-date
4 In the Outline view, Right Click the Package Catalog
5 Left Click Import Package
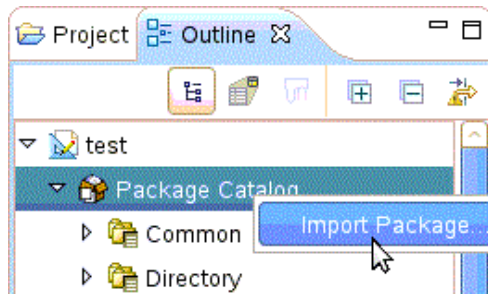
6 Select any Ellucian Banner driver packages

Or

Left Click Select All to import all of the packages displayed.

> **NOTE:** By default, only the base packages are displayed. Deselect Show Base Packages Only to display all packages.

7 Click OK to import the selected packages, and then click OK in the successfully imported packages message.

8 After the current packages are imported, then continue with section,

3.1.2   Installing the Driver

1 In Designer, open your project.

2 Right-click on the Driver-set where you want to configure the Ellucian Banner driver, select *New* and then *Driver*. In the Driver Base Package Configuration screen, scroll down to find the Banner Base package. Left-click the box next to Banner Base.
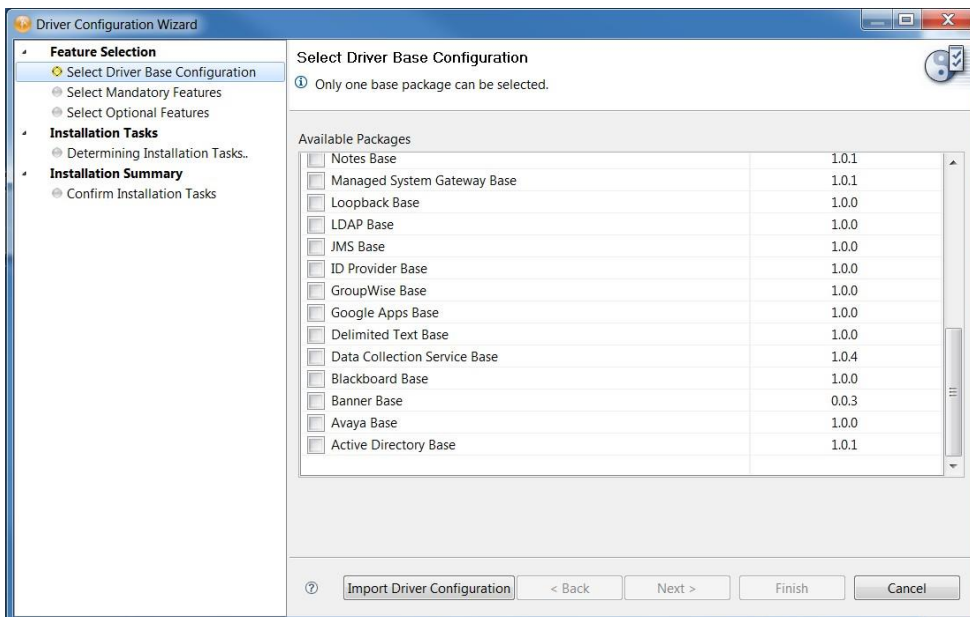
3 Select Banner Base, and then Left Click next.

4 Select the optional features to install for the Ellucian Banner driver.

NOTE: By default "show Only applicable packages versions" will be selected as expected.

Select the optional Ellucian Banner User Package.
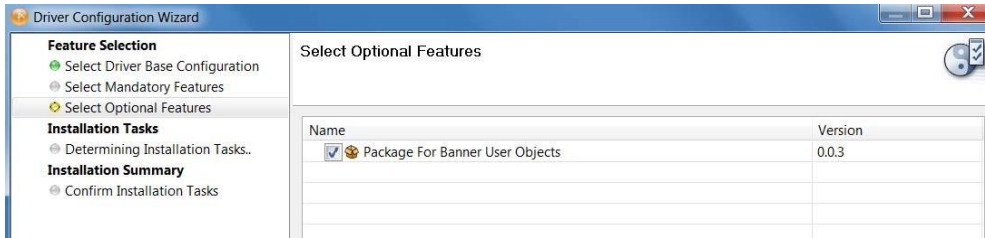
5 Left Click Next

6 (Conditional) If there are package dependencies for the packages you selected to install, you must install them to install the selected package. Left Click OK to install Package Dependencies.

NOTE: There will be mutable instance of this; one for each option selected.
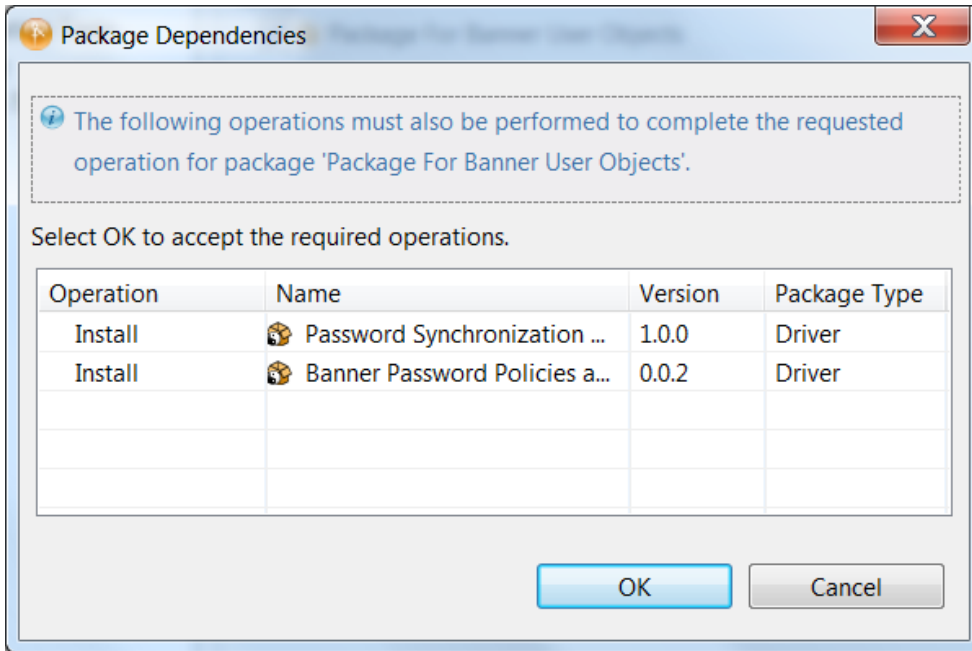
7 On the "Install Ellucian Banner Base" page, specify a name for the driver that is unique within the driver set, and then click next.

8 Set Banner Password Settings to configure how new user passwords will be generated. .

- ◆ Selecting "Random Password" to have the password policy generate a random password. Select the number of letters and the number of digit characters to be included in the password.

- ◆ Select "Attribute Value from User" to use the value of an attribute on the user as the password. The attribute name is selected from the eDirectory namespace.

NOTE: Map a UDCIdentity attribute or BEIS extension attribute to an eDirectory attribute to support this policy. Ensure the eDirectory attribute is entered in the drver filter as "Notify" to prevent the password from being written to the eDirectory attribute.

---
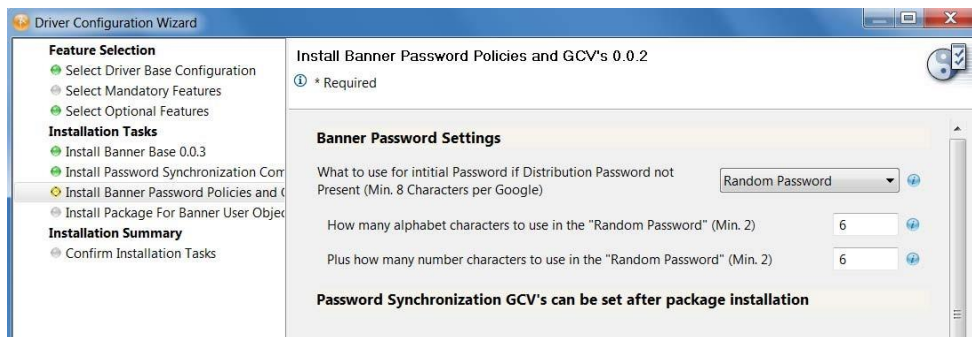
9 Configure the settings for User Objects..

- ◆ **Attribute used to match Banner Users with eDirectory Users** Select the attribute to use as the matching attributes.

  - ◆ **UDCIdentifier** Select this UDCIdentifier to use Banner's unique object ID as the matching value.

  - ◆ **CN** Select CN to use the CN as the matching attribute.

- ◆ **CN Format** CN Format lets you select from a set of pre-defined patterns for constructing the new user's CN.

  - ◆ UDCIdentifier

  - ◆ First Initial + Last Name

  - ◆ First Name + Last Initial

  - ◆ First Name + Last Name

  - ◆ First Initial + Middle Initial + Last Name

  - ◆ Last Name + First Initial + Middle Initial

- ◆ **Set Unique ID attribute in eDirectory with generated CN value** Setting this to 'true' will cause the generated CN value to also be store in the Unique ID attribute.
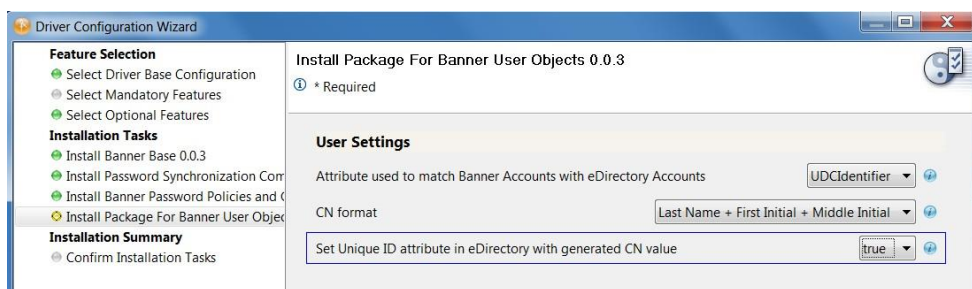
10 Review the Summary.

11 Select *Finish*.

NOTE: There is no screen during import to set authentication information. The Ellucian Banner driver requires separate server and authentication information for each channel.

3.1.3 Configuring the Driver

After importing the driver configuration file, you need to configure the driver before it can run. You should complete the following tasks to configure the driver:

- **Configure the driver properties:** There are many settings that can help you customize and optimize the driver. The settings are divided into categories such as Driver Configuration, Engine Control Values, and Global Configuration Values (GCVs). Although it is important for you to understand all of the settings, your first priority should be to review the Appendix A, "Driver Properties," on page 31 located on the Driver Configuration page. The Driver Parameters and the Global Configuration Values let you configure the Ellucian Banner login information and security credentials, and other parameters associated with the Publisher channel. These settings must be configured properly for the driver to start and function correctly. If you do not have the Driver Properties page displayed in Designer:

1 Open your project.

2 In the Modeler, right-click the driver icon or the driver connection, then select Properties.

3 Make any desired changes, then click OK to save the changes.

4 After the driver is created in Designer, it must be deployed to the Identity Vault. Proceed to Section 3.1.4, "Deploying the Driver," on page 20

- **Authentication:** This panel is not used by the Ellucian Banner driver. Leave it blank,

Driver Configuration

- **Configure the driver parameters:** The driver parameters panel contains driver-specific configuration.

  1. Driver Options The Ellucian Banner driver does not use any Driver Options. This panel is intentionally blank.

  2. Subscriber Options:

  - **URL of the remote Ellucian Banner server** Enter the IP address or URL of the BEIS listener.

    http://10.10.1.7:4041

    NOTE: If you are configuring the driver to use SSL the URL must contain a DNS name. For example: https://prod.bannerservice.com:4041

  - **Authentication ID** Enter the authentication ID the driver should use when authenticating to the BEIS listener.

  - **Authentication Password** Enter the password corresponding to the authentication ID.

  - **Proxy host and port** When a proxy host and port are used, specify the host address and the host port. For example: 192.10.1.3:18180. Choose an unused port number on your server. Otherwise leave this field blank.

3. **Publisher Options:**

- **Listening IP Address and Port** Specify the IP address of the server where this driver is installed and the port that this driver listens on as an SPML Server. You may specify 127.0.0.1 if there is only one network card installed in the server. Choose an unused port number on your server. For example: 127.0.0.1:18180. The driver listens on this address for SPML requests, processes them, and returns a result.

- **Require Authentication** Select *Show* to configure authentication information required by the Publisher channel.

- **Authentication ID** Specify the Authentication ID to validate incoming SPML requests.

- **Authentication Password** Specify the Authentication password to validate incoming SPML requests.

- **Accept HTTPS Connections** Select *Yes* to enable HTTPS connections.

- **KMO Name** When this server is configured to accept HTTPS connections, this is the KMO name in eDirectory. The KMO name is the name before the ' - ' in the RDN. Leave this field blank when a keystore file is used (see below) or when HTTPS connections are not used.

- **Keystore File** When this server is configured to accept HTTPS connections, this is the path and the name of the keystore file. For example: C:\security\keystore. Leave this field blank when a KMO name is used (see above) or when HTTPS connections are not used.

- **Keystore Password** When this server is configured to accept HTTPS connections, this is the keystore file password. Leave this field blank when a KMO name is used (see above) or when HTTPS connections are not used.

- **Server Key Alias** When this server is configured to accept HTTPS connections, this is the key alias. Leave this field blank when a KMO name is used (see above) or when HTTPS connections are not used.

- **Server Key Password** When this server is configured to accept HTTPS connections, this is the key alias password (not the keystore password). Leave this field blank when a KMO name is used (see above) or when HTTPS connections are not used.

- **Content Type** The HTTP request header will be set to this value on publisher results that are sent back to the requester.

- **Heartbeat Interval:** Specify the length of time in seconds the between heartbeats emitted by the Ellucian Banner driver's publisher channel.

- **Global Configuration Values (GCVs)**

    The GCVs are defined in

After completing the configuration tasks, continue with .

3.1.4   Deploying the Driver

After the driver is created in Designer, it must be deployed into the Identity Vault.

1 In Designer, open your project.

2 In the Modeler, right-click the driver icon or the driver connection, then select Live > Deploy.

3 Read through the deployment summary, and then click Deploy.

4 Read the success message, and then click OK.

5 Click Define Security Equivalence to assign rights to the driver.

The driver requires rights to objects within the Identity Vault. Create a user in eDirectory for the driver to use. Assign that user administrative rights to the objects that it will need to manage objects in eDirectory.

NOTE: Setting the Driver object's Security Equivalence directly to the admin user is not recommended. Also, creating a new user for the driver and setting the new user object's Security Equivalence to the Admin user is not recommended. Best practice is to assign specific administrative rights as needed by the driver to a user object created for the driver.

   5a Click Add, then browse to and select the object with the correct rights.

   5b Click OK twice.

6 Click Exclude Administrative Roles to exclude users that should not be synchronized.

   6a Click Add, then browse to and select the user object you want to exclude.

   6b Click OK.

   6c Repeat Step 6a and 6b for each object you want to exclude.

   6d Click OK.

7 Click OK

3.1.5 Extending the Schema

Extending the schema is done to synchronize the identity information of user provisioning in Ellucian HE in the existing eDirectory class USER which has been modified and following attributes have been added.

Attribute Name	Definition	Syntax	Type
udcMiddleName	Stores the middle initial, or part of the middle name.	CASE_IGNORE_ STRING	Single-valued attribute. **8** characters are stored for this attribute.
udcGender	Stores the gender: male, female, unknown.	CASE_IGNORE_ STRING	Single-valued attribute.
udcBirthDate	Stores the birthdate: mmddyy	CASE_IGNORE_ STRING	Single-valued attribute.
udcTaxID	Stores a number. This could be the Social Security number.	CASE_IGNORE_ STRING	Single-valued attribute.
udcIdentifier	A unique key to identify the individual in the Ellucian system. The driver uses this as the association key to facilitate using AccessManager to secure Ellucian's web applications.	CASE_IGNORE_ STRING	Single-valued attribute.
udcInstitutionalRoles	Role information from Ellucian HE.	CASE_IGNORE_ STRING	Multi-valued attribute.

Attribute Name	Definition	Syntax	Type
udcHomeSA	Home Street Address	CASE_IGNORE_ STRING	Single-valued attribute

3.1.6 Understanding Institutional Roles

Ellucian provides access to applications and data by the roles applied to the people in the Higher Education Institution. Any given person might have a number of roles. For example, a university student might also be a staff member. Ellucian provides 40 roles and also allows the users to add their own roles. The following list is some of the roles that Ellucian provides:

- PROSPECTIVE
- PROSPECTIVESTUDENT
- APPLICANT
- INSTITUTIONACCEPT
- APPLICANT ACCEPT
- STUDENT
- ALUMNI
- FRIENDS
- STAFF
- DEVELOPMENTOFFICER
- FINANCE
- FACULTY
- BANNERINB

See the Ellucian HE Banner Identity Handbook for a complete list of Ellucian roles, their description and possible uses.

Role Attributes

Role	Description	
Role Name	Specifies the name of the Ellucian Role.	Required.
Context	The name of the Ellucian component or system that created the role. Ellucian always sets Context to INTCOMP.	Optional.
Institution Name	If present, it identifies the institution for which this role applies.	Optional

How Institutional Roles Work

Ellucian HE does not delete users from their system. Instead, roles are added to and removed from a user to represent their access rights. A user with no roles has no access to Ellucian applications or resources. Access to resources is based on the presence of roles. Therefore, the driver synchronizes all Role information to the udcInstitutionalRoles attribute in the Identity Vault. For each XML document Ellucian sends to the driver publisher channel, a complete list of the current roles on that user is provided. The driver publishes a `<remove-all-values>` command to clear the udcInstitutionalRoles attribute before publishing the new list of roles it received from Ellucian HE.

How Roles are Stored in udcInstitutionalRoles

UdcInstitutionalRoles is a multi-valued attribute and can contain a list of roles. The three role attributes are stored in a single value, separated by semicolons. The format is: `<Role Name>;<Context>;<Institution Name>`.

Role Name is a required attribute. Context is an optional attribute. It is delimiting. A semi-colon is present even if the attribute is empty. Institution Name is also an optional attribute.

For example, given a role of BasicPerson issued from Banner at Out Of State University, the driver will generate the following:

```
<add-attr attr-name="InstitutionRoles">
  <value>BASICPERSON;Banner;OutOfStateU</value>
</add-attr>
```

3.1.7 Starting the Driver

When a driver is first created, it is the stopped by default. Start the driver in order to begin synchronizing data between Banner and eDirectory. Identity Manager is an event-driven system, so after the driver is started, it will wait for events to be sent from BEIS or eDirectory for processing.

To start the driver:

1 In Designer, select the project view.

2 Click on the Ellucian Banner driver.

3 Click the green start icon.

3.2 Activating the Driver

If you created the Ellucian Banner driver in a driver set that has not been activeate, you must activate the driver with a Ellucian Banner Driver activation within 90 days. If you do not apply a Ellucian Banner Driver activation within 90 days, the driver will stop working.

For more information on activation, refer to "Activating Novell Identity Manager Products" in the Identity Manager 4.0 Framework Installation Guide.

For information on activation, refer to "Activating Novell Identity Manager Products" in the *Identity Manager 4.0 Framework Installation Guide*.

3.3 Ellucian Banner Requirements

In order for the driver to interact with your Ellucian Banner system the Banner Enterprise Integration Server (BEIS) needs to be configured. Configuring BEIS is outside the scope of this document.

4 Customizing the Driver

The following sections provide information to help you understand what the driver does and what customization you might need to make to the driver:

4.1 Managing the Driver

As you work with the Ellucian Banner driver, there are a variety of management tasks you might need to perform, including the following:

- Starting, stopping, and restarting the driver
- Viewing driver version information
- Using Named Passwords to securely store passwords associated with the driver
- Monitoring the driver's health status
- Backing up the driver
- Inspecting the driver's cache files
- Viewing the driver's statistics
- Using the DirXML Command Line utility to perform management tasks through scripts
- Securing the driver and its information

Because these tasks, as well as several others, are common to all Identity Manager drivers, they are included in one reference, the *Identity Manager 4.0 Common Driver Administration Guide*.

4.2 Schema Mapping

This section details the default schema mapping of the driver. The schema map details how IDV attributes and classes are translated into Ellucian Banner attributes and classes.

The Ellucian Banner driver interacts with Ellucian Banner through the Banner Enterprise Integration Server (BEIS). BEIS uses the UDCIdentity schema to represent user object in the Banner system. UDCIdentity is the minimal representation of a user object. It is possible to configure BEIS to include additional Banner attributes as extension attributes in the SPML documents emitted by BEIS. The Banner driver will process these through as <add-attr> tags, however the attribute name will need to be added to the schema-map and driver filter in order to be process through to the Identity Vault.

4.2.1 User Attributes Mapping

IDVault	Ellucian Banner UDCIdentity
User	UDCIdentity
udcIdentifier	UDCIdentifier
Full Name	FormattedName
	LegalName
Given Name	GivenName
	PreferredGivenName
udcMiddleName	MiddleName
Surname	FamilyName
personalTitle	Prefix
Generational Qualifier	Suffix
udcGender	Gender
udcBirthdate	Birthdate
	Birthdate:Day
	Birthdate:Month
	Birthdate:Year
udcTaxID	TaxId
InternetEmailAddress	EmailAddress
	PrimaryAddress
co	PrimaryAddress:CountryCode
homeZipCode	PrimaryAddress:PostalCode
homeState	PrimaryAddress:Region
homeCity	PrimaryAddress:Municipality
udcHomeSA	PrimaryAddress:AddressLine
	CampusAddress
	CampusAddress:CountryCode
Postal Code	CampusAddress:PostalCode
S	CampusAddress:Region
Physical Delivery Office Name	CampusAddress:Municipality
SA	CampusAddress:AddressLine
Telephone Number	CampusPhone
	CampusPhone:InternationalCountryCode

IDVault	Ellucian Banner UDCIdentity
	CampusPhone:NationalNumber
	CampusPhone:AreaCityCode
	CampusPhone:SubscriberNumber
	CampusPhone:Extension
mobile	MobilePhone
	MobilePhone:InternationalCountryCode
	MobilePhone:NationalNumber
	MobilePhone:AreaCityCode
	MobilePhone:SubscriberNumber
	MobilePhone:Extension
Fascimile Telephone Number Fax	
	Fax:InternationalCountryCode
	Fax:NationalNumber
	Fax:AreaCityCode
	Fax:SubscriberNumber
	Fax:Extension
udcInstitutionalRoles	InstitutionRoles

A Driver Properties

This section provides information about the Driver Configuration and Global Configuration Values properties for the Ellucian Banner driver. These are the only unique properties for drivers. All other driver properties (Named Password, Engine Control Values, Log Level, and so forth) are common to all drivers. Refer to "Driver Properties" in the *Identity Manager 4.0 Common Driver Administration Guide* for information about the common properties.

The information is presented from the viewpoint of Identity Console. If a field is different in Designer, it ismarked with an 🟠 icon.

A.1 Driver Configuration

In Identity Console:

1 Click *IDM Administration*.
2 Select the driver set that contains the driver whose properties you want to edit.
3 Click the driver icon to display the driver's properties
   page.

In Designer:

1 Open a project in the Modeler.
2 Right-click the driver icon or line, then select click *Properties > Driver Configuration.*

The Driver Configuration options are divided into the following sections:

A.1.1 Driver Module

The driver module changes the driver from running locally to running remotely or the reverse.

Table A-1 *Driver Module*

Option	Description

Java	Used to specify the name of the Java class that is instantiated for the shim component of the driver. This class can be located in the `classes` directory as a class file, or in the `lib` directory as a `.jar` file. If this option is selected, the driver is running locally.
	
	The Java class name is:
	
	`com.novell.nds.dirxml.driver.sungardbannershim.SungardBa`
	`nnerDriverShim`

Native	This option is not used with the Ellucian Banner driver.
Connect to Remote Loader	Used when the driver is connecting remotely to the connected system. Designer includes two suboptions: ◆ 🌕 *Driver Object Password*: Specifies a password for the Driver object. If you are using the Remote Loader, you must enter a password on this page. Otherwise, the remote driver does not run. The Remote Loader uses this password to authenticate itself to the remote driver shim. ◆ 🌕 *Remote Loader Client Configuration for Documentation*: Includes information on the Remote Loader client configuration when Designer generates documentation for the driver.

A.1.2 Driver Object Password

Table A-2 *Driver Object Password*

Option	Description
Driver Object Password	Use this option to set a password for the driver object. If you are using the Remote Loader, you must enter a password on this page or the remote driver does not run. This password is used by the Remote Loader to authenticate itself to the remote driver shim.

A.1.3 Authentication

The authentication section stores the information required to authenticate to the connected system.

Table A-3 *Authentication*

Option	Description
Authentication ID or 🌕 *User ID*	The Ellucian Banner driver uses separate authentication configurations for each channel. The driver does not use this Authentication information. Leave it blank.

Option	Description
Authentication Context or 🟠 *Connection Information*	The Ellucian Banner driver uses separate authentications for each channel. Leave this parameter blank.
Remote Loader Connection Parameters or 🟠 *Host name* 🟠 Port 🟠 KMO 🟠 *Other parameters*	Used only if the driver is connecting to the application through the remote loader. The parameter to enter is `hostname=xxx.xxx.xxx.xxx port=xxxx kmo=certificatename`, when the host name is the IP address of the application server running the Remote Loader server and the port is the port the remote loader is listening on. The default port for the Remote Loader is 8090. The `kmo` entry is optional. It is only used when there is an SSL connection between the Remote Loader and the Metadirectory engine. Example: `hostname=10.0.0.1 port=8090 kmo=IDMCertificate`
Driver Cache Limit (kilobytes) or 🟠 *Cache limit (KB)*	Specify the maximum event cache file size (in KB). If it is set to zero, the file size is unlimited. 🟠 Click *Unlimited* to set the file size to unlimited in Designer.
Application Password or 🟠 *Set Password*	This option is not used with the Ellucian Banner driver.
Remote Loader Password or 🟠 *Set Password*	Used only if the driver is connecting to the application through the Remote Loader. The password is used to control access to the Remote Loader instance. It must be the same password specified during the configuration of the Remote Loader on the connected system.

A.1.4   Startup Option

The Startup Option section allows you to set the driver state when the Identity Manager server is started.

Table A-4   *Startup Option*

Option	Description
Auto start	The driver starts every time the Identity Manager server is started.
Manual	The driver does not start when the Identity Manager server is started. The driver must be started through Designer or Identity Console
Disabled	The driver has a cache file that stores all of the events. When the driver is set to Disabled, this file is deleted and no new events are stored in the file until the driver state is changed to Manual or Auto Start.
🟠 *Do not automatically synchronize the driver*	This option only applies if the driver is deployed and was previously disabled. If this is not selected, the driver re-synchronizes the next time it is started.

A.1.5 Driver Parameters

The Driver Parameters section allows you to configure the driver-specific parameters. When you change driver parameters, you tune driver behavior to align with your network environment. For example, you might find the default Publisher polling interval to be shorter than your synchronization requires. Making the interval longer could improve network performance while still maintaining appropriate synchronization.

Option	Description
Driver Name	The name of the driver contained in the driver configuration file is `Ellucian Banner`. Specify the actual name you want to use for the driver.
Driver is Local or Remote	Configure the driver for use with the Remote Loader service or daemon by selecting Remote, or select Local to configure the driver for local use. If Local is selected, the remaining prompts are not displayed.
Driver Password	For remote driver configuration only.
	The driver object password is used by the Remote Loader to authenticate to the Identity Manager server. It must be the same password that is specified in the Driver Object Password field on the Identity Manager Remote Loader.
URL of the Remote Ellucian Banner Server	Specify the URL for the remote Ellucian Banner server.
Authentication ID	Specify the Authentication ID for the remote Ellucian Banner server.
Authentication Password	Specify the Authentication Password for the remote Ellucian Banner server.
Proxy Host and Port	Specify the host address and the host port when a proxy host and port are used.
HTTP Errors to Retry	List the HTTP error codes that should return a retry status.
Customize HTTP Request-Header Fields	Select *Show* if you want to set mutual authentication information.
Listening IP Address and Port	Specify the IP address of the server where this driver is installed and the port number this driver listens on as an SPML server.
Require Authentication	The *basic* authentication scheme requires a user-ID and password.
Authentication ID for incoming SPML requests	Specify the Authentication ID to validate incoming SPML requests.
Authentication Password for incoming SPML requests	Specify the Authentication password to validate incoming SPML requests.
Accept HTTPS Connections	Indicates if the driver accepts HTTPS connections from Ellucian Banner.

Option	Description
KMO Name	When the server is configured to accept HTTPS connections, this is the KMO name in eDirectory.
Keystore File	When the server is configured to accept HTTPS connections, this is the path and name of the keystore file.
Keystore Password	When the server is configured to accept HTTPS connections, this is the keystore file password.
Server Key Alias	When the server is configured to accept HTTPS connections, this is the key alias.
Server Key Password	When the server is configured to accept HTTPS connections, this is the key alias password, not the keystore password.
Content-Type	The HTTP request header will be set to this value on publisher results that are sent back to the requester.
Heartbeat Interval in Minutes	Specify the heartbeat interval in minutes.

A.2 Global Configuration Values

Global configuration values (GCVs) are values that can be used by the driver to control functionality. GCVs are defined on the driver or on the driver set. Driver set GCVs can be used by all drivers in the driver set. Driver GCVs can be used only by the driver on which they are defined.

The Ellucian Banner driver includes several predefined GCVs. You can also add your own if you discover you need additional ones as you implement policies in the driver.

To access the driver's GCVs in Identity Console:

1 Click the *IDM Administration* tile.

2 Select the driver set that contains the driver whose properties you want to edit.

3 Locate the Active Directory driver icon, then click the driver icon to display the driver's properties page.

4 Click *Global Config Values* drop down to display the GCV page.

To access the driver's GCVs in Designer:

1 Open a project in the Modeler.

2 Right-click the driver icon or line, then select *Properties > Global Configuration Values.*

or

To add a GCV to the driver set, right-click the driver set icon , then click *Properties > GCVs*.

Table A-5 *Global Configuration Values*

Name	Description	Example Value
Banner Password Settings		
What to use for intitial Password if Distribution Password not Present	If the system is not set up for universal password synchronization or the user account just doesnt have a distribution password set yet, then an initial password has to be set. This GCV tells the system whether to use an attribute off of the user account for an initial password or to use a random generated password. If the accounts are going to use SAML for authentication then a Random Password would be fine. Otherwise an attribute value should be selected.	*Random Password* or *Attribute Value from User* **NOTE:** The attribute name must be specified in eDirectory namespace. The Banner attribute which contains the password value needs to be mapped to the eDirectory attribute name. The attribute should be marked as Notify in the driver filter to prevent the password value from being written to eDirectory.
eDirectory attribute to use for initial password value.	This is the name of the attribute in edirectory that the Ellucian Banner driver should use for an initial password if no Distribution password is available on creation.	Surname
Number of letters to use in the Random Password	This is the number of Letters to use in the random password. when added to the value of the "Random password numbers" GCV It will determine the number of characters in the total Length	6
Number of numbers to use in the Random Password	This is the number of numbers to use in the random password. when added to the value of the "Random password letters" GCV It will determine the number of characters in the total Length.	6
User Settings		
Attribute used to match Banner users to eDirectory users.	This GCV allows selection of the attribute used by the driver's matching policy.	*UDCIdentifier* causes the matching rule to match objects using the UDCIdentifier. This is a unique ID generated by Banner *CN* causes the matching rule to use the CN
CN Format	This GCV contains a set of patterns that can be used to generate a new User's CN	◆ UDCIdentifier ◆ First Initial + Last Name ◆ First Name + Last Initial ◆ First Name + Last Name ◆ First Initial + Middle Initial + Last Name ◆ Last Name + First Initial + Middle Initial

Name	Description	Example Value
Set Unique ID attribute in eDirectory with generated CN value	If set to *true* then the CN value on new users will be copied to the eDirectory Unique ID attribute	*true* or *false*

A.3 Extension Attributes

BEIS is configured to publish objects based on the UDCIdentity schema. All attributes of the UDCIdentity which are present on the user are published in the SPML document. Additionally, BEIS can be configured to publish other Banner attributes on Banner user objects.

The Banner driver publishes extension attributes like any other UDCIdentity schema element.

For example, given a Banner extension attribute named GORMAL_EMAIL_ADDRESS with a value of bob@outofstate.edu, the driver will generate the following:

```
<add-attr attr-name="GOREMAL_EMAIL_ADDRESS">
  <value>bob@outofstate.edu</value>
</add-attr>
```

 Since the driver only reports UDCIdentity attributes in response to a schema request extension attributes don't show up by default in the schema map. They will need to be added by hand. In a future release the driver will 'learn' about extensions and report them when schema is requested.

B Securing the Driver

`Banner Enterprise Identity Server` (BEIS) can be configured to use SSL. You can configure the driver to accept HTTPS connections and take advantage of this increased security.

IMPORTANT: Only certificates from a Java keystore are accepted. Make sure that the keystore for the certificates is a Java keystore.

The following sections provide instructions for creating a secure connection:

B.1 Configuring the Publisher Channel

1 Create a server certificate using keytool.

For more information on keytool, see Keytool - Key and Certificate Management Tool (http://java.sun.com/j2se/1.4.2/docs/tooldocs/windows/keytool.html)

. `keytool -genkey -keyalg RSA -alias selfsigned -keystore key_store_file_name -storepass password -validity 360 -keysize 2048`

For Example: `keytool -genkey -keyalg RSA -alias selfsigned -keystore keystore.jks -storepass changeit -validity 360 -keysize 2048`

You will be prompted for the following information:

- **What is your first and last name?**

  This becomes the CN of your certificate. Enter the DNS name of the server running the driver.

- **What is the name of your organizational unit?**

  Enter the name of your organizational unit. This information does not need to correlate to any information in eDirectory or DNS.

- **What is the name of your organization?**

  Enter the name of your organization. This information does not need to correlate to any information in eDirectory or DNS.

- **What is the name of your city or locality?**

  Enter the name of your city. This information does not need to correlate to any information in eDirectory or DNS

- **What is the name of your state or province?**

  Enter the name of your state. This information does not need to correlate to any information in eDirectory or DNS

         ◆ **What is the two-letter country code for this unit?**

         Enter the code for your country. This information does not need to correlate to any information in eDirectory or DNS

      keytool will present a summary of your information and ask if it is correct. Press Y.

2 Configure the Publisher Channel to use the server certificate created in Step 1 on page 39

    2a In Designer, right click on the driver and select *Properties.*

    2b On the Properties dialog, select *Driver Configuration*

    2c On Driver Configuration select the *Driver Parameters* tab.

    2d On the Driver Parameters tab select the *Publisher Options* tab.

    2e On *Accept HTTPS Connections* select *Yes.*

    2f Enter the path and filename of the keystore you created in Step 1 on page 39. For example, enter c:\keystore.jks.

    2g Enter the password of the keystore you created in Step 1 on page 39. For example, enter changeit.

    2h Enter the server key alias of the key you created in Step 1 on page 39. For example, enter selfsigned.

    2i Enter the password for the server certificate you created in Step 1 on page 39. For example, enter changeit.

3 Click *Okay* to save your changes.

B.2   Configuring the Subscriber Channel

The Subscriber Channel sends information from the Identity Vault to Banner via the Banner Enterprise Identity Server. To establish a secure connection you need a trust store containing a certificate issued by the certificate authority that signed the BEIS server certificate. You will need to obtain this certificate from a BEIS administrator.

1 Make sure you have a certificate signed by the certificate authority from the BEIS administrator

2 Import the certificate into your trust store, or create a new trust store by entering the following command at the command prompt: `keytool -import - file name_of_cert_file - trustcacerts -noprompt -keystore filename`

`-storepass password`

   For Example: `keytool -import - file beis_cert.b64 -trustcacerts -noprompt - keystore dirxml.keystore`

`-storepass changeit`

   For more information on keytool, see Keytool - Key and Certificate Management Tool (http:// java.sun.com/j2se/1.4.2/docs/tooldocs/windows/keytool.html)

3 Configure the Subscriber Channel to use the trust store created in Step 2

    3a In Identity Console, in the *Roles and Tasks*view, click *Identity Manager > Identity Manager Overview.*

    3b Locate the driver set containing the Ellucian Banner Driver. Then click the driver's icon to display the Identity Manager Driver Overview page.

3c On the Identity Manager Driver Overview page, go to configuration tab. and

3d Click *Driver parameter* dropdown and go to *Subscriber Settings.*

3d In the *Keystore File* setting, enter the path to the trust store you created in Step 2.

4 Click *Apply,* then click *Okay.*