NetIQ® Identity Manager

Driver for Blackboard REST Implementation Guide

July, 2023

Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION AND OMNIBOND SYSTEMS, LLC. PROVIDE THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation and Omnibond Systems, LLC., except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation and Omnibond Systems, LLC. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation and Omnibond Systems, LLC. may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government’s rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/.

Contents

About this Book and the Library

This *Implementation Guide* explains implementation of the NetIQ® Identity Manager 4.8 driver for Blackboard REST.

The driver enables you to synchronize data in the Identity Vault to data stored in a Blackboard system. This configurable solution allows you to increase productivity and streamline business processes by integrating Blackboard with your other IT systems.

Intended Audience

Driver for Blackboard Implementation Guide was created for the following audiences:

- System administrators

The Blackboard driver is aimed at information technology professionals who:

- Are familiar with Identity Manager and NetIQ eDirectory™
- Are familiar with the administration of systems and platforms you connect to Identity Manager

Other Information in the Library

The library provides the following information resources:

Identity Manager Setup Guide

Provides overview of Identity Manager and its components. This book also provides detailed planning and installation information for Identity Manager.

Designer Administration Guide

Provides information about designing, testing, documenting, and deploying Identity Manager solutions in a highly productive environment.

User Application: Administration Guide

Describes how to administer the Identity Manager User Application.

User Application: User Guide

Describes the user interface of the Identity Manager User Application and how you can use the features it offers, including identity self-service, the Work Dashboard, role and resource management, and compliance management.

User Application: Design Guide

Describes how to use the Designer to create User Application components, including how to work with the Provisioning view, the directory abstraction layer editor, the provisioning request definition editor, the provisioning team editor, and the role catalog.

Identity Reporting Module Guide

Describes the Identity Reporting Module for Identity Manager and how you can use the features it offers, including the Reporting Module user interface and custom report definitions, as well as providing installation instructions.

Analyzer Administration Guide

Describes how to administer Analyzer for Identity Manager.

Identity Manager Common Driver Administration Guide

Provides information about administration tasks that are common to all Identity Manager drivers.

Identity Manager Driver Guides

Provides implementation information about Identity Manager drivers.

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. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions 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

Qmunity, 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, Qmunity 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 Understanding the Blackboard Driver

The NetIQ® Identity Manager 4.8 driver for Blackboard lets you synchronize data in the Identity Vault to data stored in a Blackboard Learn implementation. Prior to 4.8, the Blackboard Driver used Java Snapshot APIs to integrate directly on the Blackboard system. In 4.8, the architecture was significantly changed in order to support the latest integration techniques recommended by Blackboard. As a result, you no longer need to install the driver directly on the Blackboard system. This change allows for both on-premise and cloud-based configurations.

The Subscriber channel receives XDS command documents for users and groups from the Identity Manager Metadirectory engine, converts them to Blackboard REST API calls, and executes them. The Publisher channel is not implemented at this time.

The Subscriber channel does not perform validation of attribute values in the XDS command document. If the requirements of Blackboard are not met, the results of the Blackboard REST API calls are unpredictable. Exceptions detected by the Blackboard REST API bubble up to the driver trace to assist in troubleshooting data validity problems.

The following sections provide a basic overview of the driver:

- “Version Support” on page 9
- “Blackboard Driver Concepts” on page 9
- “Support for Standard Driver Features” on page 11
- “Differences Between eDirectory and Blackboard” on page 12

Version Support

The Blackboard driver requires Identity Manager 4.8 or greater and Blackboard 9.1 or greater.

Blackboard Driver Concepts

The following sections explain concepts you should understand before implementing the Blackboard driver:

- “Default Data Flow” on page 10
- “Policies” on page 10
- “Driver Components” on page 11

Default Data Flow

A channel is a combination of rules, policies, and filters that is used to synchronize data between two systems. The Subscriber and Publisher channels describe the direction in which the data flows. The Subscriber and Publisher channels act independently; actions in one channel are not affected by what happens in the other.

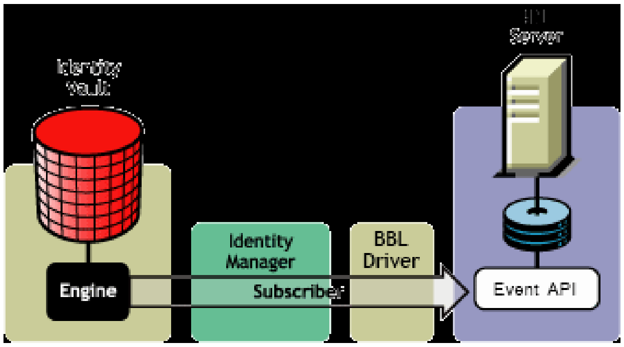
- "Subscriber Channel" on page 10
- "Publisher Channel" on page 10

Subscriber Channel

The Subscriber channel is the channel of communication from the Identity Vault to Blackboard. The channel takes events generated in the Identity Vault and sends them to the Blackboard system. The Subscriber channel also supports queries into Blackboard.

Figure 1-1 illustrates this data flow.

Figure 1-1 *Data Flow Through The Subscriber Channel*



The driver can be configured to work with Blackboard, versions 9 and later.

Publisher Channel

The Publisher channel is not implemented.

Policies

Policies are used to control the synchronization of data between the Identity Vault and Blackboard. The Blackboard driver is designed to be used with Identity Manager 4.8 Packages, but for backward compatibility the policies have been provided in an XML preconfiguration document. For information about the policies installed in the preconfiguration, see Appendix A, "Policies," on page 39. All policies contained in the Packages are included in the preconfiguration file for Identity Manager 3.6.

Driver Components

The driver contains the following components:

- **Default Driver Configuration File for Identity Manager 4.8:** A file you can import to set up default rules, style sheets, and driver parameters. The driver configuration file included with this driver is `BlackboardRESTDriver.xml`.
- **Driver Shim Installation File:** `linux_x86_64_bbdriver_install.bin`
- **Schema File:** `blackboard.sch` contains optional schema extensions to be used with the Blackboard driver.

Support for Standard Driver Features

The Blackboard driver is designed to be run as a Remote Loader Service only.

The following sections provide information about how the driver supports standard driver features:

- "Entitlements" on page 11
- "Schema" on page 11
- "Object Classes" on page 11
- "Configuration" on page 11

Entitlements

The Blackboard driver can be configured to use entitlements to manage user accounts in Blackboard. When using entitlements, this driver works in conjunction with external services, such as the User Application with workflow or role-based provisioning or the Entitlements Service driver, to manage entitlement functionality.

Schema

The Blackboard driver uses the Blackboard schema to describe the attributes of Person, Course, Organization, and Enrollment objects in Blackboard. Optional schema definitions for the Blackboard driver are included in the `blackboard.sch` file.

Object Classes

The Blackboard driver provides auxiliary classes that can be used to add Blackboard-specific schema attributes to User and Group objects in eDirectory. Optional schema definitions for the Blackboard driver are included in the `blackboard.sch` file.

Configuration

The behavior of an Identity Manager driver is governed by its configuration of options, policies, and filters. The configuration of the Blackboard driver is managed by several packages that can be installed and configured using Designer for Identity Manager.

Differences Between eDirectory and Blackboard

Organization

Blackboard is similar to eDirectory in the way information is organized with the exception of Blackboard Enrollments.

User objects in eDirectory map directly to Person objects in Blackboard. Group objects in eDirectory map directly to Course and Organization objects in Blackboard. Course and Organization objects are differentiated by the NTIQBBRTDC-sub-evt-DetermineBBObjectType Event Transform Policy. Blackboard Enrollments have additional attributes that eDirectory Group memberships do not support. In order to support Blackboard Enrollments, use the Group Member and Owner attributes to represent enrollments in Blackboard. The disadvantage of using the Member and Owner attributes is that enrollments can only be removed rather than being disabled.

While eDirectory is hierarchical, Blackboard is flat—there is no concept of a move function. The Subscriber channel rejects move commands. The sample Subscriber Event policy vetoes move events. You can change this policy to perform installation-specific processing of move events if required.

User object deletions in eDirectory result in the associated Person object in Blackboard being deleted. Group object deletions in eDirectory result in the associated Course or Organization object in Blackboard being deleted. There is no concept of rename in Blackboard. Blackboard is not hierarchical. There is no move function.

Passwords

Identity Manager uses the nspmDistributionPassword attribute to provide passwords from eDirectory. The mapping policy in the preconfigured sample policies maps nspmDistributionPassword to DirXML-BB-p-password.

2 Installing the Driver For Your Blackboard System

The NetIQ® Identity Manager 4.8 driver for Blackboard consists of the Blackboard Driver Shim installed on a Linux server.   This could be the Metadirectory server. The Driver Shim provides the conduit for information transfer between eDirectory (through Identity Manager) and the Blackboard system.

The Driver Shim should be installed on a supported Linux server to connect to the Blackboard Learn application using the Blackboard REST API. Any Linux system compatible with the Identity Manager engine requirements is supported.

This section provides the information you need for first-time installation of the NetIQ® Identity Manager 4.8 driver for Blackboard. Topics include:

Before You Begin

Before you install the NetIQ Identity Manager Driver for Blackboard in a production environment:

- You should install the driver in a test environment for use in developing your full deployment plan.
- Ensure that you have the most recent distribution, support pack, and patches for the driver.
- Review the most recent support information for the driver on the NetIQ Support Web site (http://support.netiq.com).

Required Knowledge and Skills

Although different tasks can be performed by different people, your installation and deployment team must collectively have expertise with eDirectory, Designer, Identity Console, Identity Manager, Blackboard, and XSLT.

Full administrative rights are required, both in eDirectory and on Blackboard.

For an overview of driver facilities, see Chapter 1, "Understanding the Blackboard Driver," on page 9.

Getting the Installation Files

Obtain the most recent distribution of the Identity Manager 4.8 Driver for Blackboard from the NetIQ Downloads Web site (https://dl.netiq.com/index.jsp).

At the time of this *Implementation Guide*'s release, the 4.8 driver was included in the following Field Patch, available for public download:

- `IDM 4.8 Blackboard 4.8.0.0`

Installation Tasks

Installing the Driver Shim on the Linux Server

1 Log in to the target Linux server as root.

2 Make sure Perl 5 is installed.

  2a On Red Hat, `yum install perl`

  2b On SLES, `zypper install perl`

3 Install the required Perl modules through your package manager, or use `yum install` on Red Hat and `zypper install` on SLES systems:

  - `perl-JSON`
  - `perl-JSON-XS`
  - `perl-libwww-perl`

  NOTE: For Red Hat 8.1, you will also need to install `perl-LWP-Protocol-https`.

4 If any of the Perl Modules are not available through your system package manager, they may also be installed through CPAN:

  - `cpan JSON`
  - `cpan JSON::XS`
  - `cpan LWP::UserAgent`

5 Obtain the `linux_x86_64_bbdriver_install.bin` file from your installation media and execute this self-extracting file on your Linux system.

6 Specify the language choice.

7 Read and accept the license agreement.

8 After the package is installed onto your system, you are prompted to enter Driver and Remote Loader passwords. These passwords are used to verify that an authorized driver shim is communicating with the Identity Manager engine. Follow the prompts:

  8a Enter and confirm the Remote Loader Password.

  8b Enter and confirm the Driver Object password.

9 Next, you are prompted to retrieve an SSL certificate. NetIQ eDirectory must be running to retrieve the certificate. The certificate allows SSL encryption between the Identity Manager engine and the driver shim. Enabling SSL is optional, but is recommended for better security. To retrieve the certificate, follow the prompts:

   9a Specify the DNS name or IP Address of your eDirectory server.

   9b Specify the LDAP secure port, default 636.

   9c Enter **Y** to accept the certificate.

10 The installation of the driver shim is finished, with the option of starting the Driver Shim Service. Proceed to the next section to complete the installation of the driver.

Extending the Schema for Identity Manager

If you plan on using the Identity Vault to manage connected system attributes that are not already mapped to standard eDirectory™ attributes, you will need to extend the schema. Otherwise, it is not necessary.

Extending the schema adds auxiliary classes to eDirectory User and Group objects for Blackboard user and group attributes. It also extends the schema for an effective class called DirXML-BB-Enrollment that can be used to represent an enrollment in a Blackboard Course or Organization.

To extend the schema, using the `Import Conversion Export Utility (ICE)` Command Line Interface:

1 Obtain the `blackboard.sch` file for browser access, depending on the operating system you are running:

   - **Linux:** Use the `blackboard.sch` file from `/opt/novell/eDirectory/lib/lib/nds-schema/` or obtain a copy from the `Metadirectory` directory in the ISO image or patch download.

     Windows: Copy the `blackboard.sch` file from the `Metadirectory` directory in the ISO image or patch download.

2 Open a Terminal on your eDirectory server.

3 Run the ice command using the following syntax:

```
ice -S LDIF -f blackboard.sch -D LDAP -s <host> -p <port> -d <admin> -W
```

The `host` option specifies the DNS name or IP address of the LDAP server. The default is localhost.

The `port` option specifies the integer port number of the LDAP server specified by host. The default is 389. For secure operations, the default port is 636.

The `admin` option specifies the distinguished name of the entry that should be used when binding to the server-specified bind operation.

NOTE: For a complete list of options, please see the **Import Conversion Export Utility** section of the eDirectory Administration Guide.

Configuring the REST API on your Blackboard Learn Instance

1 Setup a Blackboard Learn Application Key and Secret for your installation.

1a Login to https://developer.blackboard.com. You may need to create an account.

1b Register a new application.

1c You will need to fill out the first three fields:

- **Application Name**: NetIQ Blackboard Driver
- **Description**: Provisions users and courses to Blackboard.
- **Domain(s)**: myschool.edu (This is the domain of your Blackboard server instance)

1d Once the API Key is generated, note the *Application Key*, *Secret* and *Application ID*.

2 Create a Blackboard Learn System Role for use by the driver.

3 Assign privileges to this System Role so that courses, organizations and users can be created, deleted and modified by the driver. Privileges required:

- Administrator Panel (Courses) > Courses
- Administrator Panel (Courses) > Courses > Create Course
- Administrator Panel (Courses) > Courses > Delete Courses
- Administrator Panel (Courses) > Courses > Edit
- Administrator Panel (Courses) > Courses > Edit > Enrollments
- Administrator Panel (Courses) > Courses > Edit > Enrollments > Add Enrollment
- Administrator Panel (Courses) > Courses > Edit > Enrollments > Delete Enrollment
- Administrator Panel (Courses) > Courses > Edit > Enrollments > Edit Enrollment
- Administrator Panel (Organizations) > Organizations
- Administrator Panel (Organizations) > Organizations > Create Organization
- Administrator Panel (Organizations) > Organizations > Delete Organization
- Administrator Panel (Organizations) > Organizations > Edit > Enrollments
- Administrator Panel (Organizations) > Organizations > Edit > Enrollments > Add Enrollment
- Administrator Panel (Organizations) > Organizations > Edit > Enrollments > Delete Enrollment
- Administrator Panel (Organizations) > Organizations > Edit > Enrollments > Edit Enrollment
- Administrator Panel (Users) > Users
- Administrator Panel (Users) > Users > Create User
- Administrator Panel (Users) > Users > Delete Users
- Administrator Panel (Users) > Users > Edit > Change Password
- Administrator Panel (Users) > Users > Edit > User Properties
- Administrator Panel (Users) > Users > Edit > View Course Enrollments
- Administrator Panel (Users) > Users > Edit > View Organization Enrollments

- Course/Organization Control Panel (Users and Groups) > Users > Remove Users from Course/Organization
- Course/Organization Control Panel (Users and Groups) > Users > Change User's availability in Course/Organization

4. Create a Blackboard Learn User for use by the driver and assign the System Role you created above.
5. Follow Blackboard's instructions to setup a REST integration: Blackboard REST Integration (https://help.blackboard.com/Learn/Administrator/Hosting/System_Integration/Compare_Building_Blocks_and_Rest#register-a-rest-integration-in-blackboard-learn_OTP-4)
   - Specify the user created in Step 2 as the Learn User for the REST Integration.

   NOTE: End User Access should be set to No.

   - Enter the *Application ID* from **Step 1**.

Post-Installation Tasks

Once you have installed and configured the driver software on your Blackboard system, do the following:

1. Start the driver shim process with this command: `/etc/init.d/bbdrvd start`
2. Follow the directions in Chapter 3, "Creating a New Driver," on page 19 to set up the corresponding representation of your driver in the Identity Vault.

Uninstalling the Driver

To uninstall the driver, use rpm to remove the package with the command: `rpm -e novell-DXMLbbdrv`

3 Creating a New Driver

After the driver files are installed on the Blackboard system where you want to run the driver (see Chapter 2, “Installing the Driver For Your Blackboard System,” on page 13), you can create the driver’s representation in the Identity Vault. You do so by importing the basic driver configuration file and then modifying the driver configuration to suit your environment. The following sections provide instructions:

- “Establishing a Security-Equivalent User” on page 19
- “Creating the Driver in Designer” on page 19
- “Activating the Driver” on page 26

Establishing a Security-Equivalent User

The driver must run with security equivalent to a user with sufficient rights. You can set the driver equivalent to ADMIN or a similar user. For a stronger security, you can define a user with only the minimal rights necessary for the operations you want the driver to perform.

The driver must be a trustee of the containers where synchronized identities reside, with the rights shown in Table 3-1. Inheritance must be set for [Entry Rights] and [All Attribute Rights].

Table 3-1

Operation	[Entry Rights]	[All Attribute Rights]
Subscriber notification of account changes (recommended minimum)	Browse	Compare and Read
Retrieving passwords from the Identity Vault	Browse and Supervisor	Compare and Read

Creating the Driver in Designer

You create the Blackboard driver in Designer by importing its basic configuration file and then modifying the configuration to suit your environment. After creating and configuring the driver, you need to deploy it to the Identity Vault and start it.

- “Importing the Current Driver Packages” on page 20
- “Installing the Driver Packages” on page 20
- “Configuring the Driver” on page 23
- “Deploying the Driver” on page 23
- “The Driver Shim Configuration File” on page 24
- “Starting the Driver” on page 26

Importing 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.

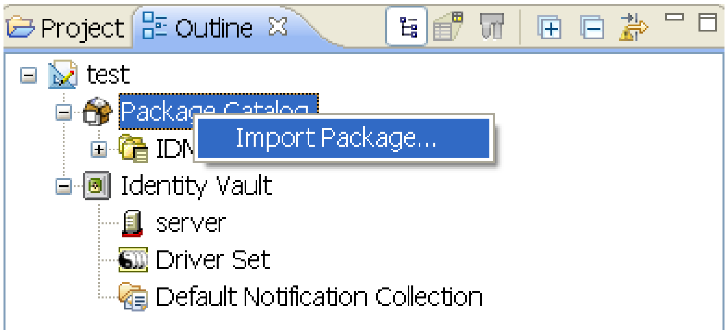
To verify you have the most recent version of the driver packages in the Package Catalog:

1. Open Designer.
2. In the toolbar, click **Help** > **Check for Package Updates**.
3. Click **OK** to update the packages

   or

   click **OK** if the packages are up-to-date.
4. In the Outline view, right-click the Package Catalog.

   Click **Import Package**.



5. Select any BlackboardREST driver packages

   or

   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.

6. Click **OK** to import the selected packages, then click **OK** in the successfully imported packages message.
7. After the current packages are imported, continue with "Installing the Driver Packages" on page 20

Installing the Driver Packages

1. In Designer, open your project.
2. In the Modeler, right-click the driver set where you want to create the driver, then select **New > Driver**.
3. Select **BlackboardREST Base**, then click **Next**.
4. Select the optional features to install the Blackboard driver. All options are selected by default. The options are:

BlackboardREST Default Configuration: This package contains the default configuration information for the Blackboard driver. Always leave this option selected.

BlackboardREST Group Based Enrollments: This package contains the policies required if you want to use Group attributes for Blackboard Enrollments.

BlackboardREST User Entitlements: This package contains the policies and entitlements required to enable the driver to account creation and management with entitlements. For more information, see the *Identity Manager 4.8 Entitlements Guide* on the Identity Manager 4.8 Documentation Site (https://www.netiq.com/documentation/identity-manager-48/).

5 Click **Next**.

6 On the **Driver Information** page, fill in the following field:

Driver Name: The name that identifies the driver in Designer and eDirectory®.

7 Click **Next**.

8 On the Remote Loader page, fill in the following fields:

Host Name: Enter the Host Name or IP Address where the `bbdrv` service has been installed and is running for this driver.

Port: Enter the Port Number where the `bbdrv` service has been installed and is running for this driver. The Default Port is 8090.

Remote Password: The Remote Loader password is used to control access to the Remote Loader instance. It must be the same password during the `bbdrv` configuration.

Driver Password: The Driver Object Password is used by the `bbdrv` service to authenticate itself to the Identity Manager server. It must be the same password that is specified as the Driver Object Password on the Identity Manager Remote Loader.

Key Material Object (KMO): Enter the Key Material Object to be used for the SSL connection to the `bbdrv` service.

9 Click **Next**.

10 On the next page fill in the following fields:

Blackboard Server Hostname: Example: bb.myschool.edu

Blackboard Server Port: This must be the SSL encrypted port. Example: 443

Blackboard Server Url: This is the base URL for the REST API. Example: /learn/api/public/v1/

Blackboard Server API Key: Enter the Blackboard Learn API Key acquired when *Configuring the REST API on your Blackboard Learn Instance*.

Blackboard Server API Secret: Enter the Blackboard Learn API Secret acquired when *Configuring the REST API on your Blackboard Learn Instance*.

11 (Conditional) This page displays only if you selected to install the Blackboard Group Based Enrollments package. Fill in the following field:

Choose the roles that should be used for users who are added to the following group attributes: This setting holds mappings from Group attributes to Blackboard Enrollment Roles. The default map contains mappings that map members of the Member attribute to Student enrollment object and members of the Owner attribute to Instructor enrollment objects. Additional roles can be supported by extending the schema and mapping the desired group attribute to a Blackboard role. Values should be in the format `<attribute>:<bb role>`.

NOTE: These values are case-sensitive and eDirectory attributes usually start with a capital letter.

NOTE: You must remember to add the additional attributes to the filter.

12 Click **Next**.

13 (Conditional) This page displays only if you selected to install the Blackboard User Entitlements package. Fill in the following field:

If a user loses the bbAccount Entitlement take the following action: Choose the desired action if a user loses the bbAccount Entitlement.

14 Click **Next**.

15 (Conditional) This page displays only if you selected to install the Blackboard Default Configuration package. (This package should always be selected.) Fill in the following fields:

Limit the driver to a base container in the Identity Vault for synchronization: Limit events the driver processes to a base container in eDirectory.

Specify the base container in the Identity Vault for User synchronization: This container is used in the Subscriber channel Event Transformation policies to limit the Identity Vault objects being synchronized. Example: users.myorg.

Specify the base container in the Identity Vault for Group synchronization: This container is used in the Subscriber channel Event Transformation policies to limit the Identity Vault objects being synchronized. Example: groups.myorg

What action should be taken on an enrollment when a Person is removed from a Group: If set to **Delete** enrollments dropped from a Group will result in the Person being removed from the Course or Organization. If set to **Disable** the Person's enrollment will be disabled in the Course or Organization.

Automatically set the required ID attribute for new Person, Course, and Organization objects to the source name of the object: If true then the required id attribute for Person, Course, and Organization types in Blackboard will be automatically set to Source Name if the id attribute is not already set. The attributes are DirXML-BB-p-id for Person, DirXML-BB-c-id for Course, and DirXML-BB-o-id for Organization.

Automatically set the required title attribute for new Course, and Organization objects to the source name of the Group: Automatically set required attribute DirXML-bb-c-course-title to the source name for Course objects if it is not already set. Automatically set required attribute DirXML-bb-o-title to source name for Organization objects.

Automatically set the required user roles attributes for Person objects: If true the default roles chosen below will be set for a user if they are not present on the user object.

Default System Role for new users: The default system role to use for new users. See Blackboard Documentation for more information about System Roles.

Default Institutional Role for new users. [ex. Student, Staff, Alumni, Guest, Faculty, Observer, or any custom defined roles]: Default Institutional Role. See Blackboard documentation for more information about Institutional Roles.

Group objects in this subtree will be synchronized as Courses in Blackboard: All group objects in this subtree will be synchronized as Courses in Blackboard. Group objects in eDirectory can represent a Course or Organization object in Blackboard.

Group objects in this subtree will be synchronized as Organizations in Blackboard: All group objects in this subtree will be synchronized as Organizations in Blackboard. Group objects in eDirectory can represent a Course or Organization object in Blackboard.

Automatically set required Person attribute DirXML-BB-p-email if it is not set: Email address is a required attribute for User creation in Blackboard. If true then the following setting will be used to create the user's email address in Blackboard.

Domain name to use for default email address: Email address is a required attribute for a Person in Blackboard. This value will be used to set the email address attribute in Blackboard for users who do not have an email address specified in their eDirectory User object. The CN of the user will be used with the value provided to create the email address.

16. Click **Next**.
17. Review the summary of tasks that will be completed to create the driver, then click **Finish**.
18. After you have installed the driver, you must change the configuration for your environment. Proceed to "Configuring the Driver" on page 23.

Configuring the Driver

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

- **Configure the driver parameters:** 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 configure the driver parameters located on the Global Configuration Values page.
- **Configure the driver filter:** Modify the driver filter to include the object classes and attributes you want synchronized between the Identity Vault and Blackboard.
- **Configure Policies:** Modify the policies as needed.

  IMPORTANT: Policies should only be modified using Designer or changes could be lost when a package is upgraded or the driver is run in "factory mode."

  For information about the default configuration policies, see Appendix A, "Policies," on page 39.
- **Configure password synchronization:** The basic driver configuration is set up to support password synchronization through Universal Password. If you don't want this setup, see "Configuring Password Flow " in the *Identity Manager 4.8 Password Management Guide*.

After completing the configuration tasks, continue with the next section, Deploying the Driver.

Deploying the Driver

After a 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 line, then select **Live > Deploy**.

3 If you are authenticated to the Identity Vault, skip to Step 5; otherwise, specify the following information:

- **Host:** Specify the IP address or DNS name of the server hosting the Identity Vault.
- **Username:** Specify the DN of the user object used to authenticate to the Identity Vault.
- **Password:** Specify the user's password.

4 Click **OK**.

5 Read the deployment summary, then click **Deploy**.

6 Read the message, then click **OK**.

7 Click **Define Security Equivalence** to assign rights to the driver.

The driver requires rights to objects within the Identity Vault. The Admin user object is most often used to supply these rights. 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.

7a Click **Add**, then browse to and select the object with the correct rights.

7b Click **OK** twice.

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

You should exclude any administrative User objects (for example, Admin and DriversUser) from synchronization.

8a Click **Add**, then browse to and select the user object you want to exclude.

8b Click **OK**.

8c Repeat Step 8a and 8b for each object you want to exclude.

8d Click **OK**.

The Driver Shim Configuration File

The driver shim configuration file controls operation of the driver shim. This file is located at `/etc/bbdrv.conf` on the Linux server hosting the driver shim.

A default configuration file is created at installation time.

You can specify the configuration options listed in Table 4-5, one per line. You can also specify these options on the driver shim command line. For details about driver shim command line options, see Section D.2, Driver Shim Command Line Options.

Table 3-2

Option (Short and Long Forms)	Description

-conn connString
-connection connString
	A string with connection options. Enclose the string in double quotes ("). If you specify more than one option, separate the options with spaces.
	port=driverShimPort
	ca="Certificate Authority Key File"

Option (Short and Long Forms)	Description
-hp httpPort -httpport httpPort	Specifies the HTTP services port number. The default HTTP services port number is 8091. You can connect to this port to view log files. For details, see Section A.1, Driver Status and Diagnostic Files.
-path driverPath	Specifies the path for driver files. The default path is /opt/novell/bbdrv.
-t traceLevel -trace traceLevel	Sets the level of debug tracing. 0 is no tracing, and 10 is all tracing. For details, see Section A.1, Driver Status and Diagnostic Files.
-tf fileName -tracefile fileName	Sets the trace file location. Default file: /opt/novell/bbdrv/logs/trace.log
-tfm *size* -tracefilemax *size*	Specifies the limit to the size of the trace file for this instance. Specify the value in kilobytes, megabytes, or gigabytes, using the abbreviation for the byte type. The minimum value is 100K. For example: ◆ `-tracefilemax 1000K` ◆ `-tracefilemax 100M` ◆ `-tracefilemax 10G` **NOTE:** ◆ When you add this option to the configuration file, the application uses the specified name for the tracefile and includes up to 9 “roll-over” files. Each file size is 1/10th of the total size specified. The roll-over files are named using the base of the main trace filename plus _`n`, where `n` is 1 through 9. ◆ If the trace file data is larger than the specified maximum when the Driver Shim is started, the trace file data remains larger than the specified maximum until roll-over is completed through all 10 files.

Example Configuration File

```
-tracefile /opt/novell/bbdrv/logs/trace.log
-trace 0
-tracefilemax 100M
-connection "ca=/opt/novell/bbdrv/keys/ca.pem port=8090"
-httpport 8091
-path /opt/novell/bbdrv/
```

Starting the Driver

When a driver is created, it is stopped by default. To make the driver work, you must start the driver and cause events to occur. Identity Manager is an event-driven system, so after the driver is started, it won't do anything until an event occurs.

To start the driver:

1. Make sure the Remote Loader driver instance is running:

   - `At the Linux server command line, enter:`

     ```
     /etc/init.d/bbdrvd start
     ```

2. In Designer, open your project.
3. In the Modeler, right-click the driver icon or the driver line, then select **Live > Start Driver**.

Activating the Driver

If you created the driver in a driver set where you have already activated the Metadirectory engine and service drivers, the driver inherits the activation. If you created the driver in a driver set that has not been activated, you must activate the driver within 90 days. Otherwise, the driver stops working.

For information on activation, refer the *Identity Manager 4.8 Installation Guide* on the Identity Manager 4.8 Documentation Site (https://www.netiq.com/documentation/identity-manager-48/).

4 Customizing the Driver

This section provides guidelines for customizing your driver to your specific business rules.

Attributes Required for Blackboard Object Creation

The Subscriber channel issues Blackboard REST API calls to process XDS commands received for objects and attributes represented in the Blackboard schema. It is up to the policy writer to ensure all required attributes are sent for Blackboard object creation. The sample policies can be configured on driver import or through global configuration values to ensure all required attributes are set on creation. The Blackboard REST API places restrictions on attribute values. It is up to the policy writer to ensure attributes mapped to Blackboard attributes contain values that conform to Blackboard attribute restrictions. The following tables list attributes required for Person, Course, Enrollment, and Organization creation in Blackboard. For information about restrictions on values for these attributes consult Blackboard documentation.

***Table 4-1** Person Attributes Required For Creation*

Blackboard Schema	Blackboard Attribute
DirXML-BB-p-ext-key	EXTERNAL_PERSON_KEY
DirXML-BB-p-id	USER_ID
DirXML-BB-p-sys-role	SYSTEM_ROLE
DirXML-BB-p-firstname	FIRSTNAME
DirXML-BB-p-lastname	LASTNAME
DirXML-BB-p-email	EMAIL

***Table 4-2** Course Attributes Required For Creation*

Blackboard Schema	Blackboard Attribute
DirXML-BB-c-id	COURSE_ID
DirXML-BB-c-course-title	COURSE_NAME

***Table 4-3** Organization Attributes Required For Creation*

Blackboard Schema	Blackboard Attribute
DirXML-BB-o-id	ORGANIZATION_ID
DirXML-BB-o-title	ORGANIZATION_NAME

Table 4-4 Course Enrollment Attributes Required For Creation

Blackboard Schema	Blackboard Attribute
DirXML-BB-enr-c-ext-key	EXTERNAL_COURSE_KEY
DirXML-BB-enr-p-ext-key	EXTERNAL_PERSON_KEY

Table 4-5 Organization Enrollment Attributes Required For Creation

Blackboard Schema	Blackboard Attribute
DirXML-BB-enr-o-ext-key	EXTERNAL_ORGANIZATION_ID
DirXML-BB-enr-p-ext-key	EXTERNAL_PERSON_KEY

Attributes and Values for Blackboard Enumeration Types

The following tables list valid values for enumeration type attributes supported by the driver.

Table 4-6 DirXML-BB-Course Enumeration Types And Valid Values

Enumeration Type Attribute	Valid Values	Description
DirXML-BB-c-duration-type	Continuous	Course is active on an ongoing basis.
	DateRange	Course is only intended to be available between specific date ranges.
	FixedNumDays	Course is only available for a set number of days.
DirXML-BB-c-enrollment-type	EmailEnrollment	Instructors have the ability to enroll users, and students can email requests to the instructor for enrollment.
	InstructorLed	Enrollment tasks for the course can only be performed by the instructor.
	SelfEnrollment	Instructors have the ability to enroll users, and students can also enroll themselves in the course.

Table 4-7 DirXML-BB-Person Enumeration Types And Valid Values

Enumeration Type Attribute	Valid Values	Description
DirXML-BB-p-educ-level	Freshman	College or university freshman.
	GraduateSchool	Graduate school student.
	HighSchool	Grades 9 through 12.
	Junior	College or university junior.
	K8	Kindergarten through 8th grade.
	PostGraduateSchool	Post-graduate school student.
	Senior	College or university senior.
	Sophomore	College or university sophomore.
	Unknown	Education level is not known, or not specified.
DirXML-BB-p-gender	Female	Female.
	Male	Male.
	Unknown	Gender is not known, or not specified.
DirXML-BB-p-sys-role	AccountAdmin	Account Administrator role.
	CourseCreator	Course Creator role.
	CourseSupport	Course Support role.
	Guest	Guest role.
	Integration	This role is private, used only for special processes that interact for data integration authentication.
	Observer	Observer role.
	Portal	Portal Administrator role.
	SystemAdmin	System Administrator role.
	SystemSupport	System Support role.
	User	Normal user role.
	(User-defined system roles)	To set a user-defined system role, click the Blackboard **Administrator Panel** > **System Role** and select a Role ID.

Table 4-8 DirXML-BB-Enrollment Enumeration Types And Valid Values

Enumeration Type Attribute	Valid Values	Description
DirXML-BB-enr-role	CourseBuilder	The Course Builder role has access to most areas of the Control Panel. This role is appropriate for a user to manage the Course without having access to Student grades. A Course Builder can still access the Course if the Course is unavailable to Students. A Course Builder cannot delete an Instructor from a Course.
	Grader	A Grader assists the Instructor in the creation, management, delivery, and grading of items, such as Tests and Discussion Board posts. A Grader also assists the Instructor with managing the Grade Center. A Grader cannot access a Course if it is unavailable to Students.
	Guest	Guests have no access to the Control Panel. Areas within the Course are made available to Guests. Visitors, such as prospective Students, alumni, or parents may be given the role of Guest.
	Instructor	Instructors have access to all areas in the Control Panel. This role is generally given to those developing, teaching, or facilitating the class. Instructors may access a Course that is unavailable to Students.
	Student	Student is the default Course Role. Students have no access to the Control Panel.
	TeachingAssistant	The Teaching Assistant role is that of a co-teacher. Teaching Assistants are able to administer all areas of a course. Their only limitations are those imposed by the Instructor or Blackboard administrator at your school. A Teaching Assistant cannot delete an Instructor from a Course.

5 Managing the Driver

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

- Starting, stopping, and restarting the driver

NOTE: If the connectivity to the database server for Blackboard is lost, the driver shim must be restarted to re-establish communication with the Blackboard Application.

- 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
- Synchronizing objects
- Migrating and resynchronizing data
- Activating the driver

Because these tasks, as well as several others, are common to all Identity Manager drivers, they are included in one reference, the *Identity Manager 4.8 Common Driver Administration Guide*, available at the Identity Manager 4.8 Documentation page (https://www.netiq.com/documentation/identity-manager-48/).

6 Troubleshooting the Driver

This section provides information about troubleshooting the Blackboard driver.

- "Viewing Driver Processes" on page 33
- "Driver Status and Diagnostic Files" on page 33
- "Troubleshooting Common Problems" on page 36
- "Shared Memory Errors" on page 38

Viewing Driver Processes

Viewing driver processes is necessary to analyze unexpected behavior. To view the driver processing events, use DSTrace. You should only use it during testing and troubleshooting the driver. Running DSTrace while the drivers are in production increases the utilization on the Identity Manager server and can cause events to process very slowly.

For more information, see the he *Identity Manager 4.8 Common Driver Administration Guide*, available at the Identity Manager 4.8 Documentation page (https://www.netiq.com/documentation/identity-manager-48/).

Driver Status and Diagnostic Files

There are several log files that you can view to examine driver operation:

- "The System Log" on page 33
- "The Trace File" on page 34
- "DSTrace" on page 35
- "The Status Log" on page 35

The System Log

The System log is used by the Blackboard REST driver shim to record urgent, informational and debug messages. Examining these should be foremost in your troubleshooting efforts. For detailed message documentation, see Appendix C, "System and Error Messages," on page 47.

The location for the system log varies from system to system and is generally configured through /etc/syslog.conf. The amount of information that is logged by the driver can also be configured through this system log configuration file. The following is a sample fragment of /etc/syslog.conf:

```
# sample /etc/syslog.conf
#
*.err;kern.notice;auth.notice                          /dev/sysmsg
*.err;kern.debug;daemon.notice;mail.crit               /var/adm/messages

*.alert;kern.err;daemon.err                            operator
*.alert                                                root
```

The options in the first column determine which messages are logged. The options in the second column specify the destination file or user to send the log output to. For example, specifying `*.err` logs all messages with a priority of err or above. For more information about syslog priorities, view your system documentation using the `man syslog` command. Messages from the driver shim and messages from the scripts are logged with various priorities as shown in Table 6-1. The information that is recorded depends on your syslog configuration.

Table 6-1

Message Topic	**Priority**
Script being called	DEBUG
Successful Linux command execution	INFO
Publication events	INFO
Failures	ERR

The Trace File

The default trace file exists on the connected system as `trace.log` in the `logs` directory under the installation folder. A large amount of debug information can be written to this file. Use the trace level setting in your driver shim configuration file to control what is written to the file. For details about the driver shim configuration file, see Section "The Driver Shim Configuration File" on page 24.

Table 6-2

Trace Level	**Description**
0	No debugging
1-3	Identity Manager messages. Higher trace levels provide more detail.
4	Previous levels plus Remote Loader, driver, driver shim and connection messages.
5-7	Previous level plus change log and loopback messages. Higher levels provide more detail.

Trace Level	Description
8	Previous level plus driver status log, driver parameters, driver command-line, driver security, driver Web Services, driver schema, driver encryption, driver PAM, driver SOAP API and driver include/exclude file messages.
9	Previous level plus low-level networking and operating system messages.
10	Previous level plus maximum low-level program details (all options).

The following is an example configuration line to set the trace level:

```
-trace 9
```

To view the trace file:

1. Use a web browser to access the driver shim at `https://driver-address:8091`. Substitute the DNS name or IP address of your driver shim for driver-address.
2. Authenticate by using any username and the password that you specified as the Remote Loader password.
3. Click `Trace`.

DSTrace

Identity Manager information using the DSTrace facility on the Metadirectory server. Use Identity Console to set the tracing level. For example, trace level 2 shows Identity Vault events in XML documents, and trace level 5 shows the results of policy execution. Because a high volume of trace output is produced, we recommend that you capture the trace output to a file. For details about using DSTrace, see the Identity Manager Administration Guide (https://www.netiq.com/documentation/identity-manager-48/)

The Status Log

The status log is a condensed summary of the events that have been recorded on the Subscriber and Publisher channels. This file exists on the connected system as `dirxml.log` in the logs directory under the driver installation directory. For details about using the status log, see the Identity Manager Administration Guide (https://www.netiq.com/documentation/identity-manager-48/)

To view the status log:

1. Use a web browser to access the driver shim at https://driver-address:8091. Substitute the DNS or IP address of your driver shim for driver-address.
2. Authenticate by using any username and the password that you specified as the Remote Loader password.
3. Click `Status`.

Troubleshooting Common Problems

- "Driver Shim Installation Failure" on page 36
- "Driver Rules Installation Failure" on page 36
- "Driver Certificate Setup Failure" on page 36
- "Driver Start Failure" on page 36
- "Driver Shim Startup or Communication Failure" on page 37
- "Users or Groups Are Not Provisioned to Blackboard Learn" on page 37
- "Identity Vault User Passwords Are Not Provisioned to Blackboard Learn" on page 37
- "Metadirectory Objects Are Not Modified, Deleted, Renamed or Moved" on page 38

Driver Shim Installation Failure

- Ensure that you used the correct installation program for your operating system and that you are running on a supported operating system.
- Ensure that you run the installation as root or equivalent.
- Ensure that your package management software, such as RPM, is installed and up-to-date.

Driver Rules Installation Failure

Ensure that you are using a version of Designer that supports your version of Identity Manager.

Driver Certificate Setup Failure

- Ensure that eDirectory is running LDAP with SSL enabled. For details about configuring eDirectory, see NetIQ eDirectory Administration Guide.
- Ensure that the connected system has network connectivity to the Metadirectory server.

You can use the command `/opt/novell/bbdrv/bin/bbdrv -s` to configure the certificate at any time.

If you cannot configure SSL using LDAP, you can install the certificate manually:

1. Click **Certificate Management** > **Trusted Root Management** options from the Identity Console landing page. The **Trusted Root Container** check box will be selected by default. Select the **Trusted Root** check box.
2. Select the appropriate trusted root certificate from the list and click the export icon.
3. In the next screen, do not select the check box for **Export Private key**.
4. Select `Base64` format, then click OK.
5. Use FTP, SSH or any other method to store the file on the connected system as `ca.pem` in the `keys` directory under the driver installation directory.

Driver Start Failure

- Examine the status log and DSTrace output.

- The driver must be specified as a Remote Loader driver, even if the Identity Vault and connected system are the same computer. You can set this option in Identity Console by editing the **Connection Parameters** on the Driver instance.
- You must activate both Identity Manager and the driver within 90 days. The Driver Dashboard, under the **IDM Administration** page, in Identity Console displays Activation Info and Activation Installation steps.
- For details about activating NetIQ Identity Manager Products, see the Identity Manager Installation Guide at (https://www.netiq.com/documentation/identity-manager-48/)

Driver Shim Startup or Communication Failure

- Examine the trace file.
- Ensure the connected systems' operating system version is supported. Apply all patches for your operating system.
- Ensure that the Remote Loader and Driver Object passwords that you specified while setting up the driver on the Metadirectory server match the passwords stored with the driver shim.
- To update these passwords on the connected system, us the `/opt/novell/bbdrv/bin/bbdrv -sp` command. The passwords are stored under keys in the driver installation directory in encrypted files `dpwdl1f40` (Driver object password) and `lpwd1f40` (Remote Loader password).
- To update these passwords on the Metadirectory server, use Designer or Identity Console to update the driver configuration. For details, see Chapter 5, "Managing the Driver," on page 31.

Users or Groups Are Not Provisioned to Blackboard Learn

- Examine the status log, DSTRACE output, trace file and script output file.
- To be provisioned, users and groups must be in the appropriate base container. You can view and change the base containers in Identity Console on the **Global Config Values** page of the Configuration tab on the **Drivers** module.
- To provision identities from the Identity Vault to Blackboard Learn, the driver Data Flow property must be set to Identity Vault to Application. To change this value, re-import the driver rules file over your existing driver.
- The user that the driver is security equivalent to must have rights to read information from the base container. For details about the rights required, see Table 3-1 on page 19.

Identity Vault User Passwords Are Not Provisioned to Blackboard Learn

- Examine the status log, DSTRACE output, and script output file.
- There are several password management properties available in Identity Console on the **Global Config Values** page under Configuration tab of the **Drivers** module. Ensure that the connected system accepts passwords from the Identity Vault. To determine the right settings for your environment, view the help for the options, or see the Identity Manager Administration Guide.
- Ensure that the user's container has an assigned Universal Password policy and that the Synchronize Distribution Password When Setting Universal Password GCV is set for this policy.

Metadirectory Objects Are Not Modified, Deleted, Renamed or Moved

- Examine the status log, DSTRACE output, trace file and script output file.
- Examine the driver Data Flow. Identity Vault and connected system identities must be associated before events are synchronized. To view an identity's associations, use the **Object Inspector** page in Identity Console and search for the object.
- Identity Vault move events can remove the identity from the base container monitored by the driver to a container that is not monitored by the driver. This makes the move appear to be a delete

Shared Memory Errors

Shared memory is used by the driver shim to safely and securely communicate with the scripts on Linux. If the system shared memory segments become unusable, you must shut down the process and fix the shared memory segments.

Shared memory segments can become unusable on some Linux systems if the driver shim is improperly terminated without detaching from the segments. For information about how to properly stop the driver shim, see Chapter 5, "Managing the Driver," on page 31. You can use the `ipcs` system tool to locate these segments and the `ipcrm` tool to manually clear them as shown in the following example:

```
> ipcs -m
------ Shared Memory Segments --------
key        shmid    owner     perms     bytes    nattch    status
0x2a065bbd 1802241  root      600       16384    1
> ipcrm -m 1802241
```

The driver shim generates default segments of 16384 bytes with permissions at 600.

A Policies

This section provides information about Policies for the Blackboard driver.

Event Transforms

NTIQBBRTDC-sub-evt-VetoRenameEvents

Description: Veto rename events.

NTIQBBRTDC-sub-evt-DetermineBBObjectType

Description: Set an operation property name "BBObjectType" that helps map the operation to the type of Blackboard object. Group objects can represent Blackboard Courses or Organizations so it is necessary to specify which one should be used.

Matching

NTIQBBRTDC-sub-mp-SubscriberMatching

Description: Search for a matching Blackboard object based on the type of Blackboard object type set in the BBObjectType operation property. Refer to Table A-1 for matching attributes.

***Table A-1** Matching Attributes*

eDirectory Object Class	eDirectory Attribute	BBObjectType	Blackboard Attribute
User	Source Name	DirXMI-BB-Person	DirXML-BB-p-id
Group	Source Name	DirXML-BB-Course	DirXML-BB-c-id
Organization	Source Name	DirXML-BB-Organization	DirXML-BB-o-id
DirXML-BB-Enrollment*	DirXML-BB-c-ext-key, DirXML-BB-p-ext-key	DirXML-BB-Enrollment	DirXML-BB-c-ext-key, DirXML-BB-p-ext-key

* The DirXML-BB-Enrollment class can represent objects using effective class DirXML-BB-Enrollment in eDirectory or can represent pseudo enrollment objects created in policy when using attributes on groups to represent enrollments. For more information see "Organization" on page 12.

Creation Policies

NTIQBBRT-sub-cp-SubscriberCreation

Description: Check to see if required attributes are set for object creation in Blackboard. If not set and specified in the GCVs default values will be set for some of the required attributes. Refer to Table A-2, Table A-3 and Table A-4 for required attributes.

Table A-2 *Required User Attributes (BBObjectType operation property = DirXML-BB-Person)*

Required User Attribute	Action
DirXML-BB-p-id	If not set and GCV auto_set_ids is true set to Source Name.
Internet Email Address	If not set and GCV auto_set_email is true set to CN + @ + GCV default_email_domain.
DirXML-BB-p-sys-role	If not set and GCV auto_set_roles is true set to value of GCV default_user_role.
DirXML-BB-p-portal-role	DirXML-BB-p-portal-role If not set and GCV auto_set_roles is true set to value of GCV default_portal_role.
DirXML-BB-p-ext-key	Set to Source Name with underscores replacing spaces.

Table A-3 *Required Group Attributes (BBObjectType operation property = DirXML-BB-Course)*

Required Group Attribute	Action
DirXML-BB-c-course-title	If not set and GCV auto_set_title is true then set value to Source Name.
DirXML-BB-c-id	If not set and GCV auto_set_ids is true then set value to Source Name.
DirXML-BB-c-ext-key	Set to Source Name with underscores replacing spaces.

Table A-4 *Required Organization Attributes (BBObjectType operation property = DirXML-BB-Organization)*

Required Organization Attribute	Action
DirXML-BB-o-title	If not set and GCV auto_set_title is true then set value to Source Name.
DirXML-BB-o-id	If not set and GCV auto_set_ids is true then set value to Source Name.
DirXML-BB-o-ext-key	Set to Source Name with underscores replacing spaces.

Command Transforms

NTIQBBRTDC-ctp-TransformLoginDisabled

Description: Transform changes on user object attribute “Login Disabled” to Blackboard DirXML-BB-Person object attributes DirXML-BB-p-row-status and DirXML-BB-p-available-ind. Refer to Table A-5 for attribute value settings.

Table A-5 Attribute Values

Login Disabled	DirXML-BB-p-row-status	DirXML-BB-p-available-ind
True	ENABLED	True
False	ENABLED	False

NTIQBBRTDC-ctp-SetClassnameForGroups

Description: Set the operation object class for groups to the Blackboard object class type based on the value in the BBObjectType operation property. BBObjectType is set in the NTIQBBRTDC-evt-DetermineBBObjectType policy. Group objects can represent a Blackboard Course or Organization so the object class determines which one the operation maps to.

NTIQBBRTGBE-sub-ctp-TransformGroupAttrsToEnrollmentObjects

Description: Transforms changes on Group attributes listed in the “attribute_role_map” GCV to DirXML-BB-Enrollment object events.

Schema Mapping

NTIQBBRTDC-smp-SchemaMapping

Description: Mapping contains some basic default mappings. Refer to Table A-6 for attribute details.

Table A-6 Object Mapping (eDirectory to BBObjectType operation property)

eDirectory Object Class	Blackboard Object Type
Group	DirXML-BB-Course
Description	DirXML-BB-c-description
Organization	DirXML-BB-Organization
Description	DirXML-BB-o-description
User	DirXML-BB-Person
Given Name	DirXML-BB-p-firstname
Internet Email Address	DirXML-BB-p-email
nspmDistributionPassword	DirXML-BB-p-password

eDirectory Object Class	Blackboard Object Type
Surname	DirXML-BB-p-lastname

Output Transforms

NTIQBBRTDC-otp-CheckRequiredAttrs

Description: Ensure attributes required by Blackboard object types are set before sending document to the driver shim. Refer to Table A-7 for required attributes.

Table A-7 *Attributes Required by Blackboard*

Blackboard Object Type	Attribute Settings Required by Blackboard
DirXML-BB-Person	DirXML-BB-p-id DirXML-BB-p-firstname DirXML-BB-p-lastname DirXML-BB-p-sys-role DirXML-BB-p-portal-role DirXML-BB-p-email DirXML-BB-p-ext-key
DirXML-BB-Course	DirXML-BB-c-id DirXML-BB-c-course-title
DirXML-BB-Organization	DirXML-BB-o-id DirXML-BB-o-title
DirXML-BB-Enrollment	DirXML-BB-enr-p-ext-key DirXML-BB-enr-c-ext-key

Input Transforms

NTIQBBRTGBE-ipt-VetoPseudoEntitlementAssociation

Description: When using group based enrollments no object exists in eDirectory that can hold an association for a corresponding Blackboard Enrollment Object. The driver shim returns a destination DN value of “pseudo-enrollment-object” if no source DN was present. This policy vetos add-association operations for pseudo-enrollment-objects.

B Global Configuration Values

This section provides information about the Driver Configuration and Global Configuration Values properties for the Blackboard driver.

- "General Settings" on page 43
- "Default Required Attribute Settings" on page 44

General Settings

***Table B-1** Global Configuration Values - General Settings*

Name	Display Name	Description	Default Value
use_entitlements	Enable the driver to use Approval Flow or Role-Based Entitlements with the Entitlements Service driver.	N/A	N/A
use_scope_filtering	Limit the driver to a base container in the Identity Vault for synchronization?	Limit events the driver processes to a base container in eDirectory	True
container_scope_filter_user	Specify the base container in the Identity Vault for User synchronization.	This container is used in the Subscriber channel Event Transformation policies to limit the Identity Vault objects being synchronized. For example: [users.myorg]	N/A
container_scope_filter_group	Specify the base container in the Identity Vault for Group synchronization.	This container is used in the Subscriber channel Event Transformation policies to limit the Identity Vault objects being synchronized. For example: [groups.myorg]	System

Name	Display Name	Description	Default Value
disable_or_delete_enrollments	What action should be taken on an enrollment when a Person is removed from a Group?	If set to Delete enrollments dropped from a Group will result in the Person being removed from the Course or Organization. If set to Disable the Person's enrollment will be disabled in the Course or Organization.	Delete

Default Required Attribute Settings

Table B-2 *Global Configuration Values - Default Required Settings on New Blackboard Objects*

Name	Display Name	Description	Default Value
auto_set_ids	Automatically set the required Id attribute for new Person, Course, and Organization objects to the source name of the object.	If true then the required id attribute for Person, Course, and Organization types in Blackboard will be automatically set to Source Name if the id attribute is not already set. The attributes are DirXML-BB-p-id for Person, DirXML-BB-c-id for Course, and DirXML-BB-o-id for Organization.	True
auto_set_title	Automatically set the required title attribute for new Course, and Organization objects to the source name of the Group.	Automatically set required attribute DirXML-bb-c-course-title to the source name for Course objects if it is not already set. Automatically set required attribute DirXML-bb-o-title to source name for Organization objects.	True

Name	Display Name	Description	Default Value
auto_set_roles	Automatically set the required user roles attributes for Person objects.	If true the default roles chosen below will be set for a user if they are not present on the user object.	True
default_user_role	Default System Role for new users	N/A	USER
default_portal_role	Default Institutional Role for new users. Example: STUDENT, STAFF, ALUMNI, GUEST, FACULTY, OBSERVER, or any custom defined roles	N/A	STUDENT
add_aux_classes	Automatically add a required Blackboard auxiliary class to Person and Course or Organization objects.	If true automatically add the DirXML-BB-Person auxiliary class to Person objects and the DirXML-BB-Course auxiliary class to Course or Organization objects.	True
bb-course-subtree	Apply DirXML-BB-Course to groups in the following subtree	N/A	N/A
bb-organization-subtree	Apply DirXML-BB-Organization to groups in the following subtree.	N/A	N/A
auto_set_email	Automatically set required Person attribute DirXML-BB-p-email if it is not set.	N/A	True
default_email_domain	Domain name to use for default email address.	Email address is a required attribute for a Person in Blackboard. This value will be used to set the email address attribute in Blackboard for users who do not have an email address specified in their eDirectory User object. The CN of the user will be used with the value provided to create the email address.	N/A

C System and Error Messages

Components of the Identity Manager 4.8 driver for Blackboard REST write messages to the system log to report operational status and problems. For more information about the system log, see "The System Log" on page 33 For detailed troubleshooting information, see Chapter 6, "Troubleshooting the Driver," on page 33.

Each message begins with a code of 3-6 characters associated with the driver component that generated the message. Use this code to find message information quickly as follows:

- "CFG Messages" on page 47
- "CHGLOG Messages" on page 48
- "DOM Messages" on page 48
- "DRVCOM Messages" on page 49
- "HES Messages" on page 49
- "LWS Messages" on page 50
- "NET Messages" on page 51
- "NIX Messages (Linux/UNIX only)" on page 51
- "OAP Messages" on page 54
- "RDXML Messages" on page 55

CFG Messages

Messages beginning with CFG are issued by configuration file processing.

CFG001E Could not open configuration file filename.

Explanation: Could not open the configuration file.

Possible Cause: The file does not exist.

Possible Cause: You don't have permission to read the file.

Action: Ensure that the configuration file exists at the correct location and that you have file system rights to read it.

CFG002E Error parsing configuration file line:

Explanation: The line is not formatted as a valid configuration statement and cannot be parsed.

Possible Cause: The configuration file contains invalid or incorrect statements.

Action: Correct the line in the configuration file.

CFG003W Configuration file line was ignored. No matching statement name found: <configline>.

Explanation: This line is formatted as a valid configuration file statement, but the statement is not recognized. The line is ignored.

Possible Cause: The statement is incorrectly typed or the statement name is used only in a newer version of the software.

Action: Correct the statement.

CFG004E Error parsing configuration file line. No statement name was found: <configLine>.

Explanation: Could not find a statement name on the configuration line.

Action: Correct the line in the configuration file to supply the required statement.

CFG005E A required statement *statement_id* is missing from the configuration file.

Explanation: The *statement_id* statement was not specified in the configuration file, but is required for the application to start.

Possible Cause: The configuration file is missing required statements.

Action: Add the required statement to the configuration file.

CHGLOG Messages

Messages beginning with CHGLOG are issued by change log processing.

CHGLOG000I nameversion Copyright 2005 Omnibond Systems, LLC. ID=code_id_string.

Explanation: This message identifies the system component version.

Action: No action is required.

DOM Messages

Messages beginning with DOM are issued by driver components as they communicate among themselves.

DOM0001W XML parser error encountered: errorString.

Explanation: An error was detected while parsing an XML document.

Possible Cause: The XML document was incomplete, or it was not a properly constructed XML document.

Action: See the error string for additional details about the error. Some errors, such as no element found, can occur during normal operation and indicate that an empty XML document was received.

DRVCOM Messages

Messages beginning with DRVCOM are issued by the include/exclude system.

DRVCOM000I nameversion Copyright 2005 Omnibond Systems, LLC. ID=code_id_string.

Explanation: This message identifies the system component version.

Action: No action is required.

DRVCOM001W Invalid include/exclude CLASS statement.

Explanation: The include/exclude configuration file contains an invalid CLASS statement.

Action: Correct the include/exclude configuration file with proper syntax.

DRVCOM002D An include/exclude Rule was added for class: class.

Explanation: The include/exclude configuration supplied a rule for the specified class.

Action: None.

DRVCOM003D An include/exclude Association Rule was added for association association.

Explanation: The include/exclude configuration supplied an association rule for the specified association.

Action: None.

HES Messages

Messages beginning with HES are issued by driver components as they use HTTP to communicate.

HES001E Unable to initialize the HTTP client.

Explanation: Communications in the client could not be initialized.

Possible Cause: Memory is exhausted.

Action: Increase the amount of memory available to the process.

HES002I Connecting to host host_name on port port_number.

Explanation: The client is connecting to the specified server.

Action: None.

HES003W SSL communications have an incorrect certificate. rc = rc.

Explanation: The security certificate for SSL services could not be verified.

Possible Cause: The certificate files might be missing or invalid.

Action: Obtain a new certificate.

LWS Messages

Messages beginning with LWS are issued by the integrated HTTP server.

LWS0001I Server has been initialized.

Explanation: The server has successfully completed its initialization phase.

Action: None. Informational only.

LWS0002I All services are now active.

Explanation: All of the services offered by the server are now active and ready for work.

Action: None. Informational only.

LWS0003I Server shut down successfully.

Explanation: The server processing completed normally. The server ends with a return code of `0`.

Action: No action is required.

LWS0004W Server shut down with warnings.

Explanation: The server processing completed normally with at least one warning. The server ends with a return code of 4.

Action: See the log for additional messages that describe the warning conditions.

LWS0005E Server shut down with errors.

Explanation: The server processing ended with one or more errors. The server ends with a return code of 8.

Action: See the log for additional messages that describe the error conditions.

LWS0006I Starting service.

Explanation: The server is starting the specified service.

Action: None. Informational only.

LWS0007E Failed to start service.

Explanation: The server attempted to start the specified service, but the service could not start. The server terminates processing.

Action: See the log for additional messages that describe the error condition.

LWS0008I Stopping all services.

Explanation: The server was requested to stop. All services are notified and will subsequently end processing.

Action: None. Informational only.

NET Messages

Messages beginning with NET are issued by driver components during verification of SSL certificates.

NET001W Certificate verification failed. Result is result.

Explanation: A valid security certificate could not be obtained from the connection client. Diagnostic information is given by result.

Possible Cause: A security certificate has not been obtained for the component.

Possible Cause: The security certificate has expired.

Possible Cause: The component certificate directory has been corrupted.

Action: Respond as indicated by result. Obtain a new certificate if appropriate.

NIX Messages (Linux/UNIX only)

Messages beginning with NIX are issued by the driver shim.

NIX000I nameversion Copyright 2005 Omnibond Systems, LLC. ID=code_id_string.

Explanation: This message identifies the system component version.

Action: No action is required.

NIX001S An error occurred attempting to attach the shared memory segment to an address space (errno=errno).

Explanation: The driver uses shared memory as the mechanism for providing information to the scripts. An error occurred attempting to attach the shared memory to a physical address for access.

Possible Cause: The calling process has no access permissions for the requested attach type.

Possible Cause: An invalid or non-page-aligned address was provided to the system routine.

Possible Cause: Memory could not be allocated for the descriptor or for the page tables.

Action: Restart the driver process and ensure that there are adequate memory resources. Verify that the driver process is run as root and has permissions to read its configuration files. Contact NetIQ® Support for additional instructions if necessary.

NIX002S An error occurred while attempting to allocate a shared memory segment (errno = errno).

Explanation: The driver uses shared memory as the mechanism for providing information to the scripts. An error occurred attempting to allocate a shared memory segment.

Possible Cause: The memory size was too small or too large.

Possible Cause: The system shared memory settings might not have adequate values

Possible Cause: The memory segment could not be created because it already exists. This could be caused by an abnormal termination of a previous driver process.

Possible Cause: All possible shared memory IDs have been taken.

Possible Cause: Allocating a segment of the requested size would cause the system to exceed the system-wide limit on shared memory.

Possible Cause: No shared memory segment exists for the given key.

Possible Cause: The user or process does not have permission to access the shared memory segment.

Possible Cause: No memory could be allocated for segment overhead.

Action: Restart the driver process and ensure that there is sufficient memory.

Action: Verify that the driver process is run as root and has permissions to read its configuration files.

Action: Verify that the driver process is run as root and has permissions to read its configuration files

Action: If there are other applications on the server that use shared memory, ensure that they are running, healthy, and do not conflict with the requirements for the driver.

Action: Contact NetIQ Support for additional instructions if necessary.

NIX003S An error occurred attempting to create a System V IPC key. The project identifier pathname = pathname.

Explanation: The driver uses shared memory as the mechanism for providing information to the scripts. An error occurred attempting to create the key used to specify the shared memory segment.

Possible Cause: The project pathname is invalid or does not exist.

Action: Restart the driver process.

Action: Ensure that the file pathname is correct and that the process has adequate permissions to read the path.

NIX004S An error occurred while writing data to shared memory (bytes = bytes, allocationSize = allocationSize).

Explanation: The driver uses shared memory as the mechanism for providing information to the shell scripts. An error occurred while writing data from the driver process into the shared memory segment.

Possible Cause: Invalid memory resources or internal error.

Action: Contact NetIQ Support.

NIX005S An error occurred attempting to set an environment variable.

Explanation: The driver uses environment variables for some of the communication between the driver and other processes called from the scripts. An error occurred setting an environment variable.

Possible Cause: There was not enough space to allocate the new environment.

Action: Restart the driver and ensure that there are adequate memory resources for the driver process.

NIX006S An error occurred attempting to execute the script [script].

Explanation: The driver uses scripts to update the system for events from the Identity Vault. An error occurred while attempting to execute one of these scripts.

Possible Cause: The script does not exist on the local system.

Possible Cause: A memory or environment allocation failure occurred.

Action: Restart the driver and ensure that the script exists on the local system.

NIX007S An error occurred attempting to terminate the script [script].

Explanation: The driver uses scripts to update the system for events from the Identity Vault. An error occurred while attempting to terminate the script.

Possible Cause: The script does not exist on the local system.

Possible Cause: A memory or environment allocation failure occurred.

Action: Restart the driver and ensure that the script exists on the local system.

NIX008S The shared memory tool was unable to retrieve a key from the environment.

Explanation: The shared memory tool uses an environment variable to retrieve the key used to unlock the shared memory region and access driver shim data. The tool could not obtain the key from the environment.

Possible Cause: The driver shim cannot set environment variables, or the environment has become corrupt during event processing.

Action: Restart the driver shim process and clear any residual shared memory segments.Action:

OAP Messages

Messages beginning with OAP are issued by driver components while communicating among themselves.

OAP001E Error in SSL configuration. Verify system entropy.

Explanation: Entropy could not be obtained for SSL.

Possible Cause: A source of entropy is not configured for the system.

Action: Obtain and configure a source of entropy for the system.

OAP002E Error in SSL connect. Network address does not match certificate.

Explanation: The SSL client could not trust the SSL server it connected to, because the address of the server did not match the DNS name or IP address that was found in the certificate for the server

Possible Cause: The appropriate credentials are missing from the configuration.

Action: If you cannot resolve the error, collect diagnostic information and call NetIQ Support.

OAP003E Error in SSL connect. Verify address and port.

Explanation: A TCP/IP connection could not be made.

Possible Cause: The server is not running.

Possible Cause: The configuration information does not specify the correct network address or port number.

Action: Verify that the server is running properly.

OAP004E HTTP Error: cause.

Explanation: The username or password provided failed basic authentication.

Possible Cause: The username or password is incorrect.

Action: Verify that username is in full context (cn=user,ou=ctx,o=org or user.ctx.org) and that the password was correctly typed.

OAP005E HTTP Error: Internal Server Error.

Explanation: The server experienced an internal error that prevents the request from being processed.

Possible Cause: A secure LDAP server is not available.

Action: Ensure that the LDAP server is available.

Action: Ensure that the LDAP host and port are configured correctly.

RDXML Messages

Messages beginning with RDXML are issued by the embedded Remote Loader.

RDXML000I nameversion Copyright 2005 Omnibond Systems, LLC. ID=code_id_string.

Explanation: This message identifies the system component version.

Action: No action is required.

RDXML001I Client connection established.

Explanation: A client has connected to the driver. This can be the Metadirectory engine connecting to process events to and from the driver, or a Web-based request to view information or publish changes through the SOAP mechanism.

Action: No action required.

RDXML002I Request issued to start Driver Shim.

Explanation: The driver received a command to start the driver shim and begin processing events.

Action: No action required.

RDXML003E An unrecognized command was issued. The driver shim is shutting down.

Explanation: The driver received an unrecognized command from the Metadirectory engine. The driver shim is shutting down to avoid further errors.

Possible Cause: Network error.

Possible Cause: Invalid data sent to the driver.

Possible Cause: The Metadirectory engine version might have been updated with new commands that are unrecognized by this version of the driver.

Possible Cause: This message is logged when the driver shim process is shut down from the connected system rather than from a Driver object request. The local system can queue an invalid command to the driver shim to simulate a shutdown request and terminate the running process.

Action: Ensure that the network connection is secured and working properly.

Action: Apply updates for the engine or driver if necessary.

Action: If the driver shim process was shut down from the local system, no action is required.

RDXML004I Client Disconnected.

Explanation: A client has disconnected from the driver. This might be the Metadirectory engine disconnecting after a driver shutdown request or a Web-based request that has ended.

Action: No action required.

RDXML005W Unable to establish client connection.

Explanation: A client attempted to connect to the driver, but was disconnected prematurely.

Possible Cause: The client is not running in SSL mode.

Possible Cause: Mismatched SSL versions or mismatched certificate authorities.

Possible Cause: Problems initializing SSL libraries because of improperly configured system entropy settings.

Action: Ensure that both the Metadirectory engine and the driver are running in the same mode: either clear text mode or SSL mode.

Action: If you are using SSL, ensure that the driver and Metadirectory engine have properly configured certificates, and that the driver system is configured properly for entropy.

RDXML006E Error in Remote Loader Handshake.

Explanation: The Metadirectory engine attempted to connect to the driver, but the authorization process failed. Authorization requires that both supply mutually acceptable passwords. Passwords are configured at installation.

Possible Cause: The Remote Loader or Driver object passwords do not match.

Action: Set the Remote Loader and Driver object passwords to the same value for both the driver and the driver shim. Use Designer or Identity Console to modify the driver properties. Re-configure the driver shim on the connected system.

RDXML007I Driver Shim has successfully started and is ready to process events.

Explanation: The Metadirectory engine has requested the driver to start the shim for event processing, and the driver shim has successfully started.

Action: No action required.

RDXML008W Unable to establish client connection from remoteName.

Explanation: A client attempted to connect to the driver, but was disconnected prematurely.

Possible Cause: The client is not running in SSL mode.

Possible Cause: Mismatched SSL versions or mismatched certificate authorities.

Possible Cause: Problems initializing SSL libraries because of improperly configured system entropy settings.

Action: Ensure that both the Metadirectory engine and the driver are running in the same mode: either clear text mode or SSL mode.

Action: If you are using SSL, ensure that the driver and Metadirectory engine have properly configured certificates, and that the driver system is configured properly for entropy.

RDXML009I Client connection established from remoteName.

Explanation: A client has connected to the driver. This can be the Metadirectory engine connecting to process events to and from the driver, or a Web-based request to view information or publish changes through the SOAP mechanism.

Action: No action required.