Implementation Guide

Identity Manager Driver for Midrange: IBM* i (i5/OS* and OS/400*) 4.7

February 23, 2018

Legal Notice

NetIQ Trademarks

For NetIQ trademarks, see the NetIQ Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

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

Contents

About this Book and the Library

This guide describes implementation of the NetIQ® Identity Manager 4.7 driver for the IBM i (formerly i5/OS and OS/400) operating system.

The driver synchronizes data from a connected IBM i system with NetIQ Identity Manager 4.7, the comprehensive identity management suite that allows organizations to manage the full user life cycle, from initial hire, through ongoing changes, to ultimate retirement of the user relationship.

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 Overview

The Identity Manager 4.7 driver for IBM i (i5/OS andOS/400) synchronizes data between the Identity Vault and a connected IBM i system. The driver runs on a target IBM i system. The Identity Vault runs on any platform supported by Identity Manager and communicates with the driver on the connected system over a secure network link.

The driver uses embedded Remote Loader technology to communicate with the Identity Vault, bidirectionally synchronizing changes between the Identity Vault and the connected system. The embedded Remote Loader component, also called the driver shim, runs as a native process on the connected IBM i system. There is no requirement to install Java* on the connected system.

The driver commits changes to the connected system using customizable Control Language (CL) programs that issue native system commands. The publication method uses exits supplied by IBM for notification of changes and a change log to save changes for subsequent publishing.

The IBM i driver uses a scriptable framework, designed so that you can easily add support for existing and future applications.

The Identity Manager driver for IBM i continues the flexibility of previous versions while adding the bidirectional support and Identity Manager policy options available with traditional Identity Manager drivers. New features include:

- Bidirectional synchronization of data without requiring Java or a separate Remote Loader
- Customizable schema to integrate all aspects of IBM i account administration
- Customizable CL programs to handle all data to be synchronized
- Low memory and processor requirements on the Metadirectory server
- No LDAP or Fan-Out core driver configuration

The following sections present a basic overview of the IBM i driver:

- Section 1.1, “Driver Architecture,” on page 11
- Section 1.2, “Configuration Overview,” on page 14

1.1 Driver Architecture

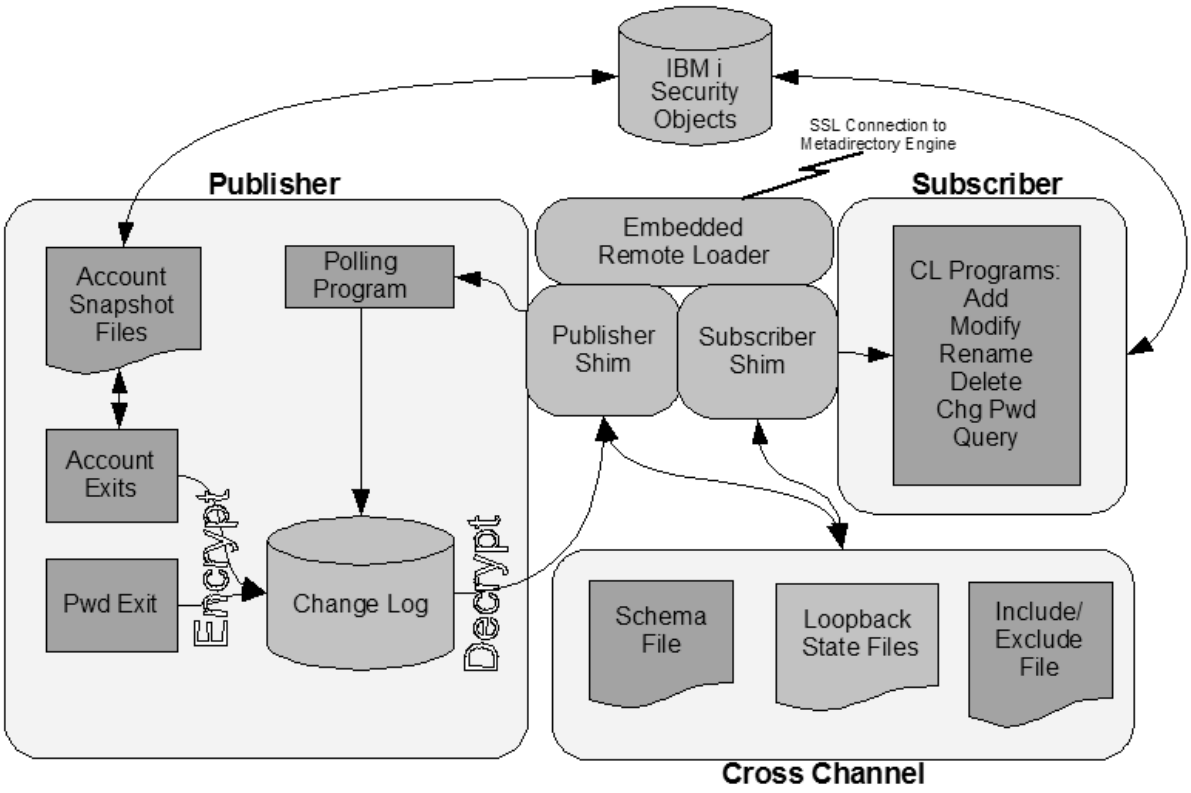
The IBM i driver synchronizes information between the Identity Vault and the IBM i security system.

The Identity Manager detects relevant changes to identities in the Identity Vault and notifies the Subscriber component of the driver. After customizable policy processing, events are sent to the Subscriber shim of the embedded Remote Loader process on the connected system. The Subscriber shim uses a user space to securely pass the information to customizable CL programs that perform the required actions.

The driver uses exits on the IBM i system for notification of identity and password changes. These changes are submitted to the change log. The Publisher shim of the embedded Remote Loader process submits the changes from the change log to the Metadirectory engine as events. The Metadirectory engine processes these events using customizable policies and posts relevant changes to the Identity Vault.

The following illustration shows an overview of the architecture.

Figure 1-1 *IBM i Driver Architecture*



1.1.1 Publisher Channel

The Publisher shim provides identity change information to the Metadirectory engine as XDS event documents. The Metadirectory engine applies policies, takes the appropriate actions, and posts the events to the Identity Vault.

Identity Changes

The Publisher shim uses standard operating system exits for notification that an account has changed.

Table 1-1 *Exit Programs*

Description	Exit Point Name
Directory Maintenance Exit Program	QIBM_QOK_NOTIFY
Change User Profile Exit Program	QIBM_QSY_CHG_PROFILE
Create User Profile Exit Program	QIBM_QSY_CRT_PROFILE
Delete User Profile Exit Program	QIBM_QSY_DLT_PROFILE
Restore User Profile Exit Program	QIBM_QSY_RST_PROFILE

The exit program notifies the Publisher shim of a change. The Publisher shim compares the state of changed objects and the account snapshot files to determine the details of the change, then submits the event to the change log.

Password Changes

The Publisher shim uses QIBM_QSY_VLD_PASSWRD, which is the Validate Password exit program, to capture password change information, and submits it to the change log.

Change Log

The change log stores identity changes in encrypted form. Events are removed from the change log by the Publisher shim at configurable intervals and submitted to the Metadirectory engine for processing. If communication with the Metadirectory engine is temporarily lost, events remain in the change log until communication becomes available again.

Account Snapshot Files

The account snapshot files hold information about the state of users and groups. The Publisher shim maintains the account snapshot files to determine details about changes, because the exits do not provide complete information.

Publisher Shim

The Publisher shim periodically scans the change log for events. When the Publisher shim finds events in the change log, it decrypts, processes, and sends them to the Metadirectory engine in XDS format over a Secure Sockets Layer (SSL) network link.

IBM i profile names are uppercase. The Publisher shim converts profile names to lowercase when sending events to the Metadirectory engine.

1.1.2 Subscriber Channel

The Subscriber channel receives XDS command documents from the Metadirectory engine, stores them as name-value variables in a user space, then calls the appropriate CL programs to handle the command.

The provided CL programs support adds, modifies, renames, and deletes for User and Group objects, and handle password synchronization. You can extend the CL programs to support other object types and events. The CL programs securely access the original command data by calling `GETIDMVAR`, which provides access to the user space.

1.1.3 Scriptable Framework

The interface between the the IBM i security system and the driver shim uses customizable CL programs. You can extend the programs that are provided with the driver to support other applications and databases.

Several helper commands are provided with the driver to enable communication with the driver shim and the change log. An extensible connected system schema file allows you to add your own objects and attributes to those already supported by the driver.

For more information about the CL programs and the scriptable framework, see Section 5.1, “The Scriptable Framework,” on page 31.

1.1.4 Schema File

The configuration of class and attribute definitions for the connected IBM i system is specified using the schema file. You can modify and extend this file to include new objects and attributes. For details about configuring the schema file, see Section 5.2, “The Connected System Schema File,” on page 33.

The schema for the connected system includes two classes: UserProfile and GroupProfile. UserProfile contains fields from both the *USRPRF object and the distribution directory. Exactly one distribution directory entry can be associated with each user profile.

1.1.5 Include/Exclude File

The include/exclude file allows local system policy to enforce which objects are included or excluded from provisioning, on both the Publisher channel and the Subscriber channel, independently. For details about using the include/exclude file, see Section 5.3, “The Connected System Include/Exclude File,” on page 37.

1.1.6 Loopback State Files

The loopback state files are used to provide automatic loopback detection for external applications that do not have mechanisms to perform loopback detection. This loopback detection prevents subscribed events from being published back to the Identity Vault.

1.2 Configuration Overview

This section discusses driver configuration details specific to the IBM i driver. For basic configuration information, see the *Identity Manager 4.7 Administration Guide* on the Identity Manager 4.7 Documentation Web site (https://www.netiq.com/documentation/identity-manager-47/). For detailed information about configuring the IBM i driver, see Chapter 6, “Configuring the IBM i Driver,” on page 43.

1.2.1 Data Flow

Filters and policies control the data flow of users and groups to and from the connected system and the Identity Vault. The Data Flow option, specified during driver import, determines how these filters and policies behave.

- **Bidirectional:** Sets classes and attributes to be synchronized on both the Subscriber and Publisher channels.
- **Application to Identity Vault:** Sets classes and attributes to be synchronized on the Publisher channel only.
- **Identity Vault to Application:** Sets classes and attributes to be synchronized on the Subscriber channel only.

1.2.2 Filter and Schema Mapping

Attributes of i5/OS profiles that correspond to attributes of eDirectory™ User and Group objects are mapped by the default driver filter and the schema mapping policy. The IBM i driver provides a file (`i5os.sch`) that you can use to add auxiliary classes to eDirectory User and Group objects to support many more IBM i user and group attributes.

The Metadirectory engine uses filters to control which objects and attributes are shared. The default filter configuration for the IBM i driver allows objects and attributes to be shared as described in Table 1-2 and Table 1-3.

The eDirectory class User corresponds to the IBM i class UserProfile.

Table 1-2 *Default eDirectory User to i5/OS UserProfile Mapping*

eDirectory User Attribute	i5/OS UserProfile Attribute
CN	USRPRF
Description	TEXT
company	CMPNY
Facsimile Telephone Number	FAXTELNBR
Full Name	FULNAM
Given Name	FSTNAM
Home Directory	HOMEDIR
Login Disabled	STATUS
Postal Address	ADDR1
preferredName	PREFNAM
Telephone Number	TELNBR1
UID	UID
departmentNumber	DEPT
Initials	INITIALS
Title	TITLE
Password Expiration Interval	PWDEXPITV
Surname	LSTNAM
Generational Qualifier	GENQUAL
Group Membership	GroupMembership
nspmDistributionPassword	PASSWORD

The eDirectory class Group corresponds to the IBM i class GroupProfile.

Table 1-3 Default eDirectory Group to IBM i GroupProfile Mapping

eDirectory Group Attribute	IBM i GroupProfile Attribute
CN	USRPRF
Description	TEXT
Member	Members
GID	GID

NOTE: GroupMembership and Members are virtual attributes used to populate the IBM i GRPPRF and SUPGRPPRF user profile fields when the driver is configured to synchronize group membership.

1.2.3 Policies

The Metadirectory engine uses policies to control the flow of information into and out of the Identity Vault. The following table describes the policy functions for the IBM i driver in the default configuration:

Table 1-4 Default i5/OS Driver Policy Functions

Policy	Description
Mapping	Maps the Identity Vault User and Group objects and selected attributes to an IBM i user or group.
Publisher Event	None is provided.
Publisher Matching	Restricts privileged accounts and defines matching criteria for placement in the Identity Vault.
Publisher Create	Defines creation rules for users and groups before provisioning into the Identity Vault.
Publisher Placement	Defines where new users and groups are placed in the Identity Vault.
Publisher Command	Defines password publishing policies.
Subscriber Matching	Defines rules for matching users and groups in the connected system.
Subscriber Create	Defines required creation criteria.
Subscriber Command	Transforms IBM i attributes and defines password subscribing policies.
Subscriber Output	Sends e-mail notifications for password failures and converts information formats from the Identity Vault to the connected system.
Subscriber Event	Restricts events to a specified container.

2 Planning for the IBM i Driver

This section helps you plan for deployment of the NetIQ® Identity Manager 4.7 driver for IBM i (i5/OS and OS/400). Topics include

For more information about planning, see the *Identity Manager 4.7 Installation Guide* on the Identity Manager 4.7 Documentation Web site (https://www.netiq.com/documentation/identity-manager-47/).

2.1 Deployment Planning

- Review Chapter 3, “Installing the IBM i Driver,” on page 21 and Chapter 6, “Configuring the IBM i Driver,” on page 43.
- Consider how you will respond to the installation prompts and other installation decisions.
- Is this a new installation, or are you replacing a Fan-Out driver Platform Services installation? For details about upgrading from the Fan-Out driver, see Chapter 4, “Upgrading from the Fan-Out Driver,” on page 29.
- How do you plan to prototype, test, and roll out your deployment?
- Do you plan to use the include/exclude file on the connected system to limit your initial deployment to a small number of users and groups?
- What are the host names or IP addresses of all systems that will participate in your configuration?
- Will you use the default TCP port numbers?

Table 2-1 *Default TCP Port Numbers*

Purpose	TCP Port Number
Driver shim connection to Metadirectory engine	8090
Secure LDAP port	636
Non-secure LDAP port	389

2.2 Migration Planning

- If you install the password exit during installation, the installation program sets the QPWDVLDPGM system value to *REGFAC and installs a Validate Password exit program. If you want to publish password change information and if you currently use a Password Validation program, you must write a new one that can be registered for the QIBM_QSY_VLD_PASSWRD exit point.
- We recommend that you use password level (IBM i QPWDLVL system value) 2 or above. For details, see Section C.3.1, “Password Levels,” on page 80.
- You can use any security level (IBM i QSECURITY system value) with the driver. IBM recommends security level 40.
- Where are the objects that you plan to manage with the IBM i driver currently stored?
- Can you use a Matching policy to select the objects to manage based on criteria, such as department, group membership, or some other attribute?

2.3 Customization Planning

- You can run more than one instance of the driver to support provisioning to other applications using custom CL programs. If you plan to do this, what library name and Integrated File System (IFS) path will you use for each instance?
- Do you plan to customize the CL programs provided with the driver?

  For details about the provided CL programs, see Table 5-1, “Identity Vault Command Processing CL Programs,” on page 32, Table 5-2, “Other CL Programs,” on page 32, and the CL programs themselves.
- Do you plan to add attributes or classes to the connected system schema file?
- Do you plan to customize policies?

  For details about customizing policies, see the Identity Manager 4.7 Documentation Web site (https://www.netiq.com/documentation/identity-manager-47/).
- Are the resources needed to perform the customization available within your organization?

2.4 Choosing between the Basic and the Advanced Installation Methods

When you import the driver, you are prompted to choose either the Basic Installation or the Advanced Installation. Select Advanced Installation for any of the following:

- You plan to maintain i5/OS attribute information, such as INLMNU, MAXSTG, and HOMEDIR, centrally from the Identity Vault. You do not want to publish changes to this information from the i5/OS system.
- You only want to publish information.
- You only want to subscribe to information.
- You want to use Role-Based Entitlements.
- You want to override the defaults and configure specific i5/OS driver options, such as synchronizing group membership.

To view the driver import configuration settings offered by each installation method, see Section 3.6, “Setting Up the Driver on the Metadirectory Server,” on page 23.

2.5 Establishing a Security-Equivalent User

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

The driver user must be a trustee of the containers where synchronized users and groups reside, with the rights shown in Table 2-2. Inheritance must be set for [Entry Rights] and [All Attribute Rights].

Table 2-2 *Base Container Rights Required by the Driver Security-Equivalent User*

Operation	[Entry Rights]	[All Attribute Rights]
Subscriber notification of account changes (recommended minimum)	Browse	Compare and Read
Creating objects in the Identity Vault without group synchronization	Browse and Create	Compare and Read
Creating objects in the Identity Vault with group synchronization	Browse and Create	Compare, Read, and Write
Modifying objects in the Identity Vault	Browse	Compare, Read, and Write
Renaming objects in the Identity Vault	Browse and Rename	Compare and Read
Deleting objects from the Identity Vault	Browse and Erase	Compare, Read, and Write
Retrieving passwords from the Identity Vault	Browse and Supervisor	Compare and Read
Updating passwords in the Identity Vault	Browse and Supervisor	Compare, Read, and Write

If you do not set Supervisor for [Entry Rights], the driver cannot set passwords. If you do not want to set passwords, set the Subscribe setting for the User class nspmDistributionPassword attribute to Ignore in the filter to avoid superfluous error messages. For details about accessing and editing the filter, see the Identity Manager 4.7 Documentation Web site (https://www.netiq.com/documentation/identity-manager-47/).

For complete information about rights, see the *NetIQ eDirectory™ Administration Guide*.

3 Installing the IBM i Driver

This section provides the information you need to install the NetIQ® Identity Manager 4.7 driver for IBM i (i5/OS and OS/400).

Topics include

3.1 Before You Begin

- Review Chapter 2, “Planning for the IBM i Driver,” on page 17.
- 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).

3.2 Required Knowledge and Skills

To successfully install, configure, and use the driver, you must have system administration skills and rights for Identity Manager and the target system. You must be proficient with using iManager to configure Identity Manager drivers. You must be familiar with the facilities of the IBM i driver, and you must have developed a deployment plan.

For an overview of driver facilities, see Chapter 1, “Overview,” on page 11.

For information about planning for the i5/OS driver, see Chapter 2, “Planning for the IBM i Driver,” on page 17.

For information about administering your i5/OS system, see your IBM system documentation.

3.3 Prerequisites

3.3.1 Connected System Requirements

One of the following operating systems:

- ❒ IBM i
- ❒ OS/400
- ❒ i5/OS

For more information about supported platforms and operating environments, see the Identity Manager 4.7 Drivers Documentation Web site (https://www.netiq.com/documentation/identity-manager-47-drivers). From this index page, you can select a readme file associated with the platform(s) for which you need support.

3.3.2 Identity Vault Requirements

- ❒ NetIQ Identity Manager 4.7 with the latest Support Pack

3.4 Getting the Installation Files

1. Obtain the most recent distribution of the Identity Manager 4.7 driver for IBM i from the NetIQ Downloads Web site (https://dl.netiq.com/index.jsp).

   The driver is part of the Identity Manager Integration Module 4.7 for Midrange.
2. The driver distribution is found in /bidirectional/AS400

Table 3-1 *Folder Contents*

Filename	Description
`Metadirectory/i5os.xml`	Driver rules file used to create the Driver object on the Metadirectory server
`Metadirectory/i5os.sch`	File for extending the eDirectory™ schema to add auxiliary classes to User and Group objects to support IBM i profile and distribution directory attributes
`i5osdrv.sav`	Driver shim distribution package

3.5 Extending the Schema for Identity Manager

Attributes of IBM i profiles that correspond to attributes of eDirectory User and Group objects are mapped by the default driver mapping policy. You must extend the schema if you want to use the Identity Vault to manage additional IBM i attributes.

For details about the attributes in the default mapping policy, see Table 1-2, “Default eDirectory User to i5/OS UserProfile Mapping,” on page 15 and Table 1-3, “Default eDirectory Group to IBM i GroupProfile Mapping,” on page 16.

Extending the schema adds auxiliary classes to eDirectory User and Group objects for the profile and distribution directory attributes.

1. In iManager, select the *Extend Schema* task under *Schema*.
2. Select *Import data from file on disk*, then click *Next*.

3 Select a file type of *Schema File*.

4 Type or browse for `i5os.sch` as the file to import, then click *Next*.

5 Specify the host name or IP address and the LDAP port number of your Metadirectory server.

To connect to the non-secure LDAP port (389), you must have the *Require TLS for Simple Binds with Password* option disabled on your LDAP Group. If necessary, you can edit this option using the *LDAP Options* task under *LDAP* in iManager. For details, see the *NetIQ eDirectory Administration Guide*.

6 Select *Authenticated login* and log in as ADMIN or another user with rights to extend the schema.

7 Click *Next* to go to the summary.

8 Click *Finish* to extend the schema.

3.6 Setting Up the Driver on the Metadirectory Server

1 In iManager, select *Identity Manager Administration*.

2 Under *Administration*, select *Identity Manager Overview*.

3 Select *Driver Sets* and choose your driver set name below.

4 Select *Drivers* > *Add driver*, then click *Next*.

5 Select *Import a driver configuration from the client (.XML file)*.

5a Under *Show*, select <*all configurations*>.

5b Under *Configurations*, browse to select *i50s-IDM3_5_0-V3.xml*.

5c Click *Next*.

6 Type in a name for the driver, select an installation method, then click *Next*.

NOTE: For details about choosing the appropriate installation method, see Section 2.4, “Choosing between the Basic and the Advanced Installation Methods,” on page 18.

7 Specify the configuration settings as described in the following table, then click *Next*.

Configuration Setting	Action	Installation Method
Data Flow	Select *Bidirectional*, *Application to Identity Vault*, or *Identity Vault to Application*. For details, see “Data Flow” on page 44.	Advanced
Polling Interval	Specify the number of seconds the Publisher shim waits after running the polling CL program and sending events from the change log to the Metadirectory engine. For details, see “Polling Interval” on page 46.	Advanced

Configuration Setting	Action	Installation Method
Base Container	Specify the Identity Vault container where synchronized users and groups reside. You can specify separate containers for users and groups by updating the driver properties later. For details, see "User Base Container" on page 48 and "Group Base Container" on page 48.	Basic and Advanced
Enable Entitlements	Select *Yes* or *No*. For details, see "Enable Entitlements" on page 44.	Advanced
Synchronize Group Membership	Select *Yes* or *No*. For details, see "Synchronize Group Membership" on page 47.	Advanced
Remote Host Name and Port	Specify the host name or IP address and TCP port number of the driver shim on your IBM i connected system. The default port number is 8090.	Basic and Advanced
Use SSL	Select *Yes* or *No*. For details, see "Use SSL" on page 44.	Advanced
Driver Object Password Remote Loader Password	Specify secure passwords and remember them. You must enter them in Step 7h on page 26 when you install the driver shim on the connected system. For details, see "Driver Object Password" on page 45 and "Remote Loader Password" on page 46.	Basic and Advanced

8 Click *Define Security Equivalences* and make the driver equivalent to ADMIN or another high-rights user so the driver can obtain information from the Identity Vault and create users and groups there.

NOTE: For details about the rights required by the user, see Table 2-2, "Base Container Rights Required by the Driver Security-Equivalent User," on page 19.

9 (Optional) Click *Exclude Administrative Roles* to exclude users with administrative rights from being processed by the driver.

10 Click *Finish* to complete the driver installation.

11 Start the driver.

Click the upper right corner of the driver icon, then click *Start driver*.

3.7 Installing the Driver Shim on the Connected System

You can install multiple instances of the driver on one IBM i system if necessary to support applications via customized CL programs. By default, the driver shim installation uses the `I5OSDRV` library and the `/usr/local/i5osdrv` IFS path.

For details see Section C.4, "Driver Shim Library and IFS Contents," on page 81.

The driver uses an embedded Remote Loader. It is not necessary to install Java on the connected system.

1. Sign on as QSECOFR or an equivalent user to the target IBM i system.
2. Use the following command to create a temporary file to contain the driver shim distribution package:

   ```
   CRTSAVF FILE(QSYS/NOVELLDIST)
   ```

3. On the workstation that you used in Step 2 on page 22, use FTP to transfer `i5osdrv.sav` to the `NOVELLDIST` file just created in Step 2 on your target IBM i system:

   ```
   >ftp server_address
   (Authenticate to the server)
   ftp> cd qsys
   ftp> bin
   ftp> put i5osdrv.sav novelldist.file
   ftp> quit
   ```

4. On the IBM i system, execute the following command to restore the driver shim distribution library:

   ```
   RSTLIB SAVLIB(NOVELLDIST) DEV(*SAVF) SAVF(QSYS/NOVELLDIST)
   ```

5. Remove the temporary file:

   ```
   DLTF FILE(QSYS/NOVELLDIST)
   ```

6. Execute the installation program:

   ```
   CALL PGM(NOVELLDIST/INSTALL)
   ```

7. Respond to the prompts as appropriate to complete the installation:

   7a Read and accept the license agreement.

   7b Specify the driver library name and the driver IFS path. These default to `I5OSDRV` and to `/usr/local/i5osdrv` respectively.

   ```
   The driver requires a library in i5os and a path in the Integrated File
   System.
   Library: I5OSDRV

   IFS Path: /user/local/i5osdrv
   ```

   7c Specify the TCP port number for the driver shim to listen on. The default port is 8090.

   ```
   The driver must listen on a port for connections from the Metadirectory
   server.

   Remote Loader Port: 8090
   ```

   7d Create a new User profile for the driver or specify an existing profile.

   ```
   The driver requires a User Profile with *SECADM and *ALLOBJ Special
   Privileges. A new Profile can be created by the installation, or an
   existing Profile can be used.
   Create New Profile: Y

   User Profile: I5OSDRV
   ```

   7e Specify a subsystem and a job queue for the driver.

   ```
   The driver must be assigned to a subsystem and a job queue.

   Subsystem: QSYSWRK

   Job Queue: QSYSNOMAX
   ```

7f Specify whether the driver should be automatically started when the system starts.

```
Autostart Job at IPL: Y
```

7g Specify whether to install the profile exits, the distribution directory exit, and the password exit.

If you do not install the exits, the driver cannot publish the corresponding information.

```
Exits must be installed for the driver to publish profile and password
changes to the Identity Vault.

Install Profile Exits: Y
   QIBM_QSY_CHG_PROFILE
   QIBM_QSY_CRT_PROFILE
   QIBM_QSY_DLT_PROFILE
   QIBM_QSY_RST_PROFILE

Install Distribution Directory Exit: Y
   QIBM_QOK_NOTIFY

Install Password Exit: Y
   QIBM_QSY_VLD_PASSWRD
```

7h Provide the Remote Loader and Driver object passwords that you entered when creating the driver in Step 7 on page 23.

```
Enter Remote Loader Password:
Confirm Remote Loader Password:
Enter Driver Object Password:
Confirm Driver Object Password:
```

7i Specify the Metadirectory server host name or IP address and secure LDAP port number.

These are used to secure the driver shim with SSL.

```
DNS name or IP address of the LDAP Server:
TCP port number for LDAP SSL (default 636):
```

8 Start the driver shim.

Enter `GO I5OSDRV/I5OSDRV`, then select option 1.

If you did not use the default library name, substitute your driver library name as shown in the following example:

`GO` *`yourDriverLibrary`*`/I5OSDRV`

3.8 Post-Installation Tasks

1 If desired, set *Startup Option* on the Driver Configuration page to *Auto start*. This causes the driver to start when the Metadirectory engine starts.

NOTE: By default, the installation program sets the driver shim to start automatically on the connected system.

---

2 Activate the driver.

Identity Manager and Identity Manager drivers must be activated within 90 days of installation or they shut down. At any time during the 90 days, or afterward, you can activate Identity Manager products.

For details about activating NetIQ Identity Manager Products, see the *Identity Manager 4.7 Installation Guide* on the Identity Manager 4.7 Documentation Web site (https://www.netiq.com/documentation/identity-manager-47/).

You can use the I5OSDRV menu on the connected system at any time to change the driver shim configuration. You can configure the Remote Loader and driver passwords, and the SSL settings. For details about using the I5OSDRV menu, see Section C.1, “Using the I5OSDRV Menu,” on page 79.

3.9 Uninstalling the Driver

1. Go to the I5OSDRV menu, select option 6, and respond to the prompts.

   For details about using the I5OSDRV menu, see Section C.1, “Using the I5OSDRV Menu,” on page 79.
2. To remove the Driver object from eDirectory, click *Delete Driver* on the Identity Manager Overview page in iManager.

4 Upgrading from the Fan-Out Driver

This section provides the information you need if you are upgrading from the Identity Manager Fan-Out driver to the Identity Manager 4.7 driver for IBM i (i5/OS and OS/400).

Topics include

We recommend that you perform the upgrade in a test environment similar to your production environment before upgrading production systems.

Before beginning the upgrade process, review Chapter 3, “Installing the IBM i Driver,” on page 21.

To prepare for installing the upgrade:

1. Verify that you have the required knowledge and skills.

   For details, see Section 3.2, “Required Knowledge and Skills,” on page 21.
2. Ensure that the prerequisites are met.

   For details, see Section 3.3, “Prerequisites,” on page 21.
3. Prepare the distribution files for installation.

   For details, see Section 3.4, “Getting the Installation Files,” on page 22.

The Fan-Out driver provides one-way synchronization to a heterogeneous mix of systems including Linux and UNIX systems, and IBM i and z/OS* systems. The Fan-Out driver also provides authentication redirection from those systems.

Moving to the IBM i driver provides two main advantages.

- **Bidirectional Synchronization:** The IBM i driver allows synchronization from the connected IBM i system.
- **Standard Identity Manager Policies That Simplify Customization:** The Fan-Out driver makes minimal use of Identity Manager policies.

Consider the following before migrating from the Fan-Out driver to the IBM i driver.

- **Heterogeneity:** The Fan-Out driver supports operating systems in addition to IBM i. You can continue to use the Fan-Out driver for those systems while using the IBM i driver for IBM i systems.
- **Scalability:** The Fan-Out driver can fan out identities to any number of systems. The IBM i driver can replicate to only one system.

  One IBM i driver is required for each connected system. For best performance, we recommend no more than a total of 60 drivers.
- **Authentication Redirection:** The Fan-Out driver uses authentication redirection from IBM i using the Change Password Validation Program exit. The IBM i driver uses bidirectional password synchronization.

4.1 Migrating Fan-Out Driver Platform Services to the IBM i Driver

Perform the following steps on your target platform system:

1. Stop the ASAMRCVR job.
2. Remove the ASAMRCVR from any subsystem autostart entries.
3. Install the driver shim on the connected system.

   For details, see Section 3.7, “Installing the Driver Shim on the Connected System,” on page 24.

4.2 Configuring the Driver

1. Install and set up the IBM i driver on the Metadirectory server.

   For details, see Section 3.6, “Setting Up the Driver on the Metadirectory Server,” on page 23.
2. Make any required policy modifications.

   Create or modify an appropriate policy to use the alternative naming attribute if one was used by the Fan-Out driver. For more information about policy customization, see the Identity Manager 4.7 Documentation Web site (https://www.netiq.com/documentation/identity-manager-47/).
3. Start the IBM i driver.

   Click the upper right corner of the driver icon, then click *Start driver*.
4. Migrate the users to make new associations. For details, see Section 6.3.1, “Migrating Identities from the Identity Vault to the Connected System,” on page 50 and Section 6.3.2, “Migrating Identities from the Connected System to the Identity Vault,” on page 50.

4.3 Post-Migration Tasks

Perform the steps listed in Section 3.8, “Post-Installation Tasks,” on page 26. After the new driver is operating properly, you can remove the Fan-Out driver components as follows:

1. Delete the Platform object from the Fan-Out driver configuration.
2. Remove Platform Services from the connected system:
   - **2a** Remove `ASAMPWD` from the QPWDVLDPGM system value.
   - **2b** Remove the `ASAM` library from your library list.
   - **2c** Remove the `ASAM` library and `/usr/local/ASAM` directory created by Platform Services installation.
3. If this is the last platform being served by the Fan-Out driver, you can uninstall the core driver:
   - **3a** Remove the `ASAM` directory from the file system.
   - **3b** Remove the ASAM System container object and all of its subordinates from the tree.
   - **3c** Uninstall the Fan-Out driver plug-ins.

5 Customizing the IBM i Driver

This section provides information about available resources for customizing the Identity Manager 4.7 driver for IBM i (i5/OS and OS/400).

Topics include

For details about the filters and policies provided with the IBM i driver, see Section 1.2.2, “Filter and Schema Mapping,” on page 15 and Section 1.2.3, “Policies,” on page 16.

5.1 The Scriptable Framework

The IBM i driver provides a comprehensive scriptable framework that you can use to add to the built-in support for the IBM i security system, and to add support for other applications.

The IBM i driver uses Control Language (CL) programs to implement driver functions. The scriptable framework includes components that simplify the job of extending the driver to support new applications.

- Embedded Remote Loader
  - Full SSL support, and an installer to easily configure the certificates
  - Web access to debugging information from the embedded Remote Loader
- Encrypted change log that stores changes from the application to the Identity Vault if there is a communication problem
- Loopback detection system to prevent subscribed events from being published back to the Identity Vault
- Helper programs for securely passing variables to and from the CL programs through a user space
- Easily extendable connected system schema file to support any application
- Include/exclude file for simplified testing and deployment by the platform administrator
- Event support, both for applications that have exits or callouts, and for applications that must be polled for changes

The names of objects and attributes in the CL programs are the names specified in the connected system schema file.

The following tables describe the major CL programs.

Table 5-1 *Identity Vault Command Processing CL Programs*

CL Program	Identity Vault Event
ADDGROUP	Add Group
ADDGRPMEM	Add Group Member
ADDUSER	Add User
DELGROUP	Delete Group
DELUSER	Delete User
MODGROUP	Modify Group
MODPWD	Password Change
MODUSER	Modify User
RMVGRPMEM	Remove Group Member
QUERY	Query
RENGROUP	Rename Group
RENUSER	Rename User

Table 5-2 *Other CL Programs*

CL Program	Purpose
ASSIGNVAR	Obtains a value from the Identity Vault or uses a default
ERROR	Trace message helper
EXEC	Executes an i5/OS command
FAILED	Trace message helper
POLL	Called to detect changes in user applications
STATUS	Trace message helper
STOREPWD	Stores a password
SUBSCRIBER	Calls the appropriate CL program based on the type of event and object
TRACE	Trace message helper
TRACEMSGS	Trace message helper

5.2 The Connected System Schema File

The schema file on the connected system is used to specify the classes and attributes that are available. The schema file is located in the driver IFS path at `schema/schema.def`. If you installed the driver using the default driver IFS path, the schema file is `/usr/local/i5osdrv/schema/schema.def`.

The schema file is read by the driver shim when the Metadirectory engine requests it. This typically happens at driver startup. The schema file is also used by the Policy Editor to map the schema of the Identity Vault to the schema of the external application.

If you change the schema file, you must restart the driver shim and the driver.

The CL programs that are provided with the driver depend on the classes and attributes in the schema file that is provided with the driver.

5.2.1 Schema File Syntax

Each line in the schema file represents an element and must begin with the element name: SCHEMA, CLASS, or ATTRIBUTE.

The first element of the schema file is the schema definition. The schema definition is followed by class definitions. Each class definition can contain attribute definitions.

Except for the values of class and attribute names, the contents of the schema file are case insensitive.

Comments

Lines that begin with an octothorpe (#) are comments.

```
# This is a comment.
```

Schema Definition

The first line in the schema file that is not a comment must be the schema definition.

```
SCHEMA [HIERARCHICAL]
```

HIERARCHICAL specifies that the target application is not a flat set of users and groups, but is organized by hierarchical components, such as a directory-based container object.

Class Definition

`CLASS` *`className`* `[CONTAINER]`

You must specify a class name.

Add the CONTAINER keyword if objects of this class can contain other objects.

The class definition is ended by another class definition or by the end of the file.

Attribute Definition

Any number of attribute definitions can follow a class definition. Attribute definitions define attributes for the class whose definition they follow.

ATTRIBUTE *attributeName* [*TypeAndProperties*]

An attribute name is required.

If no attribute type is specified, the attribute has the string type. The allowable types are

- STRING
- INTEGER
- STATE
- DN

The allowable attribute properties are

- REQUIRED
- NAMING
- MULTIVALUED
- CASESENSITIVE
- READONLY

5.2.2 Example Schema File

```
#########################################################################
#  IBM i Driver Schema File
#
# Syntax:
#   SCHEMA [HIERARCHICAL]
#
#     HIERARCHICAL defines whether the schema has a hierarchy.
#                  Default is false.
#
#   CLASS <class-name> [CONTAINER]
#
#     CONTAINER defines whether the class is a container class.
#               Default is false.
#
#   ATTRIBUTE <attribute-name> [CASESENSITIVE] [MULTIVALUED] [NAMING]
#                              [READONLY] [REQUIRED] [STRING] [INTEGER]
#                              [STATE] [DN]
#
#     CASESENSITIVE defines this attribute to be case sensitive.
#                   Default is false.
#
#     MULTIVALUED defines this attribute to be multivalue.
#                 Default is false.
#
#     NAMING defines this attribute as the class naming attribute.
#            Default is false.
#
#     READONLY defines this attribute to be read-only.
#              Default is false.
#
#     REQUIRED defines this attribute to be required for class
#              definition.
#              Default is false.
#
#     STRING defines this attribute to be of type string.
#            String is the default type.
#
#     INTEGER defines this attribute to be of type integer.
#            String is the default type.
#
#     STATE defines this attribute to be of type Boolean (TRUE or
```

```
#           FALSE)
#            String is the default type.
#
#     DN defines this attribute to be a distinguished name
#       (referential)
#            String is the default type.
#
#########################################################################

SCHEMA

  CLASS UserProfile

    ATTRIBUTE USRPRF NAMING REQUIRED  # User Profile Name
    ATTRIBUTE PASSWORD                #
    ATTRIBUTE PWDEXP                  # Password Expired *YES or *NO
    ATTRIBUTE STATUS                  # *ENABLED or #DISABLED
    ATTRIBUTE USRCLS                  # User Class
    ATTRIBUTE ASTLVL                  # Assistance Level
    ATTRIBUTE CURLIB                  # Current Library
    ATTRIBUTE INLPGM                  # Initial Program to Call
    ATTRIBUTE INLMNU                  # Initial Menu
    ATTRIBUTE LMTCPB                  # Limit Capabilities
    ATTRIBUTE TEXT                    # Text Description
    ATTRIBUTE SPCAUT                  # Special Authority
    ATTRIBUTE SPCENV                  # Special Environment
    ATTRIBUTE DSPSGNINF               # Display sign-on information
    ATTRIBUTE PWDEXPITV               # Password Expiration Interval
    ATTRIBUTE LMTDEVSSN               # Limit Device Sessions
    ATTRIBUTE KBDBUF                  # Keyboard Buffering
    ATTRIBUTE MAXSTG                  # Maximum Allowed Storage
    ATTRIBUTE PTYLMT                  # Highest Schedule Priority
    ATTRIBUTE JOBD                    # Job Description
    ATTRIBUTE GRPPRF                  # Group Profile
    ATTRIBUTE OWNER                   # Owner
    ATTRIBUTE GRPAUT                  # Group Authority
    ATTRIBUTE GRPAUTTYP               # Group Authority Type
    ATTRIBUTE SUPGRPPRF MULTIVALUED   # Supplemental Groups
    ATTRIBUTE ACGCDE                  # Accounting Code
    ATTRIBUTE MSGQ                    # Message Queue
    ATTRIBUTE DLVRY                   # Message Queue Delivery Method
    ATTRIBUTE SEV                     # Message Severity Code Filter
    ATTRIBUTE PRTDEV                  # Print Device
    ATTRIBUTE OUTQ                    # Output Queue
    ATTRIBUTE ATNPGM                  # Attention Program
    ATTRIBUTE SRTSEQ                  # Sort Sequence
    ATTRIBUTE LANGID                  # Language ID
    ATTRIBUTE CNTRYID                 # Country or Region ID
    ATTRIBUTE CCSID                   # Coded Character Set ID
    ATTRIBUTE CHRIDCTL                # Character Identifier Control
    ATTRIBUTE SETJOBATR               # Locale Job Attributes
    ATTRIBUTE LOCALE                  # Locale
    ATTRIBUTE USROPT                  # User Options
    ATTRIBUTE UID INTEGER             # User ID number
    ATTRIBUTE GID INTEGER             # Group ID number
    ATTRIBUTE HOMEDIR                 # Home Directory
    ATTRIBUTE GroupMembership MULTIVALUED # Virtual attr for GRPPRF &
                                          # SUPGRPPRF
# Distribution Directory Entry Attributes
    ATTRIBUTE USRID                   # User Identifier
    ATTRIBUTE USRD                    # User Description
    ATTRIBUTE USER                    # User Profile
    ATTRIBUTE SYSNAME                 # System Name
    ATTRIBUTE NETUSRID                # Network User ID
    ATTRIBUTE LSTNAM                  # Last Name
    ATTRIBUTE FSTNAM                  # First Name
    ATTRIBUTE MIDNAM                  # Middle Name
    ATTRIBUTE PREFNAM                 # Preferred Name
    ATTRIBUTE FULNAM                  # Full Name
    ATTRIBUTE DEPT                    # Department
```

```
  ATTRIBUTE TITLE                   # Job Title
  ATTRIBUTE CMPNY                   # Company
  ATTRIBUTE TELNBR1                 # Telephone Number 1
  ATTRIBUTE TELNBR2                 # Telephone Number 2
  ATTRIBUTE FAXTELNBR               # FAX Telephone Number
  ATTRIBUTE LOC                     # Location
  ATTRIBUTE BLDG                    # Building
  ATTRIBUTE OFC                     # Office
  ATTRIBUTE ADDR1                   # Address Line 1
  ATTRIBUTE ADDR2                   # Address Line 2
  ATTRIBUTE ADDR3                   # Address Line 3
  ATTRIBUTE ADDR4                   # Address Line 4
  ATTRIBUTE INDUSR                  # Indirect User
  ATTRIBUTE PRTPERS                 # Print Private Mail
  ATTRIBUTE PRTCOVER                # Print Cover Page
  ATTRIBUTE NFYMAIL                 # Mail Notification
  ATTRIBUTE NFYMSGS                 # Messages
  ATTRIBUTE TEXT                    # Text
  ATTRIBUTE CMDCHRID                # Command Character Identifier
  ATTRIBUTE COUNTRY                 # Country or Region ID
  ATTRIBUTE ADMD                    # Administration Domain
  ATTRIBUTE PRMD                    # Private Management Domain
  ATTRIBUTE SURNAM                  # Surname
  ATTRIBUTE GIVENNAM                # Given Name
  ATTRIBUTE INITIALS                # Initials
  ATTRIBUTE GENQUAL                 # Generational Qualifier
  ATTRIBUTE ORG                     # Organization
  ATTRIBUTE ORGUNIT MULTIVALUED     # Organizational Units
  ATTRIBUTE DMNDFNATR MULTIVALUED   # Domain-defined Attributes
  ATTRIBUTE USRDFNFLD MULTIVALUED   # User-defined Fields
  ATTRIBUTE MSFSRVLVL               # Mail Service Level
  ATTRIBUTE PREFADR                 # Preferred Address
  ATTRIBUTE CCMAILADR               # cc:Mail Address
  ATTRIBUTE CCMAILCMT               # cc:Mail Comment
  ATTRIBUTE ALWSYNC                 # Allow Synchronization
  ATTRIBUTE DLOOWN                  # DLO Owner

CLASS GroupProfile

  ATTRIBUTE USRPRF NAMING REQUIRED  # User Profile Name
  ATTRIBUTE PWDEXP                  # Password Expired *YES or *NO
  ATTRIBUTE STATUS                  # *ENABLED or #DISABLED
  ATTRIBUTE USRCLS                  # User Class
  ATTRIBUTE ASTLVL                  # Assistance Level
  ATTRIBUTE CURLIB                  # Current Library
  ATTRIBUTE INLPGM                  # Initial Program to Call
  ATTRIBUTE INLMNU                  # Initial Menu
  ATTRIBUTE LMTCPB                  # Limit Capabilities
  ATTRIBUTE TEXT                    # Text Description
  ATTRIBUTE SPCAUT                  # Special Authority
  ATTRIBUTE SPCENV                  # Special Environment
  ATTRIBUTE DSPSGNINF               # Display sign-on information
  ATTRIBUTE PWDEXPITV               # Password Expiration Interval
  ATTRIBUTE LMTDEVSSN               # Limit Device Sessions
  ATTRIBUTE KBDBUF                  # Keyboard Buffering
  ATTRIBUTE MAXSTG                  # Maximum Allowed Storage
  ATTRIBUTE PTYLMT                  # Highest Schedule Priority
  ATTRIBUTE JOBD                    # Job Description
  ATTRIBUTE GRPPRF                  # Group Profile
  ATTRIBUTE OWNER                   # Owner
  ATTRIBUTE GRPAUT                  # Group Authority
  ATTRIBUTE GRPAUTTYP               # Gropu Authority Type
  ATTRIBUTE SUPGRPPRF MULTIVALUED   # Supplemental Groups
  ATTRIBUTE ACGCDE                  # Accounting Code
  ATTRIBUTE DOCPWD                  # Document Password
  ATTRIBUTE MSGQ                    # Message Queue
  ATTRIBUTE DLVRY                   # Delivery
  ATTRIBUTE SEV                     # Severity Code Filter
  ATTRIBUTE PRTDEV                  # Print Device
  ATTRIBUTE OUTQ                    # Output Queue
```

```
ATTRIBUTE ATNPGM                # Attention Program
ATTRIBUTE SRTSEQ                # Sort Sequence
ATTRIBUTE LANGID                # Language ID
ATTRIBUTE CNTRYID               # Country or Region ID
ATTRIBUTE CCSID                 # Coded Character Set ID
ATTRIBUTE CHRIDCTL              # Character Identifier Control
ATTRIBUTE SETJOBATR             # Locale Job Attributes
ATTRIBUTE LOCALE                # Locale
ATTRIBUTE USROPT                # User Options
ATTRIBUTE UID INTEGER           # User ID number
ATTRIBUTE GID INTEGER           # Group ID number
ATTRIBUTE HOMEDIR               # Home Directory
ATTRIBUTE EIMASSOC              # EIM Association
ATTRIBUTE Members MULTIVALUED   # Virtual attribute that has
                                # all members
```

5.3 The Connected System Include/Exclude File

You can use an optional include/exclude file on the connected system to control which identities are or are not synchronized between the Identity Vault and the connected system. The include/exclude file is located in the driver IFS path at `conf/include-exclude.conf`. If you installed the driver using the default driver IFS path, the include/exclude file is `/usr/local/i5osdrv/conf/include-exclude.conf`.

The file is read when the driver shim starts. If you make changes to it, you must restart the driver shim.

The include/exclude file can contain include rules and exclude rules. To ensure optimal performance, each include/exclude file should contain no more than 50 entries total.

A default file that excludes many common i5/OS user IDs and groups, such as QSECOFR, is created by the installation process.

You can use the include/exclude file to phase in your deployment of the IBM i driver, excluding most users and groups at first, and then adding more as you gain confidence and experience.

- Section 5.3.1, “Include/Exclude Processing,” on page 37
- Section 5.3.2, “Include/Exclude File Syntax,” on page 38
- Section 5.3.3, “Example Include/Exclude Files,” on page 41

5.3.1 Include/Exclude Processing

Identity Vault events for identities that match an exclude rule are discarded by the Subscriber shim. Local events for identities that match an exclude rule are not sent to the Metadirectory engine by the Publisher shim.

Included identities are treated normally by the Subscriber and Publisher shims.

Identities that do not match an include rule or an exclude rule in the file are included.

Identities are matched in the following priority:

1. Channel-specific (Publisher or Subscriber) exclude rules
2. Channel-specific include rules
3. General exclude rules
4. General include rules

Within each level of this matching priority, identities are matched against rules in the order that the rules appear in the file. The first rule that matches determines whether the identity is included or excluded.

5.3.2 Include/Exclude File Syntax

Except for class names, attribute names, and the values to match, the contents of the include/exclude file are case insensitive.

The include/exclude file can contain any number of include sections, exclude sections, and single-line rules.

Include sections and exclude sections can contain class matching rules, and class matching rules can contain attribute matching rules. Include sections and exclude sections can also contain association matching rules.

Include and exclude sections can be contained in subscriber and publisher sections to limit their scope to the specified channel.

Class and attribute names used in the include/exclude file must correspond to the names specified in the schema file. For details about the schema file, see Section 5.2, “The Connected System Schema File,” on page 33.

Comments

Lines that begin with an octothorpe (#) are comments.

```
# This is a comment.
```

Subscriber and Publisher Sections

Subscriber and publisher sections limit the include and exclude sections they contain to the specified channel.

A subscriber section begins with a subscriber line and ends with an endsubscriber line.

```
SUBSCRIBER
  .
  .
  .
ENDSUBSCRIBER
```

A publisher section begins with a publisher line and ends with an endpublisher line.

```
PUBLISHER
  .
  .
  .
ENDPUBLISHER
```

Each subscriber and publisher section can contain include and exclude sections.

Include and Exclude Sections

Include and exclude sections provide rules to specify which objects are to be included or excluded from synchronization.

An include section begins with an include line and ends with an endinclude line.

```
INCLUDE
  .
  .
  .
ENDINCLUDE
```

An exclude section begins with an exclude line and ends with an endexclude line.

```
EXCLUDE
  .
  .
  .
ENDEXCLUDE
```

You can use class matching rules and association matching rules within an include section and an exclude section.

Class Matching Rules

Use a class matching rule within an include section or an exclude section to specify the name of a class of objects to include or exclude.

A class matching rule is defined by a class line that specifies the name of the class and ends with an endclass line.

```
CLASS className
  .
  .
  .
ENDCLASS
```

You can use attribute matching rules within a class matching rule.

Attribute Matching Rules

You can use attribute matching rules within a class matching rule to limit the objects that are included or excluded. If no attribute matching rules are specified for a class, all objects of the specified class are included or excluded.

An attribute matching rule comprises an attribute name, an equals sign (=), and an expression. The expression can be an exact value, or it can use limited regular expressions. For details about limited regular expressions, see “Limited Regular Expressions” on page 40.

```
attributeName=expression
```

Multiple attribute matching rules can be specified for a given class.

Attribute matching rules within a class matching rule are logically ANDed together. To logically OR attribute matching rules for a class, specify multiple class matching rules. For example, the following include/exclude file excludes both user01 and user02:

```
# Exclude the User object if its USRPRF is USER01 or USER02.
EXCLUDE
CLASS UserProfile
    USRPRF=USER01
ENDCLASS
CLASS UserProfile
    USRPRF=USER02
ENDCLASS
ENDEXCLUDE
```

Association Matching Rules

You can specify association matching rules in an include or exclude section. Association matching rule expressions can specify an exact association or a limited regular expression. For details about limited regular expressions, see “Limited Regular Expressions” on page 40.

By default, an association is defined as the profile name. Association formation can be customized in the Subscriber CL programs.

For example, to exclude the QSECOFR user, specify

```
EXCLUDE
  QSECOFR
ENDEXCLUDE
```

Single-Line Rules

`[SUBSCRIBER|PUBLISHER] INCLUDE|EXCLUDE [`*`className`*`] `*`objectSelection`*

Where *objectSelection* can be

{*associationMatch* | *attributeName=expression*}

Single-line rules can specify the Subscriber or Publisher channel at the start of the rule. If a channel is specified, the rule applies only to that channel. Otherwise it applies to both channels.

You must specify whether the rule is to include or exclude the objects it matches.

You can specify a class name to limit matches to only objects of that class.

You must specify either an association or an attribute matching expression. The syntax of the association and attribute matching expression is the same as that of association matching rules and attribute matching rules previously described. For details, see “Association Matching Rules” on page 40 and “Attribute Matching Rules” on page 39.

For example, to ignore events from the ADMIN user in the Identity Vault:

```
# Do not subscribe to events for the ADMIN user.
SUBSCRIBER EXCLUDE adminUserProfile
```

Limited Regular Expressions

A limited regular expression is a pattern used to match a string of characters.

Character matching is case sensitive.

Any literal character matches that character.

A period (`.`) matches any single character.

A bracket expression is a set of characters enclosed by left (`[`) and right (`]`) brackets that matches any listed character. Within a bracket expression, a range expression is a pair of characters separated by a hyphen, and is equivalent to listing all of the characters that sort between the given characters. For example, `[0-9]` matches any single digit.

An asterisk (`*`) indicates that the preceding item is matched zero or more times.

A plus sign (`+`) indicates that the preceding item is matched one or more times.

A question mark (`?`) indicates that the preceding item is matched zero or one times.

You can use parentheses to group multiple expressions into a single item. For example, `(abc)+` matches `abc`, `abcabc`, `abcabcabc`, etc. Nesting of parentheses is not supported.

5.3.3 Example Include/Exclude Files

Example 1

```
# Exclude users whose names start with TEMP
EXCLUDE
    CLASS UserProfile
        USRPRF=TEMP.*
    ENDCLASS
ENDEXCLUDE
```

Example 2

```
# Exclude USERA and USERB
# Because attribute rules are ANDed, these must be in separate
# CLASS sections.
EXCLUDE
    CLASS UserProfile
        USRPRF=USERA
    ENDCLASS
    CLASS UserProfile
        USRPRF=USERB
    ENDCLASS
ENDEXCLUDE
```

Example 3

```
# Exclude all users except those whose names start with IDM
# This works because channel-specific matching takes precedence
# over general matching.
EXCLUDE
    CLASS UserProfile
    ENDCLASS
ENDEXCLUDE

SUBSCRIBER INCLUDE UserProfile USRPRF=IDM.*
PUBLISHER INCLUDE UserProfile USRPRF=IDM.*
```

5.4 Managing Additional Attributes

You can add additional attributes to the driver for both the Publisher and Subscriber channels. These attributes can be accessed by the CL programs for all event types.

To publish or subscribe to additional attributes, you must add them to the filter and add support for them into the CL programs.

5.4.1 Modifying the Filter

1. On the iManager Driver Overview page for the driver, click the *Filter* icon on either the Publisher or Subscriber channel. It is the same object.
2. In the Filter Edit dialog box, click the class containing the attribute to be added.
3. Click *Add Attribute*, then select the attribute from the list.
4. Select the flow of this attribute for the Publisher and Subscriber channels.
   - **Synchronize:** Changes to this object are reported and automatically synchronized.
   - **Ignore:** Changes to this object are not reported and not automatically synchronized.

- **Notify:** Changes to this object are reported, but not automatically synchronized.
- **Reset:** Resets the object value to the value specified by the opposite channel. (You can set this value on either the Publisher or Subscriber channel, but not both.)

5 Click *Apply*.

If you want to map this attribute to an existing attribute in the i5/OS schema, modify the Schema Mapping policy for the driver.

For complete details about managing filters and Schema Mapping policies, see the Identity Manager 4.7 Documentation Web site (https://www.netiq.com/documentation/identity-manager-47/).

5.4.2 Modifying the CL Programs for New Attributes

In the Subscriber channel, a specific CL program is called to take the appropriate action for each type of event. If the additional attribute is required for adds and modifies of users, modify `ADDUSER` and `MODUSER` to process the additional attribute.

To edit a CL program, use the following command:

`EDTF FILE(`*`LibName`*`/QCLSRC) MBR(`*`PgmName`*`)`

LibName is the name of the driver library and *PgmName* is the name of the CL program. The default driver library name is `I5OSDRV`.

CL programs must be compiled for use. To compile a CL program, use the following command:

`CRTBNDCL PGM(`*`LibName/PgmName`*`) SRCFILE(`*`LibName`*`/QCLSRC)`

LibName is the name of the driver library and *PgmName* is the name of the CL program. The default driver library name is `I5OSDRV`.

Publishing additional attributes requires that you act on changes made in the i5/OS source application.

6 Configuring the IBM i Driver

After you have installed the Identity Manager 4.7 driver for IBM I (i5/OS and OS/400), use the information in this section for configuration. Topics include

6.1 Driver Parameters and Global Configuration Values

You can control the operation of the IBM i driver by modifying the properties described in the following sections.

IMPORTANT: Changing these values requires a restart of the driver.

To change import-only properties, you must re-import the driver configuration file `i5os.xml` over the existing driver. For details, see Section 3.6, “Setting Up the Driver on the Metadirectory Server,” on page 23.

To edit the properties shown on the Driver Configuration page and the Global Configuration Values page:

1. In iManager, select *Identity Manager Overview* from the Identity Manager task list on the left side of the window.
2. Navigate to your Driver Set by searching the tree or by entering its name.
3. Click the driver to open its overview.
4. Click the driver icon.
5. Select *Driver Configuration* or *Global Config Values* as appropriate.
6. Edit the property values as desired, then click *OK*.

6.1.1 Properties That Can Be Set Only during Driver Import

Properties that you can set only during driver import are used to generate policies and other configuration details.

Table 6-1 Driver Import-Only Parameters

Property Name	Values or Format
Data Flow	Bidirectional Application to Identity Vault Identity Vault to Application
Enable Entitlements	Yes No
Use SSL	Yes No

Data Flow

- **Bidirectional:** Identities are synchronized from both the Identity Vault and the connected system (application). After all pending events are processed, the Identity Vault and connected system mirror each other.
- **Application to Identity Vault:** Identities are synchronized from the connected system (application) to the Identity Vault, but not vice versa. For example, an identity created in the Identity Vault is not created on the connected system unless explicitly migrated.
- **Identity Vault to Application:** Identities are synchronized from the Identity Vault to the connected system (application), but not vice versa. For example, changes made to an i5/OS identity are not synchronized to the Identity Vault.

Enable Entitlements

Specifies whether the driver uses either Approval Flow or Roles-Based Entitlements with the Entitlements Service driver.

Enable entitlements for the driver only if you plan to use the User Application or Roles-Based Entitlements with the driver.

You can use Roles-Based Entitlements to integrate the IBM i driver with the Identity Manager User Application. For more information see the NetIQ® Identity Manager 4.7 Web site (https://www.netiq.com/documentation/idm45/).

Use SSL

Specifies whether the driver uses Secure Sockets Layer (SSL) to encrypt the connection between the Identity Vault and the application.

We strongly recommend that you use SSL. If you do not use SSL, identity data, including passwords, is sent across the network in clear text.

6.1.2 Driver Configuration Page

Table 6-2 *Driver Configuration Page*

Property Name	Values or Format
Driver Module	Connect to Remote Loader must be selected.
Driver Object Password	Text Value
Authentication ID	Not used by the IBM i driver.
Authentication Context	Not used by the IBM i driver.
Remote Loader Connection Parameters	Host name or IP address and port number of the driver shim on the connected system, and the RDN of the object with server certificate
Driver Cache Limit	The recommended value is 0 (zero).
Application Password	Not used by the IBM i driver.
Remote Loader Password	Text Value
Startup Option	Auto start Manual
Automatic Loopback Detection	Yes No
Polling Interval	Number of seconds
Heartbeat Interval	Number of seconds
Publisher Disabled	Yes No

Driver Object Password

The Driver object password is used by the driver shim (embedded Remote Loader) to authenticate itself to the Metadirectory engine. This must be the same password that is specified as the Driver object password on the connected system driver shim.

Remote Loader Connection Parameters

The Remote Loader Connection Parameters option specifies information that the driver uses for Secure Sockets Layer (SSL) communication with the connected system.

Table 6-3 Remote Loader Connection Parameters

Parameter	Description
`host=hostName`	Connected system host name or IP address.
`port=portNumber`	Connected system TCP port number. The default is 8090.
`kmo=objectRDN`	The RDN of the object with the server certificate signed by the tree's certificate authority. Enclose the RDN in double quotes (") if the name contains spaces.

The following is an example Remote Loader connection parameter string:

```
hostname=192.168.17.41 port=8090 kmo="SSL CertificateIP"
```

Remote Loader Password

The Remote Loader password is used to control access to the driver shim (embedded Remote Loader). This must be the same password that is specified as the Remote Loader password on the connected system driver shim.

Automatic Loopback Detection

Specifies whether the driver shim discards events that would cause loopback conditions. This function supplements the loopback detection provided by the Metadirectory engine.

Polling Interval

Specifies the number of seconds that the Publisher shim waits after running the polling CL program and sending events from the change log to the Metadirectory engine. The default interval is 60 seconds.

Publisher Disabled

Specifies whether the Publisher shim is active.

Select *Yes* if you are using Identity Vault to Application (one-way) data flow. This saves processing time.

Heartbeat Interval

Specifies how often, in seconds, the driver shim contacts the Metadirectory engine to verify connectivity. Specify 0 to disable the heartbeat.

6.1.3 Global Configuration Values Page

Table 6-4 *Global Configuration Values*

Property Name	Values or Format
Connected System or Driver Name	Text Value
Synchronize Group Membership	Yes No
The IBM i Connected System Accepts Passwords from the Identity Vault	Yes No
The Identity Vault Accepts Passwords from the IBM i Connected System	Yes No
Publish Passwords to NDS Password	Yes No
Publish Passwords to Distribution Password	Yes No
Require Password Policy Validation before Publishing Passwords	Yes No
Reset User's External System Password to the Identity Manager Password on Failure	Yes No
Notify the User of Password Synchronization Failure via E-Mail	Yes No
User Base Container	Identity Vault Container object
Group Base Container	Identity Vault Container object

To view and edit Password Management GCVs, select *Show* for *Show Password Management Policy*.

To view and edit User and Group Placement GCVs, select *Show* for *Show User and Group Placements*.

Connected System or Driver Name

Specifies the name of the driver. This value is used by the e-mail notification templates.

Synchronize Group Membership

Specifies whether the driver synchronizes group membership between the connected system and the Identity Vault.

The IBM i Connected System Accepts Passwords from the Identity Vault

Specifies whether the driver allows passwords to flow from the Identity Vault to the connected IBM i system.

The Identity Vault Accepts Passwords from the IBM i Connected System

Specifies whether the driver allows passwords to flow from the connected IBM i system to the Identity Vault.

Publish Passwords to NDS Password

Specifies whether the driver uses passwords from the connected IBM i system to set non-reversible NDS® passwords in the Identity Vault.

Publish Passwords to Distribution Password

Specifies whether the driver uses passwords from the connected IBM i system to set NMAS™ Distribution Passwords, which are used for Identity Manager password synchronization.

Require Password Policy Validation before Publishing Passwords

Specifies whether the driver applies NMAS password policies to published passwords. If so, a password is not written to the Identity Vault if it does not conform.

Reset User's External System Password to the Identity Manager Password on Failure

Specifies whether, on a publish Distribution Password failure, the driver attempts to reset the password on the connected IBM i system using the Distribution Password from the Identity Vault.

Notify the User of Password Synchronization Failure via E-Mail

Specifies whether the driver sends an e-mail to a user if the password cannot be synchronized.

User Base Container

Specifies the base container object in the Identity Vault for user synchronization. This container is used in the Subscriber channel Event Transformation policy to limit the Identity Vault objects being synchronized. This container is used in the Publisher channel Placement policy as the destination for adding objects to the Identity Vault. Use a value similar to the following:

```
users.myorg
```

Group Base Container

Specifies the base container object in the Identity Vault for group synchronization. This container is used in the Subscriber channel Event Transformation policy to limit the Identity Vault objects being synchronized. This container is used in the Publisher channel Placement policy as the destination when adding objects to the Identity Vault. Use a value similar to the following:

```
groups.myorg
```

6.2 The Driver Shim Configuration File

The driver shim configuration file controls operation of the driver shim.

The default driver shim configuration file is in the IFS `/etc` directory. So that the exit programs can find the file, its name is the lowercased name of the driver library. For example, if you installed the driver shim into the `I5OSDRV` library, the configuration file is `/etc/i5osdrv.conf`.

You can specify the configuration options listed in Table 6-5, one per line.

Table 6-5 *Driver Shim Configuration File Statements*

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>`

`-i5oslibrary <libraryName>`	Specifies the library name where the driver shim is installed. The default is `I5OSDRV`.
`-path <driverPath>`	Specifies the IFS path for driver files. The default path is `/usr/local/i5osdrv`.
`-t <traceLevel>` `-trace <traceLevel>`	Sets the level of debug tracing. 0 is no tracing, and 10 is all tracing. For details, see Section A.1.2, “The Trace File,” on page 59. The output file location is specified by the `tracefile` option.
`-tf <fileName>` `-tracefile <fileName>`	Sets the trace file location. The default is `logs/trace.log` in the driver IFS path.

Example Driver Shim Configuration File

```
-tracefile /usr/local/i5osdrv/logs/trace.log
-trace 0
-connection "ca=/usr/local/i5osdrv/keys/ca.pem port=8090"
-path /usr/local/i5osdrv/
```

6.3 Migrating Identities

When you first run the IBM i driver, you might have identities in the Identity Vault that you want to provision to the connected system, or vice versa. Identity Manager provides a built-in migration feature to help you accomplish this.

6.3.1 Migrating Identities from the Identity Vault to the Connected System

1. In iManager, open the Identity Manager Driver Overview for the driver.
2. Click *Migrate from Identity Vault*. An empty list of objects to migrate is displayed.
3. Click *Add*. A browse and search dialog box that allows you to select objects is displayed.
4. Select the objects you want to migrate, then click *OK*.

To view the results of the migration, click *View the Driver Status Log*. For details about the log, see Section A.1.5, “The Status Log,” on page 60.

If a user has a Distribution Password, the Distribution Password is migrated to the connected system as the user’s password. Otherwise, no password is migrated. For information about Universal Passwords and Distribution Passwords, see the appropriate version of the *Password Management Administration Guide* at the NetIQ Documentation Web site (https://www.netiq.com/documentation).

6.3.2 Migrating Identities from the Connected System to the Identity Vault

1. In iManager, open the Identity Manager Driver Overview for the driver.
2. Click *Migrate into Identity Vault* to display the Migrate Data into the Identity Vault window.
3. Specify your search criteria:
   - **3a** To view the list of eDirectory™ classes and attributes, click *Edit List*.
   - **3b** Select class User or class Group.

     IMPORTANT: Identity Manager imports objects by class in the order specified in the list. Migrate users before you migrate groups so that the users can be added to the newly created groups.

   - **3c** Select the attributes to be used as search criteria for objects of the selected class, then click *OK*.

     The eDirectory attributes map to i5/OS attributes as specified by the driver schema: CN maps to USRPRF, etc. For the default mappings, see Table 1-2, “Default eDirectory User to i5/OS UserProfile Mapping,” on page 15 and Table 1-3, “Default eDirectory Group to IBM i GroupProfile Mapping,” on page 16.

     To see i5/OS attributes, click *Show all attributes from all classes* above the attribute list.

   - **3d** Specify values for the selected attributes, then click *OK*.

     The values can include basic regular expressions.
4. Click *OK*.

To view the results of the migration, click *View the Driver Status Log*. For details about the log, see Section A.1.5, “The Status Log,” on page 60.

Because local passwords cannot be retrieved from the IBM i security system, they cannot be submitted to the Metadirectory engine until they are changed. The Validate Password exit program captures password changes.

6.3.3 Synchronizing the Driver

To generate events for associated objects that have changed since the driver's last processing, open the Identity Manager Driver Overview page for the driver in iManager, then click *Synchronize*.

7 Using the IBM i Driver

This section provides information about operational tasks commonly used with the Identity Manager 4.7 driver for IBM i (i5/OS and OS/400).

Topics include

7.1 Starting and Stopping the Driver

To start the driver:

1. In iManager, navigate to the Driver Overview for the driver.
2. Click the upper right corner of the driver icon.
3. Click *Start driver*.

To stop the driver:

1. In iManager, navigate to the Driver Overview for the driver.
2. Click the upper right corner of the driver icon.
3. Click *Stop driver*.

7.2 Starting and Stopping the Driver Shim

To start the driver shim, enter `GO I5OSDRV/I5OSDRV` on the command line, then select option 1.

To stop the driver shim, enter `GO I5OSDRV/I5OSDRV` on the command line, then select option 2.

If you did not use the default library name, substitute your driver library name as shown in the following example:

`GO yourDriverLibrary/I5OSDRV`

7.3 Displaying the Driver Shim Version

To see version information for the driver shim, enter the following command on the command line:

```
I5OSDRV/I5OSDRV OPTION(*VERSION)
```

If you did not use the default library name, substitute your driver library name as shown in the following example:

```
yourDriverLibrary/I5OSDRV OPTION(*VERSION)
```

7.4 Monitoring Driver Messages

The IBM i driver writes messages to the driver shim job log. Monitor driver activity there in the same way you monitor other key system functions. Use the `DSPJOBLOG` command or IBM i Navigator to view the job log. For details about the messages written by the driver, see Appendix B, “System and Error Messages,” on page 65.

7.5 Changing Passwords

To publish password change information, you must change passwords with a method that uses the Validate Password exit program. The driver obtains password change information from this exit. Administrative password resets must be performed in the Identity Vault.

8 Securing the IBM i Driver

This section describes best practices for securing the Identity Manager 4.7 driver for IBM i (i5/OS and OS/400). Topics include

For additional information about Identity Manager security, see the *NetIQ® Identity Manager 4.7 Administration Guide* on the Identity Manager 4.7 Documentation Web site (https://www.netiq.com/documentation/identity-manager-47/).

8.1 Using SSL

Enable SSL for communication between the Metadirectory engine and the driver shim on the connected system. For more information, see “Use SSL” on page 44.

If you don’t enable SSL, you are sending information, including passwords, in the clear.

8.2 Physical Security

Keep your servers in a physically secure location with access by authorized personnel only.

8.3 Network Security

Require users outside of the corporate firewall to use a VPN to access corporate data.

8.4 Auditing

Track changes to sensitive information. Examine audit logs periodically.

For details about using NetIQ Audit to monitor driver operation, see the NetIQ Audit Documentation Web site (http://www.novell.com/documentation/novellaudit20/index.html).

8.5 Driver Security Certificates

SSL uses security certificates to control, encrypt, and authenticate communications.

Ensure that the `keys` security certificate directory in the driver IFS path is appropriately protected. The installation program sets secure file permissions for this directory.

The Driver Shim and the Identity Manager engine communicate through SSL using a certificate created in the Identity Vault and retrieved by the driver shim during the installation process. For more information on this certificate and how to renew or install third-party certificates, refer to the *Identity Manager Administration Guide*.

The Embedded Remote Loader web interface uses a dynamically generated, self-signed certificate for SSL communication. The details of this certificate are as follows:

Table 8-1 *Driver Security Certificate Details*

Property Name	Values / Parameters
Subject	SSL Server
Issuer	SSL Server
Validity	1 year
Serial Number	0
Key	1024-bit RSA

Renewal of this certificate automatically occurs when the Driver Shim is restarted on the connected platform.

8.6 Driver Shim Programs and CL Programs

The driver uses CL programs to perform updates on the connected system, and to collect changes made there. The CL programs reside in the i5/OS driver library.

Ensure that the i5/OS driver library is appropriately protected. The installation program sets the appropriate library security.

8.7 The Change Log

The change log file contains information about events on the connected system, including passwords. It is encrypted, but it should be protected against access by unauthorized users.

Ensure that the `changelog` directory in the driver IFS path is appropriately protected. The installation program sets secure file permissions for this directory.

8.8 Driver Passwords

Use strong passwords for the Driver object and Remote Loader passwords, and restrict knowledge of them to authorized personnel. These passwords are stored in encrypted form in the `keys` security certificate directory in the driver IFS path. The installation program sets secure file permissions for this directory.

8.9 Administrative Users

Ensure that accounts with elevated rights on the Metadirectory system, Identity Vault systems, and the connected systems are appropriately secure. Protect administrative user IDs with strong passwords.

8.10 Connected Systems

Ensure that connected systems can be trusted with account information, including passwords, for the portion of the tree that is configured as their base containers.

A Troubleshooting

This section provides information about troubleshooting the Identity Manager 4.7 driver for IBM i (i5/OS and OS/400). Major topics include

A.1 Driver Status and Diagnostic Files

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

A.1.1 The Job Log

The job log is used by the driver shim to provide urgent, informational, and debug messages. These messages come from the driver shim and from CL programs called by the driver shim to process events. Examining these should be foremost in your troubleshooting efforts.

Use the `DSPJOBLOG` command or IBM i Navigator to view the job log.

For detailed message documentation, see Appendix B, “System and Error Messages,” on page 65.

A.1.2 The Trace File

The default trace file exists on the connected i5/OS system in the driver IFS path at `logs/trace.log`. A large amount of debug information can be written to this file. Use the trace level setting in the driver shim configuration file to control what is written to the file. For details, see Section 6.2, “The Driver Shim Configuration File,” on page 49.

Table A-1 *Driver Shim Trace Levels*

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

Trace Level	Description
8	Previous level plus driver status log, driver parameters, driver command line, driver security, driver Web server, driver schema, driver encryption, 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 file line to set the trace level:

```
-trace 9
```

A.1.3 CL Program Output

Output from the CL programs is written to the job log. Use the `DSPJOBLOG` command or i5/OS Navigator to view the job log.

If the trace level is set to at least 4, CL program output is also written to the trace file. For details about the trace file and trace levels, see Section A.1.2, “The Trace File,” on page 59.

A.1.4 DSTRACE

You can view Identity Manager information using the DSTRACE facility on the Metadirectory server. Use iManager 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 *NetIQ® Identity Manager Administration Guide* on the Identity Manager 4.7 Documentation Web site (https://www.netiq.com/documentation/identity-manager-47/).

A.1.5 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 in the driver IFS path at `logs/dirxml.log`. You can also view the status log in iManager on the Driver Overview page. You can change the log level to specify what types of events to log. For details about using the status log, see the *NetIQ Identity Manager Administration Guide* on the Identity Manager 4.7 Documentation Web site (https://www.netiq.com/documentation/identity-manager-47/).

A.2 Troubleshooting Common Problems

- Section A.2.8, “Connected System User Passwords Are Not Provisioned to the Identity Vault,” on page 63
- Section A.2.9, “Users or Groups Are Not Modified, Deleted, Renamed, or Moved,” on page 63

A.2.1 Driver Rules Installation Failure

Ensure that you use a version of iManager that is compatible with your version of Identity Manager.

A.2.2 Driver Certificate Setup Failure

To set up certificates, the driver shim communicates with the Metadirectory server using the LDAP secure port (636).

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

To configure the certificate, use the I5OSDRV menu. For more information about the menu, see Section C.1, “Using the I5OSDRV Menu,” on page 79.

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

1. In iManager, browse the Security container to locate your tree’s Certificate Authority (typically named *`treeName`* `CA`).
2. Click the Certificate Authority object.
3. Click *Modify Object*.
4. Select the *Certificates* tab.
5. Click *Public Key Certificate*.
6. Click *Export*.
7. Select *No* to export the certificate without the private key, then click *Next*.
8. Select *Base64 format*, then click *Next*.
9. Click *Save the exported certificate to a file*, then specify a location to save the file.
10. Use FTP or another method to store the file on the connected system in the driver IFS path as `keys/ca.pem`.

    If you installed the driver using the default driver IFS path, store the file as `/usr/local/i5osdrv/keys/ca.pem`.

A.2.3 Driver Start Failure

- Examine the status log and DSTRACE output.
- The driver must be specified as a Remote Loader driver. You can set this option in the iManager Driver Edit Properties window.
- You must activate both Identity Manager and the driver within 90 days. The Driver Set Overview page in iManager shows when Identity Manager requires activation. The Driver Overview page shows when the driver requires activation.

  For details about activating NetIQ Identity Manager Products, see the *Identity Manager Installation Guide* on the Identity Manager 4.7 Documentation Web site (https://www.netiq.com/documentation/identity-manager-47/).

For more information about troubleshooting Identity Manager engine errors, see the Identity Manager 4.7 Documentation Web site (https://www.netiq.com/documentation/identity-manager-47/).

A.2.4 Driver Shim Startup or Communication Failure

- Examine the trace file.
- 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.

  The passwords are stored in the driver IFS path in the `keys` directory in encrypted files `dpwdlf40` (Driver object password) and `lpwdlf40` (Remote Loader password).

  To update these passwords on the connected system, use the I5OSDRV menu. For more information about the menu, see Section C.1, “Using the I5OSDRV Menu,” on page 79.

  To update these passwords on the Metadirectory server, use iManager to update the driver configuration. For details, see Section 6.1.2, “Driver Configuration Page,” on page 45.
- Ensure that the correct host name and port number of the connected system are specified in the Driver Configuration Remote Loader connection parameters. You can change the port number (default 8090) in the driver shim configuration file.

A.2.5 Users or Groups Are Not Provisioned to the Connected System

- Examine the status log, DSTRACE output, trace file, and job log.
- To be provisioned, users and groups must be in the appropriate base container. You can view and change the base containers in iManager on the Global Configuration Values page of the Driver Edit Properties window. For more details, see Section 6.1.3, “Global Configuration Values Page,” on page 47.
- To provision identities from the Identity Vault to the connected system, the driver Data Flow property must be set to Bidirectional or 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 2-2, “Base Container Rights Required by the Driver Security-Equivalent User,” on page 19.

A.2.6 Users or Groups Are Not Provisioned to the Identity Vault

- Examine the status log, DSTRACE output, and trace file.
- Examine the User Base Container and Group Base Container GCV values. For more details, see Section 6.1.3, “Global Configuration Values Page,” on page 47.
- To provision identities from the connected system to the Identity Vault, the driver Data Flow property must be set to Bidirectional or Application to Identity Vault. 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 update the base container. For details about the rights required, see Table 2-2, “Base Container Rights Required by the Driver Security-Equivalent User,” on page 19.

A.2.7 Identity Vault User Passwords Are Not Provisioned to the Connected System

- Examine the status log, DSTRACE output, and job log.
- There are several password management properties available in iManager on the Global Configuration Values page of the Driver Edit Properties window. 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 *NetIQ Identity Manager 3.6.1 Administration Guide* on the Identity Manager 4.7 Documentation Web site (https://www.netiq.com/documentation/identity-manager-47/).
- Ensure that the user's container has an assigned Universal Password policy and that the *Synchronize Distribution Password When Setting Universal Password* option is set for this policy.

A.2.8 Connected System User Passwords Are Not Provisioned to the Identity Vault

- Examine the status log, DSTRACE output, and the trace file.
- Ensure that the *The Identity Vault Accepts Passwords from the i5/OS Connected System* GCV is set.
- To publish password change information, you must change passwords with a method that uses the Validate Password exit program. The driver obtains password change information from this exit. Administrative password resets must be performed in the Identity Vault.
- If the *Require Password Policy Validation before Publishing Password GCV* is set, the user's password must satisfy the password rules in the password policy assigned to the user container.

A.2.9 Users or Groups Are Not Modified, Deleted, Renamed, or Moved

- Examine the status log, DSTRACE output, trace file, and job log.
- Examine the driver Data Flow setting to verify the authoritative source for identities.
- Identity Vault and connected system identities must be associated before events are synchronized. To view an identity's associations, use Modify User/Group in iManager and click the *Identity Manager* tab. You can migrate identities to establish associations. For details, see Section 6.3, "Migrating Identities," on page 49.
- Renaming profiles is not supported by i5/OS. The driver can optionally process rename commands by deleting and recreating a profile with identical attributes and the new name. Before using this functionality, please review the CL *PGM source found in rename.cl, renuser.cl, rengroup.cl and make sure it meets the requirements of your environment. For details, see Section 5.1, "The Scriptable Framework," on page 31. To enable rename processing, disable the Veto Rename Events policy in the Event Transformation.
- 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.

B System and Error Messages

Components of the Identity Manager 4.7 driver for IBM i (i5/OS and OS/400) write messages to the driver shim job log to report operational status and problems. You can use the `DSPJOBLOG` command or IBM i Navigator to view the job log. For more information about the job log, see Section A.1.1, “The Job Log,” on page 59. For detailed troubleshooting information, see Appendix A, “Troubleshooting,” on page 59.

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:

B.1 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: <*configline*>.

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

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.

Action: Add the required statement to the configuration file.

B.2 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.

B.3 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.

B.4 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.

B.5 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.

B.6 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.

LWS0009I Local host is *host_name* (*IP_address*).

Explanation: This message shows the host name and IP address of the machine that the server is running on.

Action: None. Informational only.

LWS0010I Local host is *IP_address*.

Explanation: This message shows the IP address of the machine that the server is running on.

Action: None. Informational only.

LWS0011I Server is now processing client requests.

Explanation: The server has successfully started all configured services, and it is ready for clients to begin requests.

Action: None. Informational only.

LWS0012I *service* is now active on port *number*.

Explanation: The server *service* is running on the specified TCP port *number*. Clients can begin making requests to the specified service.

Action: None. Informational only.

LWS0013I *service* is now inactive on port *number*.

Explanation: The server *service* is not active on the specified TCP port *number*. Processing continues, but no client requests can be made to the service until it becomes active again.

Action: None. Informational only.

LWS0014E An error was encountered while parsing execution parameters.

Explanation: An error occurred while parsing the execution parameters. The server terminates with a minimum return code of 8.

Action: Collect diagnostic information and contact NetIQ® Technical Support.

LWS0015E *service* failed to start with error *number*.

Explanation: The specified service failed to start. The server terminates with a minimum return code of 8.

Action: Collect diagnostic information and contact NetIQ Technical Support.

LWS0020I Server *version* level: *level*.

Explanation: This message contains information detailing the current service level for the server program being executed. The value of *version* indicates the current release of the server. The value of *level* is a unique sequence of characters that can be used by NetIQ Technical Support to determine the maintenance level of the server being executed.

Action: Normally, no action is required. However, if you report a problem with the server to NetIQ Technical Support, you might be asked to provide the information in the message.

LWS0023I Listen port *number* is already in use.

Explanation: The displayed listen port is already in use by another task running on the local host. The server retries establishing the listen port.

Action: Determine what task is using the required port number and restart the server when the task is finished, or specify a different port in the configuration file. If the port number is changed for the server, the client must also specify the new port number.

LWS0024W Too many retries to obtain port *number*.

Explanation: The server tried multiple attempts to establish a listen socket on the specified port number, but the port was in use. The server terminates with a return code of 4.

Action: Determine what task is using the required port number, and restart the server when the task is finished, or specify a different port in the configuration file. If the port number is changed for the server, the client must also specify the new port number.

LWS0025I Local TCP/IP stack is down.

Explanation: The server detected that the local host TCP/IP service is not active or is unavailable. The server retries every two minutes to reestablish communication with the TCP/IP service.

Action: Ensure that the TCP/IP service is running.

LWS0026E Unrecoverable TCP/IP error *number* returned from *internal_function_name*.

Explanation: An unrecoverable TCP/IP error was detected in the specified internal server function name. The server ends with a minimum return code of 8. The error number reported corresponds to a TCP/IP errno value.

Action: Correct the error based on TCP/IP documentation for the specified errno.

LWS0027W Listen socket was dropped for port *number*.

Explanation: The server connection to the displayed listen port was dropped. The server attempts to reconnect to the listen port so that it can receive new client connections.

Action: Determine why connections are being lost on the local host. Ensure that the host TCP/IP services are running.

LWS0028E Unable to reestablish listen socket on port *number*.

Explanation: The listen socket on the specified port number was dropped. The server tried multiple attempts to reestablish the listen socket, but all attempts failed. The server ends with a return code of 8.

Action: Determine if the host's TCP/IP service is running. If the host's TCP/IP service is running, determine if another task on the local host is using the specified port.

LWS0029I <*id*> Client request started from *ip_address* on port *number*.

Explanation: A new client request identified by *id* has been started from the specified IP address on the displayed port number.

Action: None. Informational only.

LWS0030I <*id*> Client request started from *host* (*ip_address*) on port *number*.

Explanation: A new client request identified by *id* has been started from the specified host and IP address on the displayed port number.

Action: None. Informational only.

LWS0031W Unable to stop task *id*: *reason*.

Explanation: The server attempted to terminate a service task identified by *id*. The server could not stop the task for the specified reason. The server ends with a return code of 4.

Action: See the reason text for more information about why the task could not terminate.

LWS0032I <*id*> Client request has ended.

Explanation: The client requested identified by *id* has ended.

Action: None. Informational only.

LWS0033I <*id*> Client request: *resource*.

Explanation: The client connection identified by *id* issued a request for *resource*.

Action: None. Informational only.

LWS0034W <*id*> Write operation for client data has failed.

Explanation: A write operation failed for the connection identified by *id*. This is normally because the client dropped the connection. The client connection is dropped by the server.

Action: Ensure that the client does not prematurely drop the connection. Retry the client request if necessary.

LWS0035W <*id*> Read operation for client data has timed out.

Explanation: A read operation on the connection identified by *id* has timed out because of inactivity. The client connection is dropped by the server.

Action: Ensure that the client does not prematurely drop the connection. Retry the client request if necessary.

LWS0036W <*id*> Client request error: *error_code* - *error_text*.

Explanation: The server encountered an error while processing the client request. The server terminates the request.

Action: Determine why the request was in error by viewing the error code and error text that was generated.

LWS0037W <*id*> Client request error: *code*.

Explanation: The server encountered an error while processing the client request. The server terminates the request.

Action: Determine why the request was in error by viewing the error code and error text that was generated.

LWS0038I Received command: *command_text*.

Explanation: The server has received the displayed command from the operator. The server processes the command.

Action: None. Informational only.

LWS0043E Task *id* ended abnormally with RC=*retcode*.

Explanation: The server detected a task that ended with a non-zero return code. The server ends with a minimum return code of 8.

Action: View the log for other messages that might have been generated regarding the error.

LWS0045I Idle session time-out is *number* seconds.

Explanation: The message shows the idle time limit for connections. The server automatically terminates sessions that are idle for longer than the specified number of seconds.

Action: None. Informational only.

LWS0046I Maximum concurrent sessions limited to *number*.

Explanation: The message shows the maximum number of concurrent sessions allowed. The server allows only the specified number of concurrent sessions to be active at any given time. All connections that exceed this limit are forced to wait until the total number of connections drops below the specified value.

Action: None. Informational only.

LWS0047W Unable to delete log file *filename*.

Explanation: The log file could not be deleted as specified.

Possible cause: The user service or daemon does not have file system rights to delete old log files.

Action: Verify that the user service or daemon has the appropriate rights.

Action: Examine the current logs for related messages.

LWS0048I Log file *filename* successfully deleted.

Explanation: The log file has been deleted as specified.

Action: None. Informational only.

LWS0049E Error *error* authenticating to the directory as *fdn*.

Explanation: The connection manager could not connect to the directory as user *fdn*. The error was *error*.

Possible cause: The configuration parameters do not contain the correct user or password.

Action: Correct the cause of the error as determined from *error*.

Action: Verify that the User object has the appropriate rights.

Action: Verify that the password given for the User object in the configuration parameters is correct.

LWS0050E Server application initialization failure was detected.

Explanation: During server initialization, an error was detected while initializing the server Application object.

Possible Cause This message is commonly logged when the driver is started and then immediately shut down. This can happen during installation, when the shim is started to generate keys or configure SSL. You can safely ignore this message in those cases.

Action: See the error logs for additional messages that indicate the cause of the error.

LWS0051E Server initialization failure was detected.

Explanation: The server failed to initialize properly because of an initialization error specific to the operating system.

Action: See the log for additional messages that indicate the cause of the error.

LWS0052W This server is terminating because of another instance already running (*details*).

Explanation: The server is shutting down because there is another active instance of this server running on the host.

Possible cause: A previous instance of the server was not stopped before starting a new instance.

Action: Stop or cancel the previous server instance before starting a new one.

LWS0053I The parameter *keyword* is no longer supported.

Explanation: The specified parameter is no longer supported in this release and might be removed in future releases.

Possible cause: An execution parameter was specified that is no longer supported.

Action: Do not specify the unsupported parameter.

LWS0054I The execution parameter *keyword* is in effect.

Explanation: The specified execution parameter is in effect for the server.

Action: Informational only. Processing continues.

LWS0055W Invalid execution parameter detected: *keyword*.

Explanation: An invalid execution parameter was detected.

Action: Do not specify the invalid or unknown execution parameter.

LWS0056I Not accepting new connections because of the MAXCONN limit. There are *number* active connections now for *service*.

Explanation: The specified service has a maximum connection limit that has been reached. The service no longer accepts new connections until at least one of the active connections ends.

Action: If you receive this message frequently, increase the MAXCONN limit for this service or set the MAXCONN to unlimited connections.

LWS0057I New connections are now being accepted for *service*.

Explanation: The service was previously not accepting new connections because of the imposed MAXCONN limit. The service can now accept a new connection because at least one active connection has ended.

Action: None. Informational only.

LWS0058I Listen socket on port *number* has been re-established.

Explanation: The previously dropped listen socket has been re-established. Services using the specified port can now continue. The listen socket previously dropped because of an error or TCP/IP connectivity problems has been re-established. Client connection processing continues.

Action: None. Informational only.

LWS0059W Server is terminating because the required service *serviceName* is ending.

Explanation: The specified required service has ended. The server terminates because it cannot continue running without the required service.

Action: See related log messages to determine why the required service ended. Correct the problem and restart the server.

B.7 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.

B.8 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 contact NetIQ Technical 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.

Action: Correct the configuration.

OAP004E HTTP Error: *cause*.

Explanation: The user name or password provided failed basic authentication.

Possible cause: The user name or password is incorrect.

Action: Verify that user name 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.

B.9 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 is 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 is 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 is 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 iManager 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 is 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 is required.

C Technical Details

Topics in this section include

C.1 Using the I5OSDRV Menu

You can use the I5OSDRV menu to control and configure the driver shim.

To load the I5OSDRV menu, enter `GO LibName/I5OSDRV` on the command line. Substitute the name of the driver library that you specified during installation for *LibName*. If you installed the driver using the default library, use the following command:

```
GO I5OSDRV/I5OSDRV
```

The I5OSDRV menu contains several functions.

```
1. Start the I5OSDRV Driver Shim
2. Stop the I5OSDRV Driver Shim
3. Modify the I5OSDRV configuration file
4. Secure the I5OSDRV using SSL and trusted certificates
5. Set the remote loader and driver object passwords
6. Uninstall the I5OSDRV Driver Shim
```

Enter the number of the function you want to perform, then respond to the prompts.

C.2 Driver Shim Command Line Options

The following options can be specified on the driver shim command line.

Table C-1 *Driver Shim Command Line Options*

Option	Description
CONFIG	Instructs the driver shim to read options from the specified configuration file. Options are read from `/etc/i5osdrv.conf` by default.

CONNECTION	Specifies connection options.
	`port=<driverShimPort>`
	`ca=<Certificate Authority Key File>`

Option	Description
TRACE	Sets the level of debug tracing. 0 is no tracing, and 10 is all tracing. For details, see Section A.1.2, “The Trace File,” on page 59. The output file location is specified by the TRACEFILE option.
TRACEFILE	Sets the trace file location. The default is logs/trace.log in the driver IFS path.
OPTION(*SECURE)	Secures the driver by creating SSL certificates, then exits.
OPTION(*SETPASS)	Sets the Remote Loader and Driver object passwords.
OPTION(*VERSION)	Displays driver shim version information.

The following is an example driver shim command line:

```
I5OSDRV/I5OSDRV CONFIG('/etc/i5osdrv.conf')
   CONNECTION('port=8090 ca=/usr/local/i5osdrv/keys/ca.pem')
   TRACEFILE('/tmp/trace.out')
   HTTPPORT(8888)
   TRACE(10)
```

C.3 Driver Limitations

- Section C.3.1, “Password Levels,” on page 80
- Section C.3.2, “Character Fields,” on page 80
- Section C.3.3, “Distribution Directory Entry Limits,” on page 81

C.3.1 Password Levels

Password levels (i5/OS QPWDLVL system value) 0 and 1 support a maximum password length of ten characters. The allowable characters for passwords are the uppercase letters (A–Z), the digits (0–9), the dollar sign ($), the at sign (@), the octothorpe (#), and the underscore (_).

If you use password level 0 or 1, the Subscriber channel CL programs convert passwords to uppercase and truncate passwords to ten characters. The Publisher shim converts passwords to lowercase.

With password levels 2 and above, passwords can be mixed case and can be up to 128 characters long.

We recommend that you use password level 2 or above for best integration with Identity Manager.

C.3.2 Character Fields

Data is converted to the default coded character set identifier (CCSID) for the driver shim job. This is usually the QCCSID system value. You can use the CHGUSRPRF command to specify a CCSID for the user profile that runs the job. By default, the installation program creates a user profile named I5OSDRV for the driver shim job.

C.3.3 Distribution Directory Entry Limits

Distribution directory entries are linked to user profiles by a two-element USRID value, which comprises a user ID and a user address. These elements can have a maximum of 8 characters. User profile names can have a maximum of 10 characters. The Subscriber shim CL programs obtain the user ID by truncating user profile names to 8 characters and set the user address to the system name. To avoid collisions in the distribution directory, IBM recommends that you limit user profile names to 8 characters.

C.4 Driver Shim Library and IFS Contents

C.4.1 Driver Library

The default name for the driver library is `I5OSDRV`. The driver library contains the following objects:

- Driver shim program and commands
- CL program source and bound programs
- User space
- Menu
- Job description

C.4.2 Driver IFS Path

The default driver IFS path is `/usr/local/i5osdrv`. The driver IFS path contains the following directories:

Table C-2 *IFS Path Directories*

Directory	Description
`changelog`	Holds event information until it is sent to the Metadirectory engine
`conf`	Contains the include/exclude file
`keys`	Contains the Driver object password, the Remote Loader password, and SSL certificate information
`logs`	Contains trace and log files
`loopback`	Contains information used by the scriptable framework for loopback detection
`schema`	Contains connected system schema information
`snapshot`	Holds information about the state of users and groups used to complete change event descriptions

C.4.3 Driver Shim Configuration File

The default driver shim configuration file is in the IFS `/etc` directory. So that the exit programs can find the file, its name is the lowercased name of the driver library. For example, if you installed the driver shim into the `I5OSDRV` library, the configuration file is `/etc/i5osdrv.conf`.

D Documentation Updates

This section describes updates to this document since its original release date of October 28, 2014.

D.1 July 28, 2017

Location	Update
Section 2.1	Removed “Driver shim HTTP services for log viewing” row from table.
Section 6.1	Removed “Ignore Renames” from table and removed section it links to.
Section 6.1	Removed “Remove Owned Objects” from table and removed section it links to.
Section A.1.2	Removed “To view trace file:” and steps.
Section A.1.5	Removed “To view the status log:” and steps.
Section A.2.9	Removed reference to deleted “Removed Owned Objects” section.
Section C.2	Removed “HTTPPORT” row from table.