Information Builders

iWay

iWay Application Protocol Adapter for LDAP User's Guide

Version 7.0.x and Higher

August 16, 2018

Contents

Preface 7

Documentation Conventions 8

Related Publications 9

Customer Support 9

Help Us to Serve You Better 9

User Feedback 12

Information Builders Consulting and Training 12

1. Introducing the iWay Application Protocol Adapter for LDAP 13

Features of the iWay Application Protocol Adapter for LDAP 13

Component Information for the iWay Application Protocol Adapter for LDAP 14

Component Information Roadmap. 14

iWay Service Manager. 15

iWay Explorer. 15

iWay Business Services Provider. 15

2. Supported Platforms Matrix 17

iWay Application Protocol Adapter for LDAP Overview 17

LDAP Versions 17

Operating Systems 18

Databases 18

Java Development Kit (JDK) 18

Communication Modes 18

Object Types and Interfaces 19

Communication Types 19

Operations 19

Data Types 20

Other Functions 20

Known Limitations 20

Related Information for Specific iWay Releases 21

3. Installing the iWay Application Protocol Adapter for LDAP 23

Installation Prerequisites 23

Installing the iWay Application Protocol Adapter for LDAP 24

Required Installation Files. 24

4. Configuring and Managing Connections to an LDAP Server 27

Starting iWay Explorer 27

Adding the LDAP Adapter to iWay Explorer 31

Working With a Target 33

Understanding the LDAP Tree Display. 42

5. Initializing a Secure Connection to an LDAP Server 47

Prerequisites Before SSL Connection to LDAP 47

Installing a Secure Certificate for an LDAP Server 48

6. Creating XML Schemas for LDAP 51

LDAP Processing Overview 51

Browsing LDAP Entries 51

Schema Node Browsing. 56

Generating XML Schemas for LDAP Operations 56

Service Adapter Run-Time Operations. 57

Get. 57

Update. 59

Delete. 60

Create. 61

Move. 61

Working With LDAP Action Dialogs. 62

Creating New LDAP Entries. 62

Updating LDAP Entries. 64

Deleting LDAP Entries. 65

Moving LDAP Entries. 66

Schema Location. 66

7. Creating and Publishing iWay Business Services 69

Understanding iWay Business Services 69

Naming Considerations. 69

Creating iWay Business Services 69

8. Configuring Events for LDAP 75

LDAP Event Handling Overview 75

Creating an Event Port 75
Using the Default Port. 86
Creating a Channel 87
Configuring the Ldap Connection Configuration Tab. 93
Configuring the Event Strategy Configuration Tab. 96
Configuring the Asynchronous Event Subscription Configuration Tab. 98

A. Configuring the Adapter in an iWay Environment 101

Configuring the Adapter in iWay Service Manager 101

B. Understanding Active Directory Error Messages 105

Error Messages 105

Preface

This document describes how to use the iWay Application Protocol Adapter for LDAP to provide connectivity to LDAP compliant servers and create, update, search, and delete selected LDAP entries. It is assumed that readers understand web technologies and have a general understanding of Microsoft Windows and UNIX systems.

Note: This Release 7.0.x content is currently being updated to support iWay Release 8.0.x software. In the meantime, it can serve as a reference for your use of iWay Release 8. If you have any questions, please contact *Customer_Success@ibi.com*.

How This Manual Is Organized

This manual includes the following chapters:

	Chapter/Appendix	Contents
1	Introducing the iWay Application Protocol Adapter for LDAP	Provides an overview of the iWay Application Protocol Adapter for LDAP. Describes key features and functionality of the adapter.
2	Supported Platforms Matrix	Specifies version, platform, and database support information for iWay Application Protocol Adapter for LDAP.
3	Installing the iWay Application Protocol Adapter for LDAP	Provides installation prerequisites and describes how to install the iWay Application Protocol Adapter for LDAP.
4	Configuring and Managing Connections to an LDAP Server	Describes how to configure and manage connections to LDAP using iWay Explorer.
5	Initializing a Secure Connection to an LDAP Server	Describes how to initialize an SSL connection to an LDAP Server.
6	Creating XML Schemas for LDAP	Describes how to create XML schemas for selected LDAP entries using iWay Explorer.
7	Creating and Publishing iWay Business Services	Describes how to create and publish iWay Business Services using iWay Explorer.

	Chapter/Appendix	Contents
8	Configuring Events for LDAP	Describes how to create ports and channels to extract events from an LDAP directory using iWay Explorer.
A	Configuring the Adapter in an iWay Environment	Describes how the iWay Application Protocol Adapter for LDAP can be used.
B	Understanding Active Directory Error Messages	Lists and describes Active Directory error messages.

Documentation Conventions

The following table describes the documentation conventions that are used in this manual.

Convention	Description
THIS TYPEFACE or this typeface	Denotes syntax that you must enter exactly as shown.
this typeface	Represents a placeholder (or variable), a cross-reference, or an important term. It may also indicate a button, menu item, or dialog box option that you can click or select.
underscore	Indicates a default setting.
Key + Key	Indicates keys that you must press simultaneously.
{ }	Indicates two or three choices. Type one of them, not the braces.
|	Separates mutually exclusive choices in syntax. Type one of them, not the symbol.
...	Indicates that you can enter a parameter multiple times. Type only the parameter, not the ellipsis (...).
. . .	Indicates that there are (or could be) intervening or additional commands.

Related Publications

Visit our Technical Documentation Library at *http://documentation.informationbuilders.com*. You can also contact the Publications Order Department at (800) 969-4636.

Customer Support

Do you have any questions about this product?

Join the Focal Point community. Focal Point is our online developer center and more than a message board. It is an interactive network of more than 3,000 developers from almost every profession and industry, collaborating on solutions and sharing tips and techniques. Access Focal Point at *http://forums.informationbuilders.com/eve/forums*.

You can also access support services electronically, 24 hours a day, with InfoResponse Online. InfoResponse Online is accessible through our website, *http://www.informationbuilders.com*. It connects you to the tracking system and known-problem database at the Information Builders support center. Registered users can open, update, and view the status of cases in the tracking system and read descriptions of reported software issues. New users can register immediately for this service. The technical support section of *http://www.informationbuilders.com* also provides usage techniques, diagnostic tips, and answers to frequently asked questions.

Call Information Builders Customer Support Services (CSS) at (800) 736-6130 or (212) 736-6130. Customer Support Consultants are available Monday through Friday between 8:00 a.m. and 8:00 p.m. EST to address all your questions. Information Builders consultants can also give you general guidance regarding product capabilities and documentation. Please be ready to provide your six-digit site code number (*xxxx.xx*) when you call.

To learn about the full range of available support services, ask your Information Builders representative about InfoResponse Online, or call (800) 969-INFO.

Help Us to Serve You Better

To help our consultants answer your questions effectively, be prepared to provide specifications and sample files and to answer questions about errors and problems.

The following tables list the environment information our consultants require.

Platform	
Operating System	
OS Version	

JVM Vendor	
JVM Version	

The following table lists the deployment information our consultants require.

Adapter Deployment	For example, JCA, Business Services Provider, iWay Service Manager
Container	For example, WebSphere
Version	
Enterprise Information System (EIS) - if any	
EIS Release Level	
EIS Service Pack	
EIS Platform	

The following table lists iWay-related information needed by our consultants.

iWay Adapter	
iWay Release Level	
iWay Patch	

The following table lists additional questions to help us serve you better.

Request/Question	Error/Problem Details or Information
Did the problem arise through a service or event?	
Provide usage scenarios or summarize the application that produces the problem.	

Request/Question	Error/Problem Details or Information
When did the problem start?	
Can you reproduce this problem consistently?	
Describe the problem.	
Describe the steps to reproduce the problem.	
Specify the error message(s).	
Any change in the application environment: software configuration, EIS/database configuration, application, and so forth?	
Under what circumstance does the problem *not* occur?	

The following is a list of error/problem files that might be applicable.

- ❑ Input documents (XML instance, XML schema, non-XML documents)
- ❑ Transformation files
- ❑ Error screen shots
- ❑ Error output files
- ❑ Trace files
- ❑ Service Manager package to reproduce problem
- ❑ Custom functions and agents in use
- ❑ Diagnostic Zip
- ❑ Transaction log

For information on tracing, see the *iWay Service Manager User's Guide*.

User Feedback

In an effort to produce effective documentation, the Technical Content Management staff welcomes your opinions regarding this document. Please use the Reader Comments form at the end of this document to communicate your feedback to us or to suggest changes that will support improvements to our documentation. You can also contact us through our website, *http://documentation.informationbuilders.com/connections.asp*.

Thank you, in advance, for your comments.

Information Builders Consulting and Training

Interested in training? Information Builders Education Department offers a wide variety of training courses for this and other Information Builders products.

For information on course descriptions, locations, and dates, or to register for classes, visit our website (*http://education.informationbuilders.com*) or call (800) 969-INFO to speak to an Education Representative.

Chapter 1 Introducing the iWay Application Protocol Adapter for LDAP

The following section provides an overview of the iWay Application Protocol Adapter for LDAP.

In this chapter:

- Features of the iWay Application Protocol Adapter for LDAP
- Component Information for the iWay Application Protocol Adapter for LDAP

Features of the iWay Application Protocol Adapter for LDAP

The iWay Application Protocol Adapter for LDAP is used to provide connectivity to LDAP compliant servers. Connections are made using an LDAP URL and port number. The adapter also provides a means to exchange data between LDAP servers and third-party application, database, or external business partner systems.

The adapter uses XML messages to enable applications to communicate and exchange information with LDAP servers using one of the following methods:

- **Service Adapter.** Provides LDAP directory introspection using iWay Explorer.
  - Interactions are available to create update, search, and delete LDAP entries.
  - Read-only introspection of the LDAP schema supported by the LDAP provider.
  - Dynamic schema generation based on the selected LDAP entry.
  - The schemas serve as XML request and response schemas to enable the creation of web services.
  - Support for multi-valued attributes.
  - Supported operations include Create, Update, Delete, and Get "access" to the LDAP directory.
- **Event Adapter.** Provides the ability to extract events from the LDAP directory using:
- A directory sync protocol.
- An asynchronous event notification.

The iWay Application Protocol Adapter for LDAP supports user ID and password authentication of the LDAP simple bind standard. The adapter is tested with Microsoft Active Directory (LDAP), OpenLDAP, and the Apache Directory Server.

Component Information for the iWay Application Protocol Adapter for LDAP

The iWay Application Protocol Adapter for LDAP works in conjunction with one of the following components:

- iWay Service Manager
- iWay Business Services Provider (iBSP)

When hosted in an iWay environment, the adapter is configured through iWay Service Manager and iWay Explorer. iWay Explorer is used to configure adapter connections, create web services, and configure event capabilities.

When the adapter is hosted in a third party application server environment, iWay Explorer (used to configure LDAP server connections, create web services, and configure event capabilities) can be configured to work in a web services environment in conjunction with iBSP.

Component Information Roadmap

The following table lists the deployment component and the location of component information for the iWay Application Protocol Adapter for LDAP.

Deployed Component	For more information, see
iWay Service Manager	Appendix A of this guide *iWay Service Manager User's Guide*
iWay Explorer	Chapters 3, 4, 5, and 6 of this guide *iWay Service Manager User's Guide*
iWay Business Services Provider (iBSP)	*iWay Installation and Configuration*

iWay Service Manager

iWay Service Manager is the heart of the Universal Adapter Framework and is an open transport service bus. Service Manager uses graphical tools to create sophisticated integration services without writing custom integration code by:

- Creating metadata from target applications.
- Transforming and mapping interfaces.
- Managing stateless processes.

Its capability to manage complex adapter interactions makes it ideally suited to be the foundation of a service-oriented architecture.

iWay Explorer

iWay Explorer uses a tree metaphor to introspect the LDAP entries. The explorer enables you to create XML schemas and web services for the associated entry. In addition, you can create ports and channels to listen for events. External applications that access the iWay Application Protocol Adapter for LDAP use either XML schemas or web services to pass data between the external application and the adapter.

iWay Business Services Provider

The iWay Business Services Provider (iBSP) exposes (as web services) enterprise assets that are accessible from adapters regardless of the programming language or the particular operating system.

iBSP simplifies the creation and execution of web services when running:

- Custom and legacy applications.
- Database queries and stored procedures.
- Packaged applications.
- Terminal emulation and screen-based systems.
- Transactional systems.

Coupled with a platform and language independent messaging protocol called SOAP (Simple Object Access Protocol), XML enables application development and integration by assembling previously built components from multiple web services.

Chapter 2

Supported Platforms Matrix

iWay Software is committed to support the diverse environments and varied systems of our users through support for leading enterprise applications, platforms, and databases.

This section specifies version, platform, and database support information for iWay Application Protocol Adapter for LDAP (Lightweight Directory Access Protocol). It is designed to provide a consolidated view of the versions, operating systems, operations, and data types, which are supported by the adapter.

In this chapter:

- iWay Application Protocol Adapter for LDAP Overview
- LDAP Versions
- Operating Systems
- Databases
- Java Development Kit (JDK)
- Communication Modes
- Object Types and Interfaces
- Communication Types
- Operations
- Data Types
- Other Functions
- Known Limitations
- Related Information for Specific iWay Releases

iWay Application Protocol Adapter for LDAP Overview

iWay Application Protocol Adapter for LDAP is used to provide connectivity to LDAP compliant servers. LDAP is a standard way to access and maintain directory information over the Internet Protocol. Connections are made using an LDAP URL and port number. The adapter provides a way to exchange data between LDAP servers and third-party applications, or secure LDAP connections between servers.

LDAP Versions

iWay Application Protocol Adapter for LDAP supports the following LDAP versions.

Microsoft

- Windows Server Active Directory 2008

- Windows Server Active Directory 2008R2
- Windows Server Active Directory 2012
- Windows Server Active Directory 2012R2

Others

- OpenLDAP (2.4.8 and higher versions)
- Apache Directory Server 2.0 (m1 and higher).

Contact Customer Support for any LDAP servers that are not included on this list.

Operating Systems

iWay Application Protocol Adapter for LDAP supports the following operating systems:

- Microsoft Windows
- Enterprise Linux (RHEL, CentOs, Oracle Linux, SUSE)
- Unix

Contact Customer Support for any host operating systems that are not included on this list.

Databases

iWay Application Protocol Adapter for LDAP does not function directly with databases, but uses the LDAP Application Interface (API).

Java Development Kit (JDK)

iWay Application Protocol Adapter for LDAP supports the Java Development Kit (JDK) versions that are listed in the *iWay Installation and Configuration Guide* under *Java Requirements*.

Communication Modes

iWay Application Protocol Adapter for LDAP supports the following communication modes:

- **Services (Outbound).** iWay Application Protocol Adapter for LDAP can send messages to LDAP.
- **Events (Inbound).** iWay Application Protocol Adapter for LDAP can receive messages from LDAP.

Object Types and Interfaces

The following object types and interfaces are supported by iWay Application Protocol Adapter for LDAP:

- **Host.** Fully Qualified Domain Name (FQDN) of the LDAP server.
- **Port.** Network port of the LDAP server.
- **DN.** Distinguished name of an entry or an entry search base.
- **Attributes.** Attributes that belong to a DN entry.
- **Filter.** Search filter for the tree based directory.

Communication Types

iWay Application Protocol Adapter for LDAP supports the following communication types:

- **LDAP**
- **LDAPS** (Secured and encrypted with the configured security certificate.)

Operations

The following operations are supported by iWay Application Protocol Adapter for LDAP:

- Simple Bind
- Search entry
- Retrieve entry
- Add a new entry
- Modify an entry
- Delete an entry
- Modify or Move DN (Active Directory only)
- UnBind

Data Types

The following Data Types are supported by iWay Application Protocol Adapter for LDAP:

- byte
- short
- int
- long
- float
- double
- Boolean
- char
- String

Other Functions

Other functions are not applicable to the iWay Application Protocol Adapter for LDAP.

Known Limitations

This section lists and describes known limitations for iWay Application Protocol Adapter for LDAP.

- Operations depend on access level and user rights. Update operations on certain Active Directory nodes at the group level are not currently possible (for example, defined groups: Users, Computers, and so on).
- Not all functionality may be supported on extended operating systems. Some Linux and Unix systems restrict LDAP events or updates.
- Microsoft Active Directory Application Mode (ADAM) is not supported.
- Only *Simple Bind* is supported. Specifically, *anonymous* and *SASL_mechanism* as described in RFC_2195 are not supported.

Related Information for Specific iWay Releases

For more information, see the *iWay New Features Bulletin and Release Notes* documentation for a specific release (for example, iWay Version 7.0.3).

Chapter 3

Installing the iWay Application Protocol Adapter for LDAP

This section provides installation prerequisites and describes how to install the iWay Application Protocol Adapter for LDAP.

In this chapter:

- Installation Prerequisites
- Installing the iWay Application Protocol Adapter for LDAP

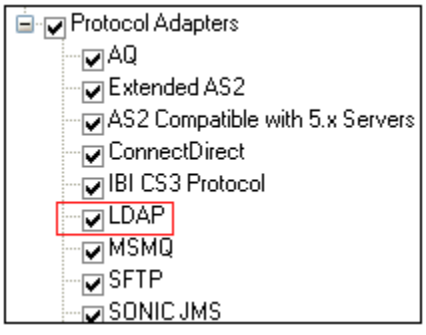
Installation Prerequisites

The following components must be installed and configured before installing the iWay Application Protocol Adapter for LDAP:

- iWay Service Manager Version 7.0 or higher (running with Java 1.7). For more information, see the *iWay Installation and Configuration Guide* and the *iWay Service Manager User's Guide*.
- Third-party application (Optional).
- Access to a system running LDAP, or the Microsoft Active Directory.

Installing the iWay Application Protocol Adapter for LDAP

In iWay Service Manager (iSM) Version 7.0, the iWay Application Protocol Adapter for LDAP supports 32- and 64-bit JVM environments. The required components for both environments are automatically installed. During the iSM installation process, ensure that LDAP is selected under the Protocol Adapters category in the Adapter Selection pane, as shown in the following image.



Required Installation Files

The iSM installation process installs the following LDAP adapter components in the *<ism_home>*\lib directory:

- **iwldap.jar.** Exposes design time and runtime interfaces for the iWay Application Protocol Adapter for LDAP.
- **ldapbp.jar**

The following required file is specific to the JVM version being used:

- **Dnsns.jar**

Note: The functionality of the ldapsec.jar file is now part of the rt.jar file, and no longer independently shipped.

These JVM files can be downloaded from the Oracle Technology Network website:

http://www.oracle.com/technetwork/java/index.html

Copy the Dnsns.jar file to the following directory.

JRE_Home`\lib\ext`

where:

JRE_Home

Is the root installation directory for your Java Runtime Environment.

Chapter 4

Configuring and Managing Connections to an LDAP Server

The following section describes how to configure and manage connections to LDAP using iWay Explorer.

In this chapter:

- Starting iWay Explorer
- Adding the LDAP Adapter to iWay Explorer
- Working With a Target

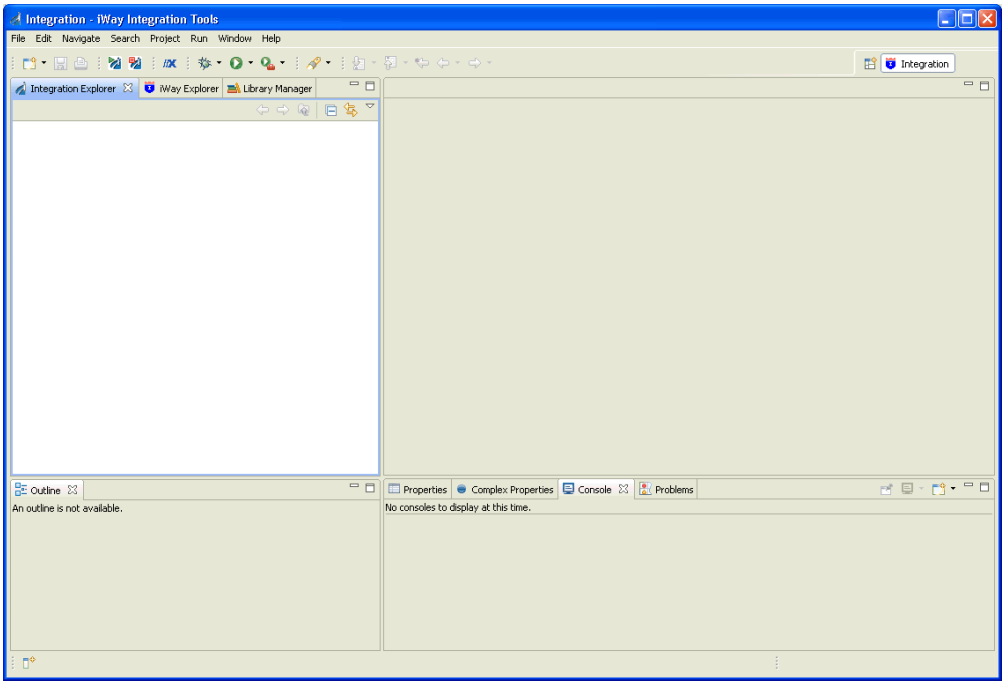
Starting iWay Explorer

This section describes how to start iWay Explorer.

Procedure: How to Open iWay Integration Tools

1. Navigate to your local drive where you have iIT installed, and open the *eclipse* folder.
2. Double-click *iit.exe*.

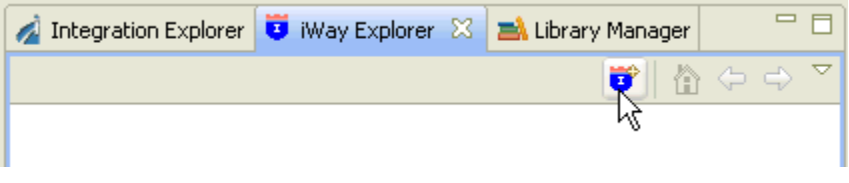
iWay Integration Tools suite opens.



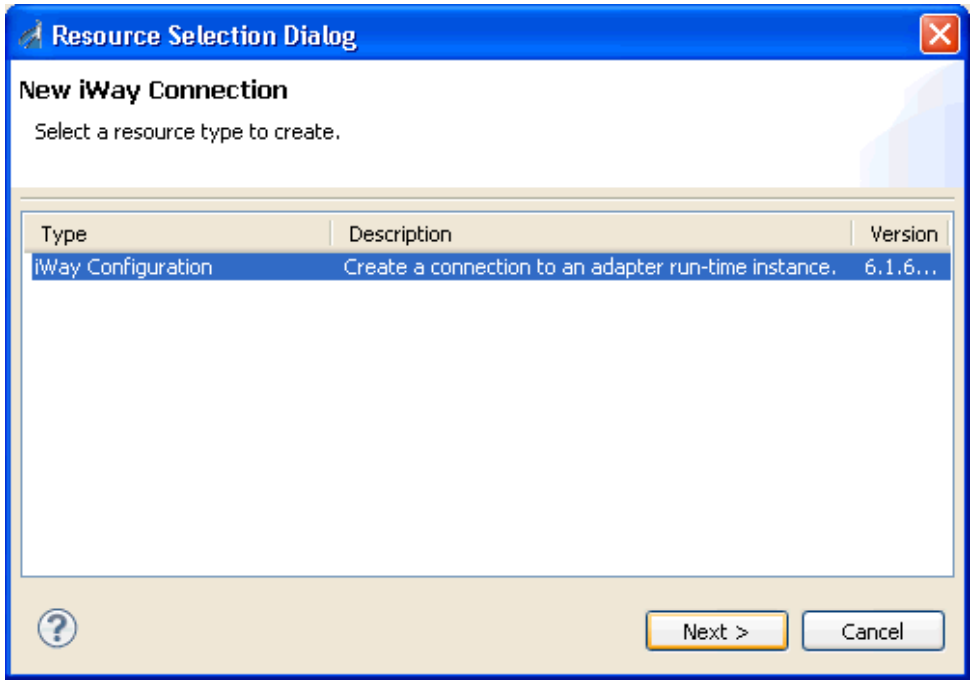
Procedure: How to Create an iWay Explorer Connection to an iSM Server

This procedure assumes that you have opened iWay Integration Tools (iIT) and are in the Workbench.

1. Click the *iWay Explorer* tab to make it active.
2. Click the *Launch iWay Resource Creator Wizard* button on the tool bar.
   In the following image, the iWay Explorer tab is active, and the cursor is pointing to the Launch iWay Resource Creator Wizard button.



When you click the button, the Resource Selection Dialog opens and displays the New iWay Connection pane, as shown in the following image.



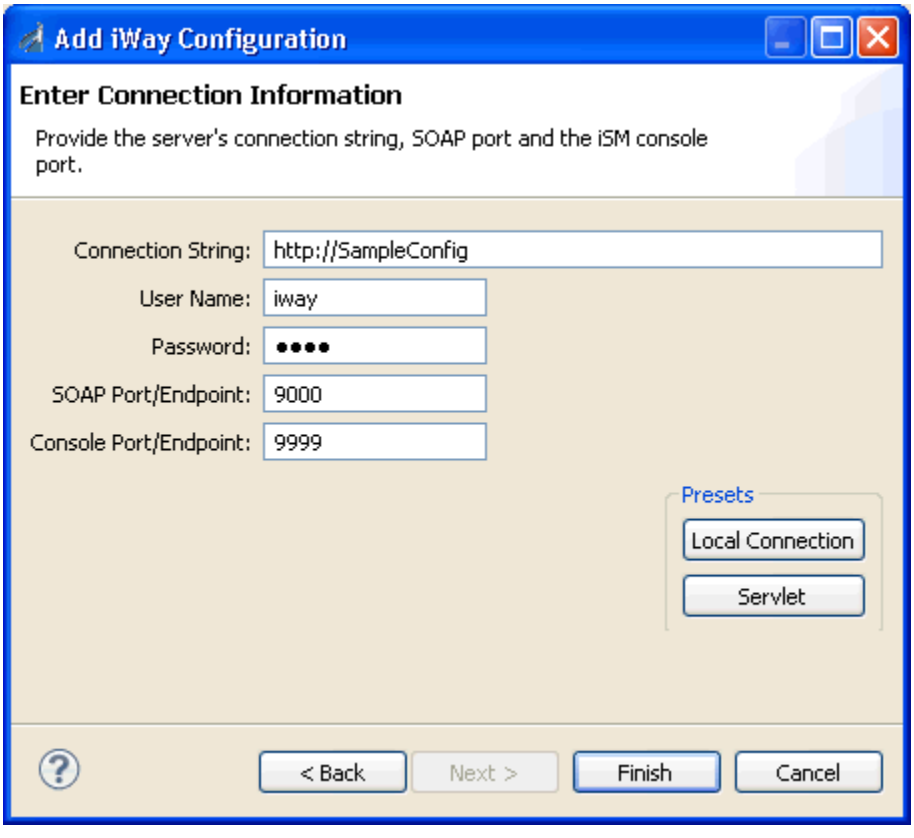
3. Under the Type heading, click *iWay Configuration*, which is the type of resource that you are going to create.
4. Click *Next*.

   The Add iWay Configuration dialog box opens and displays the Select Connection Types pane.
5. In the Configuration Alias field, type a name for the new configuration (for example, *SampleConfig*).

   Tip: The name that you supply is used only for display purposes in the tree. It is not a server connection property.
6. For Connection Type, ensure that the *HTTP Connection* is selected.
7. Optionally, select the *Connect to Host upon Wizard Completion* check box if you want iWay Explorer to automatically connect to this instance of iSM after you have created it. If you select this option, all the explorer environments under the new iSM connection are automatically connected to iSM when this procedure is finished.

   If you do not select this option, the explorer environments are not automatically connected to iSM. You can connect to an individual explorer environment when you want to access it.

8. Click *Next* to continue the procedure.
9. If you selected an HTTP Connection, the Enter Connection Information pane opens, as shown in the following image.



- Verify the values in the three fields, or type the valid value or values.
  - The Connection String field contains the URL that connects to the iSM.
  - The SOAP Port/Endpoint field contains the SOAP port number.
  - The Console Port/Endpoint field contains the port number that the iSM Administration Console is listening on.
- Optionally, under Presets, click *Local Connection* to insert values for a local default iSM connection in the fields, or click *Servlet* to insert values for a sample servlet connection.

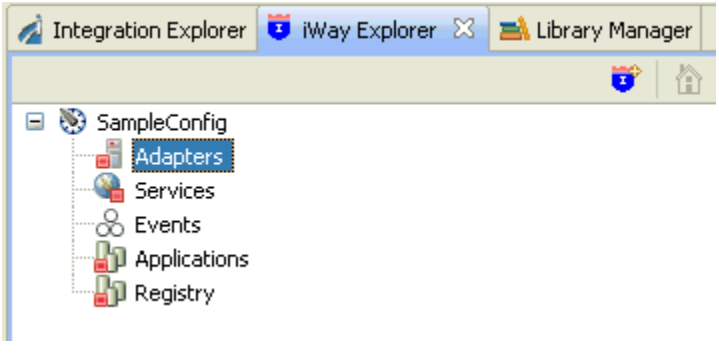
- Click *Finish*.
- In the File Path field, browse to the full path for your iWay installation directory and insert the path in the field. This path is used to locate the iWay adapters and store the XML schemas. For example:

  ```
  C:\Program Files\iWay7
  ```

- In the Configuration Name field, verify the name of your iWay server configuration. The base configuration is specified by default. Alternatively, you can type the name of the server configuration.
- Click *Finish*.

The new iSM connection is added to the tree on the iWay Explorer tab.

In the following image, an iSM connection named SampleConfig was added to iWay Explorer. The tree is expanded to show the five explorer environments that are available.



Adding the LDAP Adapter to iWay Explorer

iWay Explorer supports access to many different application systems. When you connect to and expand the Adapters node, the iWay adapters for the supported application systems are displayed. They are the iWay adapters that you have installed and are licensed to use.

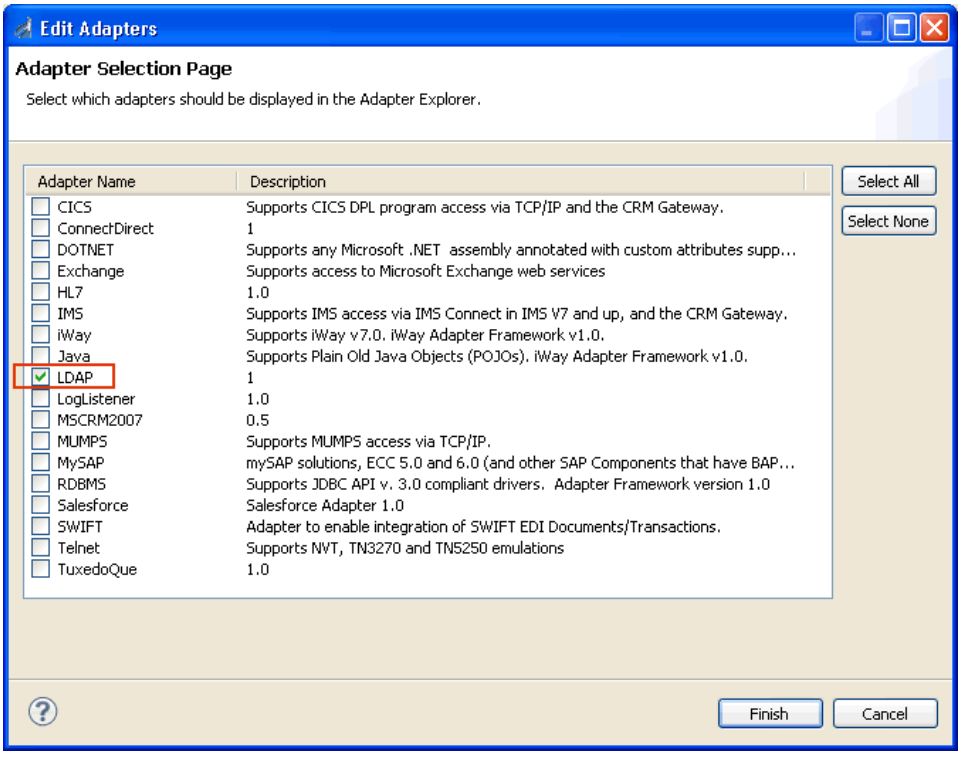
Procedure: How to Add the LDAP Adapter to iWay Explorer

In this procedure, you are going to add the iWay Application Protocol Adapter for LDAP to the list of adapters displayed in the Adapters node.

1. Right-click the *Adapters* node, and click *Edit* from the menu.

   The Edit Adapters dialog opens, prompting you to select the iWay adapter or adapters to add to iWay Explorer.

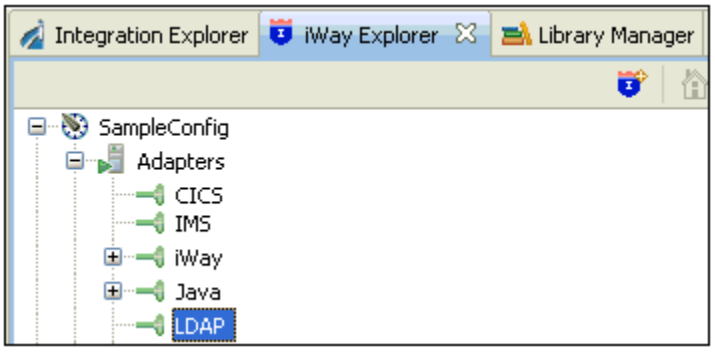
2. Select the check box for *LDAP*, as shown in the following image.



3. Click *Finish*.

   The tree is automatically refreshed and displays the new adapter.

   In the following image, the LDAP node is displayed in the Adapters node of iWay Explorer, as shown in the following image.



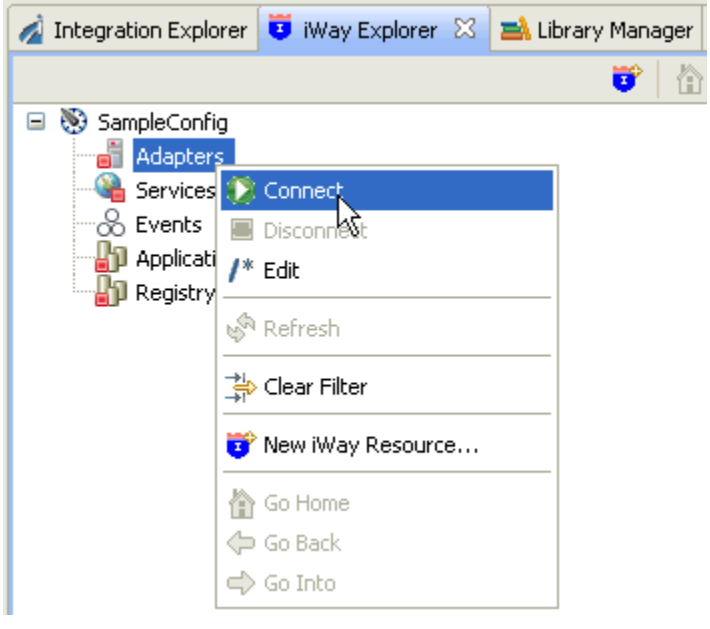
Working With a Target

To browse the metadata and objects of an application system, you must create a target for that system. The target is the means by which you connect to the system. It contains the logon properties used to access the system.

Using the target, you must establish a connection to an application system every time you want to browse the system in iWay Explorer.

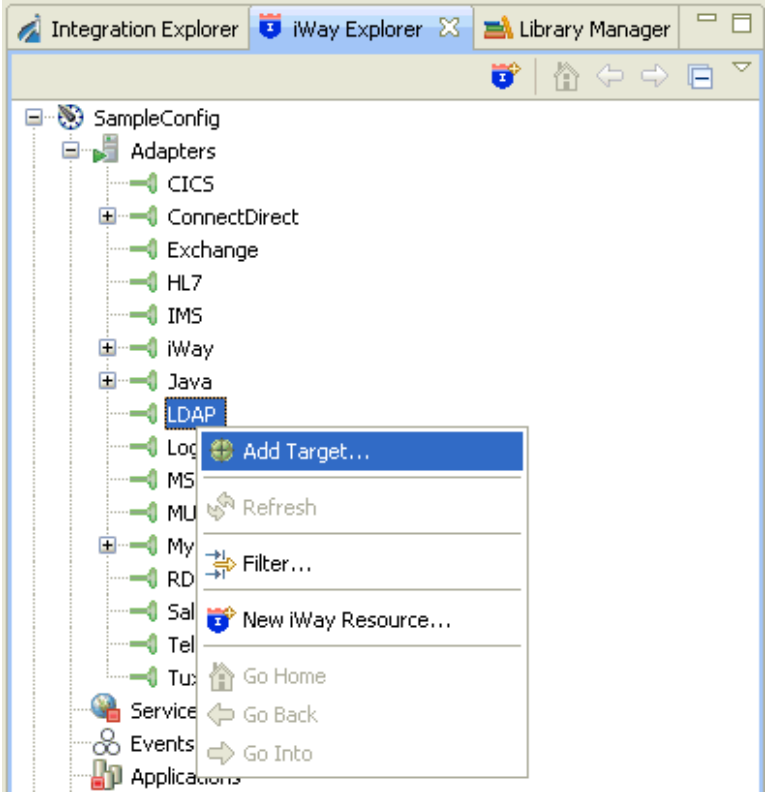
Procedure: How to Create a Target

1. Right-click the *Adapters* node, and click *Connect* from the menu, as shown in the following image.

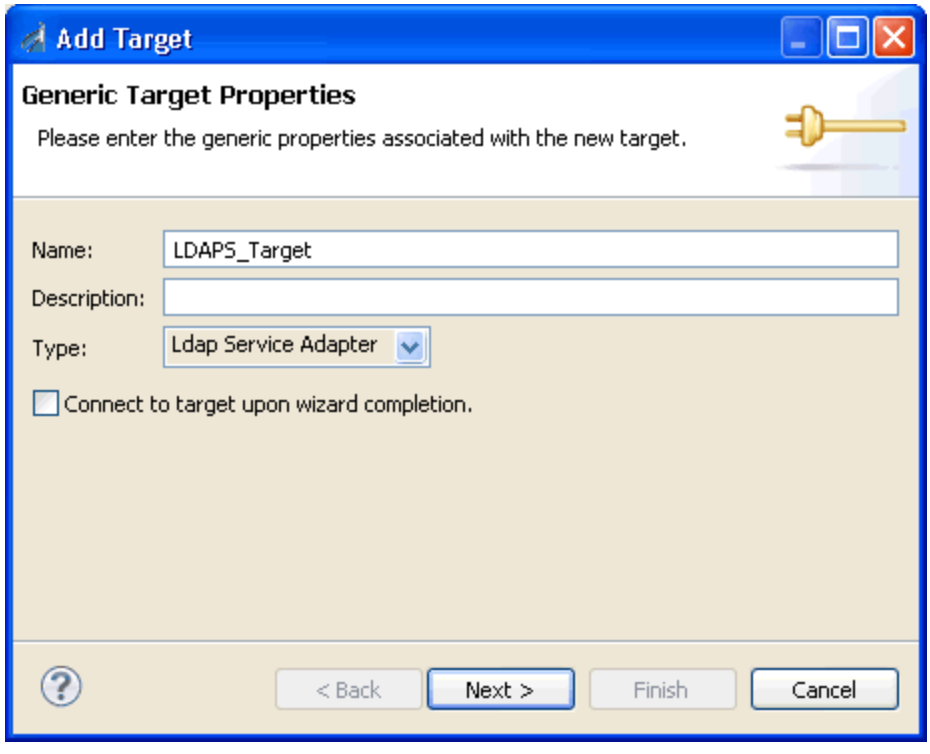


2. Once you are connected, expand the *Adapters* node.

3. Right-click *LDAP*, and click *Add Target* from the menu, as shown in the following image.



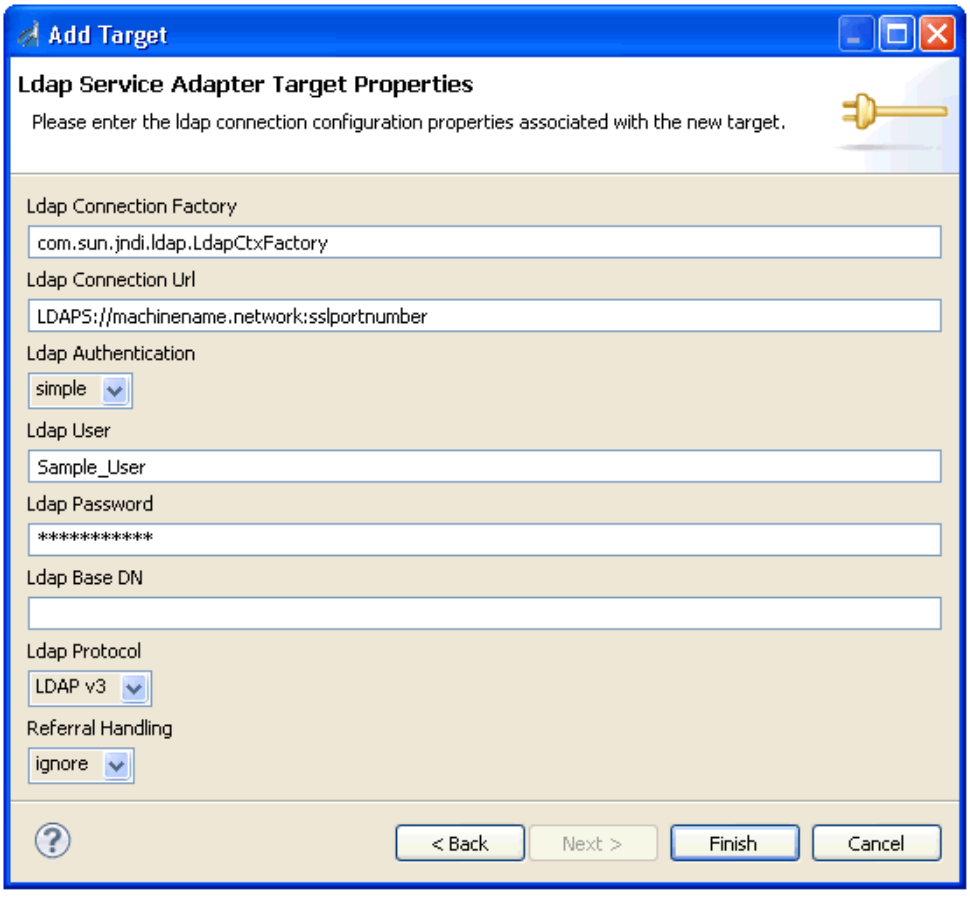
The Add Target dialog opens and displays the Generic Target Properties pane, as shown in the following image.



4. Supply the values for the fields on the dialog box as follows.
   a. In the Name field, type a descriptive name for the target (for example, *LDAPS_Target*).
   b. In the Description field, optionally type a brief description of the target.
   c. From the Type drop-down list, select *Ldap Service Adapter* (default).
5. Select the *Connect to target upon wizard completion* check box if you want iWay Explorer to automatically connect to this target after it has been created.

   If you deselect this option, iWay Explorer will not automatically connect to the target. From the tree, you can connect to an individual target when you want to access the associated application system.
6. Click *Next*.

The Add Target dialog opens and displays the Ldap Service Adapter Target Properties pane, as shown in the following image.



7. Supply the connection information for the LDAP system to which you are connecting.

   The following table lists and describes the LDAP connection parameters.

Parameter	Description
Ldap Connection Factory	The connection factory class that is used to access the LDAP server. The default connection factory implementation is com.sun.jndi.ldap.LdapCtxFactory, as provided by Java SDK.

Parameter	Description

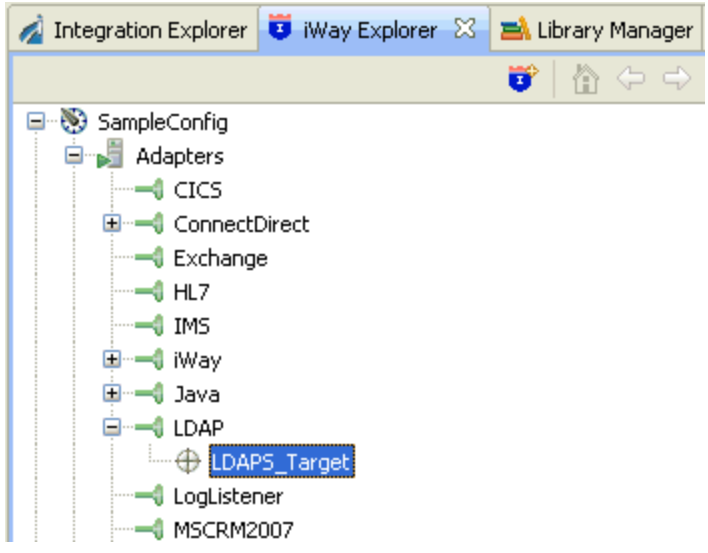
Ldap Connection Url	The connection URL that is used to identify the LDAP server and connection context. This URL can use the following formats:
	❑ For unsecured access:
	`LDAP://machinename.network:portnumber`
	where:
	machinename
	Is the name of the system hosting the LDAP server.
	network
	Is the network of the LDAP server (such as *mycompany.com*).
	portnumber
	Is the port number of the LDAP server.
	❑ For secured access:
	`LDAPS://machinename.network:sslportnumber`
	where:
	machinename
	Is the name of the system hosting the LDAPS Directory Server.
	network
	Is the network of the LDAPS Directory Server (such as *mycompany.com*).
	sslportnumber
	Is the SSL port number of the LDAPS Directory Server.

Ldap Authentication	The authentication mechanism that is used to connect to the LDAP server. Currently, the adapter supports User ID and Password authentication of the *simple* bind standard.

Parameter	Description
Ldap User	The user password used that is used to access the LDAP server.
Ldap Password	A valid password that is associated with the user name.
Ldap Base DN	The relative entry point of the LDAP tree. If this field is empty, then the root DN is used.
Ldap Protocol	Currently, the adapter supports LDAP version 2 and LDAP version 3, as per target server requirements. Select one of the following LDAP versions from the drop down list: ❑ LDAP v3 (default) ❑ LDAP v2
Referral Handling	Select one of the following options from the drop-down list: ❑ ignore (default) ❑ follow

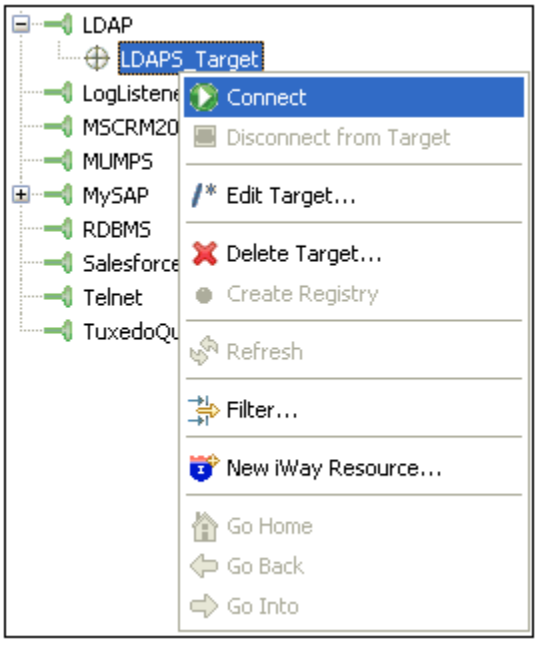
8. Click *Finish* when you are done.

The new LDAP target is added to the Adapters node of iWay Explorer, as shown in the following image.

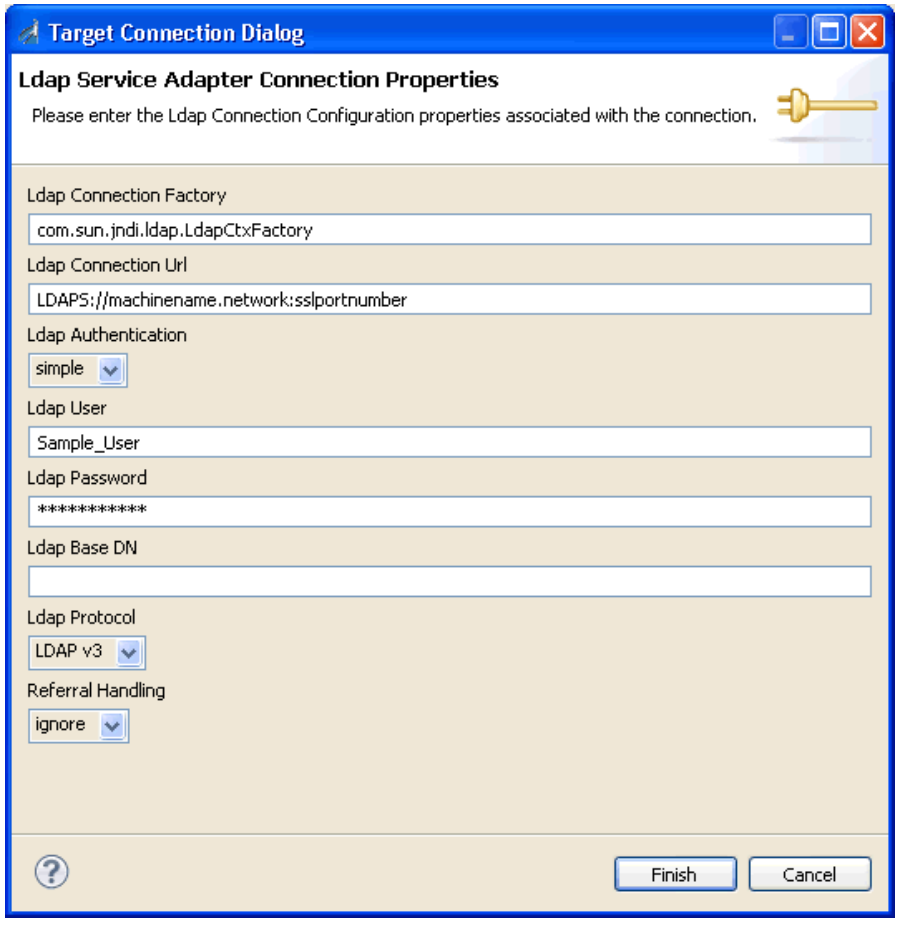


Procedure: How to Connect to a Target

1. Expand the *LDAP* node to locate the name of the target that you want to connect to, for example, *LDAPS_Target*.
2. Right-click the target, and click *Connect* from the menu, as shown in the following image.

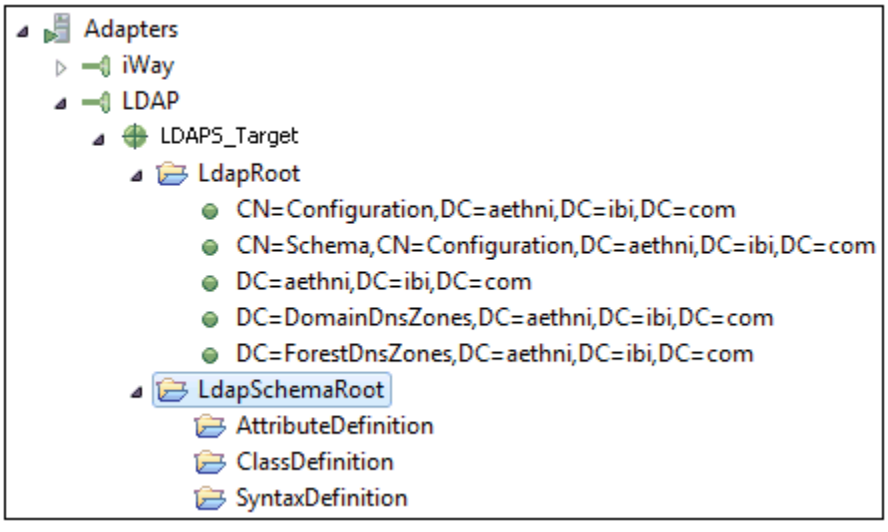


The Target Connection Dialog opens, as shown in the following image.



3. Enter a valid password for the configured LDAP target and click *Finish*.

The LDAPS_Target node icon changes to green, and two folders are displayed (LdapRoot and LdapSchemaRoot), reflecting a successful connection. You can click a folder and then expand it to display its contents.



Understanding the LDAP Tree Display

This section describes how LDAP objects are structured and represented in iWay Explorer after a successful connection to an adapter target is made.

- **Schema Root.** The base of the definitions of objects in the directory tree.
  - **Class Definition.** Determines the type of objects that are defined in the directory tree.
  - **Attribute Definition.** Attributes are predefined holders of information for a directory entity, or the operational information about the entity. For example, *address* and *datecreated*.
  - **Syntax Definition.** An LDAP server may return information about permitted syntax combinations using the schema.
- **LDAP Root.** The root (or 0) level of the entity tree, or the root branch if a value for the *Ldap Base DN* connection parameter is provided.

Procedure: How to Disconnect From a Target

Although you can maintain multiple open connections to different application systems, it is a good practice to close a connection when you are not using it.

1. In the tree, expand the *LDAP* node to locate the name of the target from which you want to disconnect, for example, *LDAPS_Target*.
2. Right-click the target, and click *Disconnect from Target* from the menu.

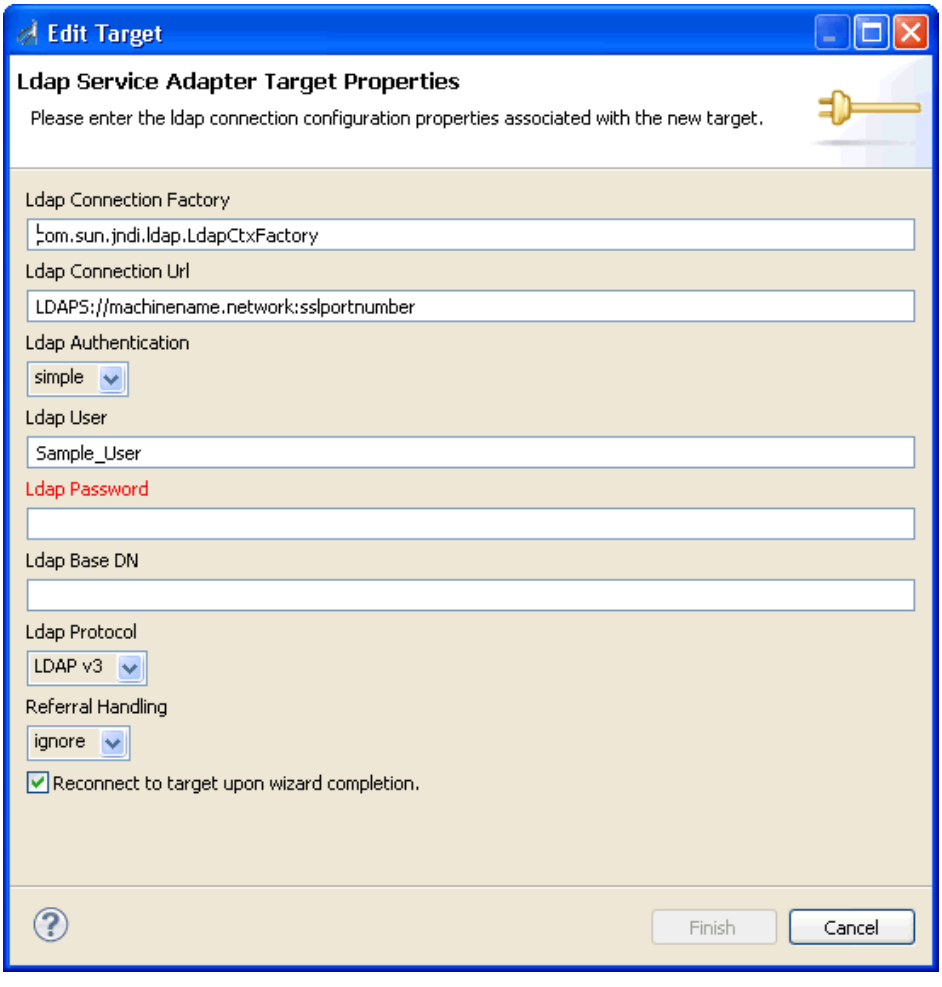
   The connection to the application system is closed.

Procedure: How to Edit a Target

After you create a target, you can edit the information that you provided during the creation procedure.

1. In the tree, expand the *LDAP* node to locate the name of the target that you want to edit, for example, *LDAPS_Target*.
2. Right-click the target, and click *Edit Target* from the menu.

The Edit Target dialog opens and displays the LDAP adapter target properties, as shown in the following image.



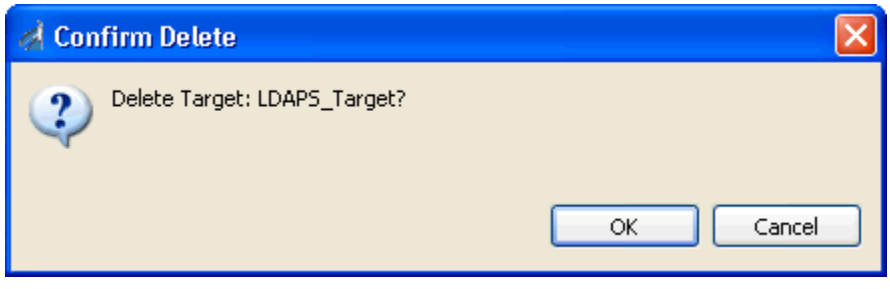
3. Modify the connection properties as required.
4. Optionally select the *Reconnect to target upon wizard completion* check box if you want iWay Explorer to automatically connect to this target after it has been edited. iWay Explorer will use the modified properties to connect.
5. Click *Finish* when you have made your edits.

Procedure: How to Delete a Target

You can delete a target that is no longer needed. You can delete it whether or not it is closed. If open, the target automatically closes before it is deleted.

1. In the tree, expand the *LDAP* node to locate the name of the target that you want to delete, for example, *LDAPS_Target*.
2. Right-click the target, and click *Delete Target* from the menu.

   iWay Explorer displays a prompt, asking you to confirm the deletion of the selected target, as shown in the following image.



3. Click *OK* to proceed with the deletion.

Chapter 5 Initializing a Secure Connection to an LDAP Server

This section describes how to initialize an SSL connection to an LDAP Server.

Note: After you finish installing the required certificate for the LDAP Server as a trusted certificate in the Java keystore, proceed to *Configuring and Managing Connections to an LDAP Server* on page 27.

In this chapter:

- Prerequisites Before SSL Connection to LDAP
- Installing a Secure Certificate for an LDAP Server

Prerequisites Before SSL Connection to LDAP

Before you initialize an SSL connection to LDAP, ensure that the following prerequisites are followed:

- A signed SSL certificate from the LDAP Server must be available.
- The name of the LDAP Server certificate must match the name of the machine to which you are connecting.
- The LDAP certificate must be installed in the *JAVA_HOME*\jre\lib\security directory of the trust store within the Java Runtime Environment (JRE).

  where:

  JAVA_HOME

  Is the root installation directory of your Java Runtime Environment (JRE).
- The alias name in the Import command must match the name of the LDAP Server to which you are connecting.
- The default keystore password is *changeit*.
- During the adapter target configuration process, you must specify the LDAP connection URL as follows:

  `LDAPS://machinename.network:sslportnumber`

where:

machinename

Is the name of the system hosting the LDAP Server.

network

Is the network of the LDAP Server.

sslportnumber

Is the SSL port number of the LDAP Server.

Installing a Secure Certificate for an LDAP Server

Before you create a LDAP over SSL (LDAPS) connection using the iWay Application Protocol Adapter for LDAP, the certificate for the LDAP Server (Active Directory Server, Open LDAP, or other type) must first be installed as a trusted certificate in the Java keystore.

Procedure: How to Add a Certificate to the Java Keystore File

By default, the Java Runtime Environment (JRE) maintains a Common Access Card (CAC) keystore, which is called *cacerts*, in the *JAVA_HOME*\jre\lib\security directory.

1. Copy the *servername*.crt file to the *JAVA_HOME*\jre\lib\security directory.

   where:

   servername

   Is the name of the LDAP Server.

   JAVA_HOME

   Is the root installation directory of your Java Runtime Environment (JRE).

2. Open a command prompt window as an Administrator and navigate to the *JAVA_HOME*\jre\lib\security directory.

3. Execute the following command:

   ```
   keytool -import -trustcacerts -alias servername -file servername.crt -
   keystore cacerts
   ```

   where:

   servername

   Is the name of the LDAP Server.

   You are prompted for the keystore password.

4. Type *changeit* and press Enter.
   You are prompted whether you want to trust this certificate.
5. Type *yes* and press Enter.

   A message is displayed indicating that the certificate was successfully added to the keystore.

   For more information on obtaining a certificate from Microsoft Active Directory, see the following web site:

   http://social.technet.microsoft.com/wiki/contents/articles/2980.ldap-over-ssl-ldaps-certificate.aspx

   If the location of this online document should change or the link is invalid, go to *http://technet.microsoft.com* and search for a document called *LDAP over SSL (LDAPS) Certificate*.

   Secure LDAP on other platforms may require the installation of OpenSSL or other operating system packages. Consult the vendor for the instructions on when the certificate is installed and how to acquire a client copy of the server's certificate.

   The other option that is available to all users is a third-party signing authority that provides a certificate for the link between the parties. For more information, see the *Transport Layer Security* topic on the following website:

   http://en.wikipedia.org/wiki/Transport_Layer_Security

Procedure: How to Enable a Specific Keystore File With Java

As an alternative to the previous procedure, you can configure your Java Runtime Environment (JRE) to use a specific (user-created) keystore file.

1. Copy the keystore file to a location on your file system (for example, c:\iway7).
2. Set the following Java system properties:

   ```
   -Djavax.net.ssl.keyStorePassword = changeit
   -Djavax.net.ssl.keyStore = c:/iway7/servername.jks
   -Djavax.net.ssl.trustStore = c:/iway7/servername.jks
   ```

   where:

   servername

   Is the name of the LDAP Server.

The following list describes the specific keys you must set in more detail:

- **javax.net.ssl.keyStorePassword.** Password to access the private key from the keystore file specified by javax.net.ssl.keyStore. This password is used twice, to unlock the keystore file (store password), and to decrypt the private key stored in the keystore (key password).
- **javax.net.ssl.keyStore.** Location of the Java keystore file containing a certificate and private key of an application process. On Windows, the specified path name must use forward slash characters (/), in place of back slash characters (\).
- **javax.net.ssl.trustStore.** Location of the Java keystore file containing the collection of CA certificates trusted by this application process (trust store). On Windows, the specified path name must use forward slash characters (/), in place of back slash characters (\).

Reference: Additional Considerations and Online Resources

For more information on using the Java keytool, see the following web site:

http://docs.oracle.com/javase/6/docs/technotes/tools/solaris/keytool.html

If the location of this online document should change or the link is invalid, go to *http://docs.oracle.com* and search for a document called *keytool - Key and Certificate Management Tool*.

It is also important to know the format of the certificate used for authentication, since not all tools and methods accept all formats. If you are using a Windows platform, see the following web site:

http://technet.microsoft.com/en-us/library/cc770735(v=ws.10).aspx

If the location of this online document should change or the link is invalid, go to *http://technet.microsoft.com* and search for a document called *Certificate File Formats*.

If you are using OpenSSL or other products for Linux, UNIX, or other operating systems, see the following web site for more information on certificate management with OpenSSL:

http://gagravarr.org/writing/openssl-certs/general.shtml

It may also be necessary to convert certificate file formats if the certificate type provided to you by the certificate authority is not the type you are using in your SSL certificate store.

Chapter 6

Creating XML Schemas for LDAP

The following section describes how to create XML schemas for LDAP entries using iWay Explorer.

In this chapter:

- LDAP Processing Overview
- Browsing LDAP Entries
- Generating XML Schemas for LDAP Operations

LDAP Processing Overview

The iWay Application Protocol Adapter for LDAP enables the processing of LDAP entries.

External applications that access LDAP through the adapter use either XML schemas or web services to pass data between the external application and the adapter. You can use iWay Explorer to create the required XML schemas and web services. iWay Explorer also provides interactive dialogs to perform LDAP operations.

LDAP must be installed, configured, and available for client access. iWay Explorer need not reside on the same system as the application system being accessed, but network access is required.

Browsing LDAP Entries

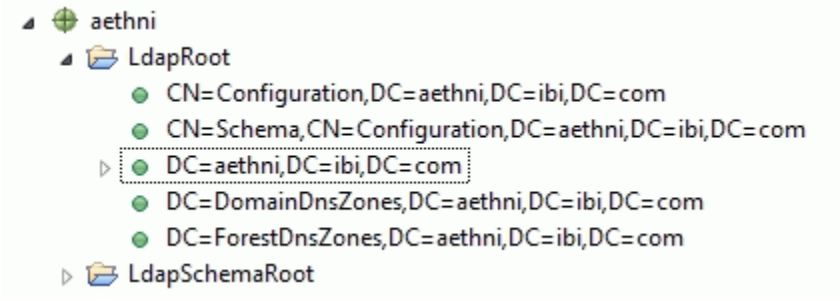
After you are connected to LDAP, iWay Explorer enables you to explore and browse LDAP entry metadata.

Procedure: How to Browse LDAP Entries

To browse LDAP entries:

1. Connect to a LDAP target, as described in *Configuring and Managing Connections to an LDAP Server* on page 27.
2. In the left pane, expand the target node.

LDAP entries are located under the target node.

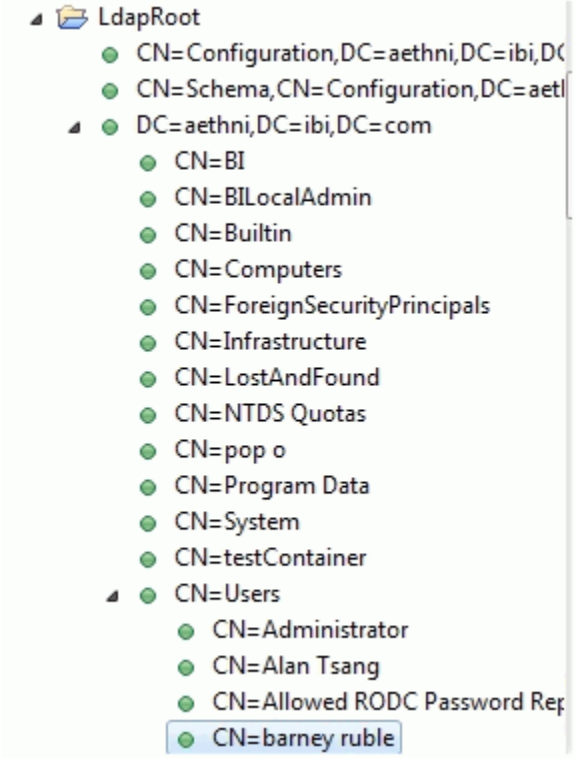


The *Schema* and *Configuration* nodes contain the permissible objects and attributes for this instance of LDAP, which is provided by the server.

The *LdapRoot* node contains the managed objects of the server. If the server has multiple partitions, you may have more than one Domain Component. Each Domain Component has subentries defined by their categories or by their common name.

Note: An entry may be an item or a reference to an item. The resolution to an object may reside on another server and access may be limited by security. It also depends on the setting of the Referral Handling parameter in the adapter target.

A sample subtree of the Domain Component *aethni* is shown in the following image. Each item has a relative domain name composed of the nodes to the item, and a parent context that defines the general realm of definitions.



The following image shows the Properties tab in iWay Explorer, which lists the simple properties of the entry:

- Name
- Type
- Container (true/false)
- RDN

- Parent

Properties | Complex Properties | Console | Problems

Property	Value
Ldap Entry RDN	CN=barney ruble,CN=Users,DC=aethni,DC=ibi,DC=com
Ldap Parent Context	CN=Users,DC=aethni,DC=ibi,DC=com
Name	CN=barney ruble

To view a complete listing of properties for an entry, click the *Complex Properties* tab, as shown in the following image.

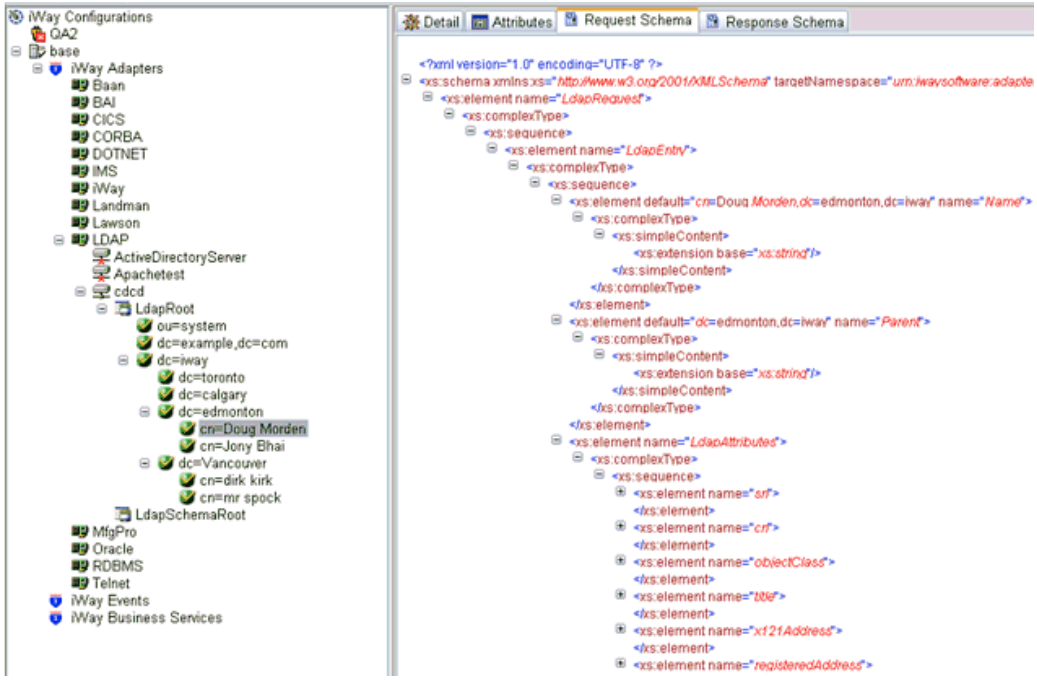
Properties | Complex Properties | Console | Problems

Ldap Attribute ...	Ldap Attribute Value	Ldap Attribute ...	Ldap Attribute ...
objectClass	top|person|organizationalPerson|user		true
instanceType	4		true
nTSecurityDesc...	null		true
objectCategory	CN=Person,CN=Schema,CN=Configu...		true
cn	barney ruble		false
description	null		false
distinguishedN...	CN=barney ruble,CN=Users,DC=aethn...		false
whenCreated	20110405175208.0Z		false
whenChanged	20110405175208.0Z		false
subRefs	null		false
displayName	barney ruble		false
uSNCreated	16822		false
isDeleted	null		false
dSASignature	null		false
objectVersion	null		false
repsTo	null		false
repsFrom	null		false
memberOf	CN=iwqual,CN=Users,DC=aethni,DC=...		false
ownerBL	null		false
uSNChanged	16828		false
uSNLastObjRem	null		false
showInAdvanc...	null		false
adminDisplayN...	null		false
proxyAddresses	null		false
adminDescripti...	null		false
extensionName	null		false
uSNDSALastOb...	null		false
displayNamePr...	null		false

You may need to expand this window to view the complete list of properties for the entry.

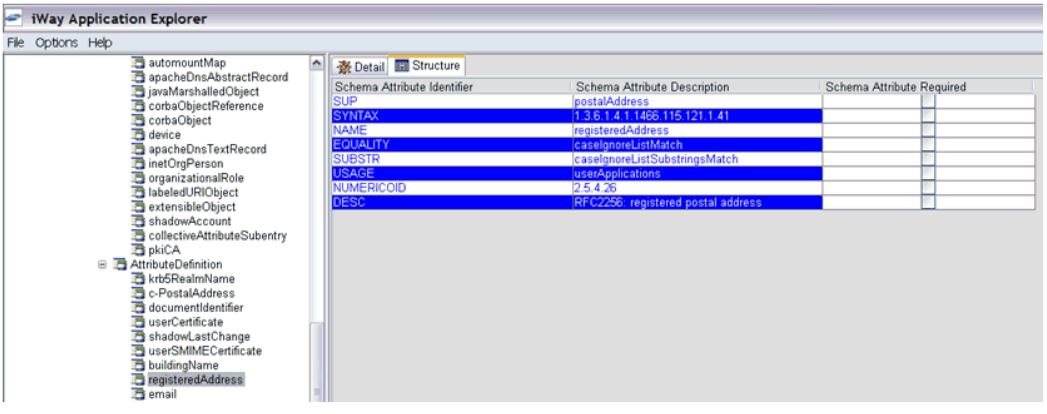
The objectClass attribute provides a complete list of categories to which the user belongs, starting from the root. Attributes provide additional information about an entry. Many of the entries are null, which means that no entry exists. Some schema properties are required, which means that they must be entered.

An XML request schema can be used to build a run-time request for a selected object. To export a schema, right-click a selected object in the left pane, and select *Export Schemas* from the context menu.

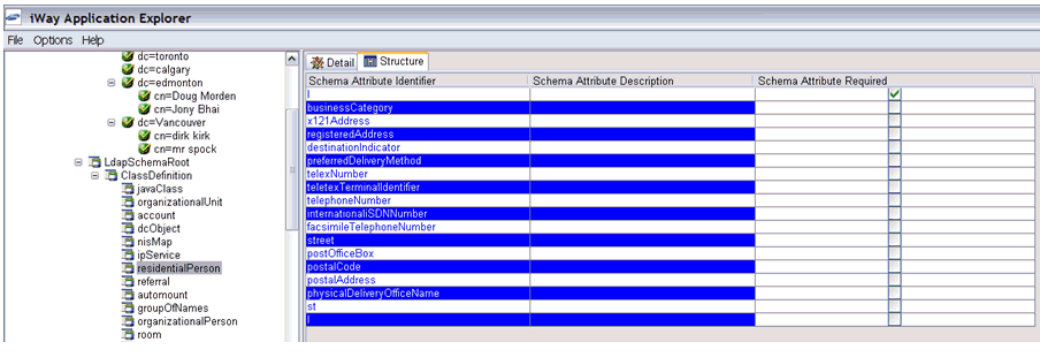


Schema Node Browsing

The Schema node appears under a specific schema and may also appear in the general tree of entries. The object classes define the categories that contain an entry and the attributes determine the information contained in the directory entry. Some LDAP servers may allow you to browse the Syntax node, while others do not. The Schema node is used to define the information contained in the directory. Browse the schema for general information about the directory and the related objects. No operations can be performed at this level.



The schema browsing view displays Class Definition views, Attribute Definition views, and Syntax Definition views.



Generating XML Schemas for LDAP Operations

The supported LDAP operations are:

- Create
- Update

- Delete
- Get
- Move

You must ensure that security access for these operations is granted. If not, then these operations will be denied when they are being executed, during run time.

Browse to an entry that will require a Move, Get, Update, or Delete operation to be performed. Right-click the entry and select *Create Schema* from the context menu. If an object is being created, then the parent object level should be selected.

Using an XML editor, the XML schemas that are generated can now be used to create the corresponding XML instance documents to execute these operations. Each schema has an attributes section with the attributes that the entry can use at the level in the tree where the schema was created, and a set of attribute conditions that can be used to select entries similar to a database selection clause.

Service Adapter Run-Time Operations

This section describes service adapter run-time operations (Get, Update, Delete, Create, and Move). This section also provides examples of XML instance documents generated from the LDAP schemas and sent to the adapter.

Get

The Get method is used to retrieve LDAP information based on specified conditions.

```
<m:LdapRequest operation="get">
       <m:LdapEntry>
          <m:Name> </m:Name>
          <m:Parent>DC=iway</m:Parent>
          <m:LdapAttributes>
              <m:sn> </m:sn>
              <m:cn> </m:cn>
              <m:objectClass> </m:objectClass>
              <m:userPassword> </m:userPassword>
              <m:telephoneNumber> </m:telephoneNumber>
              <m:seeAlso> </m:seeAlso>
              <m:description> </m:description>
          </m:LdapAttributes>
```

```
            <m:LdapCondition>
                <m:sn>String</m:sn>
                <m:cn>String</m:cn>
                <m:objectClass>String</m:objectClass>
                <m:userPassword>String</m:userPassword>
                <m:telephoneNumber>String</m:telephoneNumber>
                <m:seeAlso>String</m:seeAlso>
                <m:description>String</m:description>
            </m:LdapCondition>
        </m:LdapEntry>
</m:LdapRequest>
```

The *LdapEntry* element is the base element, which represents the LDAP request element.

Note: The *Parent* node is mandatory and is used to determine the LDAP search context.

The *LdapAttributes* node is used to filter the attributes required in the result document. The result will contain only those attributes as indicated by the child node names of the *LdapAttribute* node. Information for the *LdapAttributes* node is optional. If this information does not exist, by default, the adapter will return all populated nodes.

The *LdapCondition* Node is used to specify the criteria for the Get method.

For example:

```
<cn>*</cn>
```

This returns all entries in the parent context that have a *cn* attribute.

```
<cn>lyer</cn>
<address>Toronto</address>
```

This returns all entries with a *cn* value of *lyer* and an *address* value of *Toronto*.

The response consists of a response header and a response body.

```
<LdapResponse>
       <LdapResultHeader>
         <Operation>get</Operation>
         <Status>Success</Status>
       </LdapResultHeader>
      <LdapResultBody>
         <LdapEntry>
          <Name>cn=Ganesh Iyer,dc=toronto,dc=iway</Name>
          <LdapAttributes>
            <postalcode>654736</postalcode>
            <description>I am Mr iyer</description>
            <objectclass>top,person,organizationalPerson,
             country,organizationalRole</objectclass>
            <postaladdress>Toronto5023 Perennial Drive
             Canada</postaladdress>
            <sn>Iyer</sn>
            <cn>Ganesh Iyer</cn>
            <c>test</c>
          </LdapAttributes>
         </LdapEntry>
      </LdapResultBody>
</LdapResponse>
```

The name is the fully qualified Distinguished Name (DN) of the retrieved entry.

Update

The Update method is used to update LDAP information based on specified conditions.

Note: Attributes having multiple values can be set using commas ",". For example:

```
<telephoneNumber>12345,456767,778888</telephoneNumber>
```

This will add three values to the *telephoneNumber* attribute.

```
<m:LdapRequest operation="update">
         <m:LdapEntry>
          <m:Name> </m:Name>
          <m:Parent>DC=iway</m:Parent>
          <m:LdapAttributes>
            <m:sn>newval1 </m:sn>
            <m:cn> newval2</m:cn>
            <m:userPassword> new password</m:userPassword>
            <m:telephoneNumber> 3456753</m:telephoneNumber>
            <m:description>Updated iway employee </m:description>
           </m:LdapAttributes>
              <m:LdapCondition>
                <m:cn>Ganesh Iyer</m:cn>
              </m:LdapCondition>
         </m:LdapEntry>
</m:LdapRequest>
```

The *LdapEntry* element is the base element, which represents the LDAP request element.

Note: The *Parent* node is mandatory and is used to determine the LDAP search context.

The *LdapAttributes* node is used to provide the attributes that need to be updated with updated values.

The *LdapCondition* node is used to specify the criteria for the Update operation.

For example:

```
<cn>lyer</cn>
<address>Toronto</address>
```

This returns all entries with a *cn* value of *lyer* and an *address* value of *Toronto*.

The response consists of a response header:

```
<LdapResponse>
        <LdapResultHeader>
           <Operation>update</Operation>
           <Status>Success</Status>
        </LdapResultHeader>
</LdapResponse>
```

Delete

The Delete method is used to delete LDAP information based on specified conditions.

```
<m:LdapRequest operation="delete">
       <m:LdapEntry>
         <m:Name> </m:Name>
         <m:Parent>DC=iway</m:Parent>
          <m:LdapCondition>
            <m:cn>Ganesh Iyer</m:cn>
          </m:LdapCondition>
       </m:LdapEntry>
</m:LdapRequest>
```

The *LdapEntry* element is the base element, which represents the LDAP request element.

Note: The *Parent* node is mandatory and is used to determine the LDAP search context.

The *LdapCondition* node is used to specify the criteria for the Update operation.

For example:

```
<cn>Ganesh lyer</cn>
```

This deletes all entries in the parent context which have a *cn* attribute of *Ganesh lyer*.

```
<cn>lyer</cn>
<address>Toronto</address>
```

This deletes all entries with a *cn* value of *lyer* and an *address* value of *Toronto*.

The response consists of a response header:

```
<LdapResponse>
        <LdapResultHeader>
           <Operation>delete</Operation>
           <Status>Success</Status>
        </LdapResultHeader>
</LdapResponse>
```

Create

The Create method is used to create an LDAP entry in the directory:

```
<m:LdapRequest operation="create">
        <m:LdapEntry>
         <m:Name>CN=Ganesh Iyer  </m:Name>
         <m:Parent>dc=Toronto, dc=iway</m:Parent>
         <m:LdapAttributes>
           <m:sn>newval1 </m:sn>
           <m:cn> newval2</m:cn>
           <m:userPassword> new password</m:userPassword>
           <m:telephoneNumber> 3456753</m:telephoneNumber>
           <m:description>Updated iway employee </m:description>
         </m:LdapAttributes>
        </m:LdapEntry>
</m:LdapRequest>
```

The *LdapEntry* element is the base element, which represents the LDAP request element.

Note: The *Parent* node is mandatory and is used to determine the LDAP search context.

The *LdapAttributes* node is used to provide the attributes that need to be created.

The response consists of a response header:

```
<LdapResponse>
        <LdapResultHeader>
           <Operation>create</Operation>
           <Status>Success</Status>
        </LdapResultHeader>
</LdapResponse>
```

Move

The Move method is used to move an object within the tree (subject to permissions).

The following is an example of a move operation:

```
<iwldap:LdapRequest operation="move"
xsi:schemaLocation="urn:iwaysoftware:adapter:iwldap:CN=iws3,CN=Computers,DC=
aethni,DC=ibi,DC=com file:///G:/workspace/ldap/Schemas/CN=iws3_request.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:iwldap="urn:iwaysoftware:adapter:iwldap:CN=iws3,CN=Computers,DC=aethni
,DC=ibi,DC=com">
        <iwldap:LdapEntry>
           <Operation>create</Operation>
           <Status>Success</Status>
        </LdapResultHeader>
</LdapResponse>

<iwldap:LdapRequest operation="move"
xsi:schemaLocation="urn:iwaysoftware:adapter:iwldap:CN=iws3,CN=Computers,
DC=aethni,DC=ibi,DC=com file:///G:/workspace/ldap/Schemas/
CN=iws3_request.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:iwldap="urn:iwaysoftware:adapter:iwldap:CN=iws3,CN=Computers,DC=aet
hni,DC=ibi,DC=com">
        <iwldap:LdapEntry>
                <iwldap:Name>CN=iws3,CN=Computers,DC=aethni,DC=ibi,DC=com
                </iwldap:Name>
                <iwldap:Parent>CN=Computers,DC=aethni,DC=ibi,DC=com
                </iwldap:Parent>
                <iwldap:NewParent>CN=Branch office,DC=aethni,DC=ibi,DC=com
                </iwldap:NewParent>
```

Working With LDAP Action Dialogs

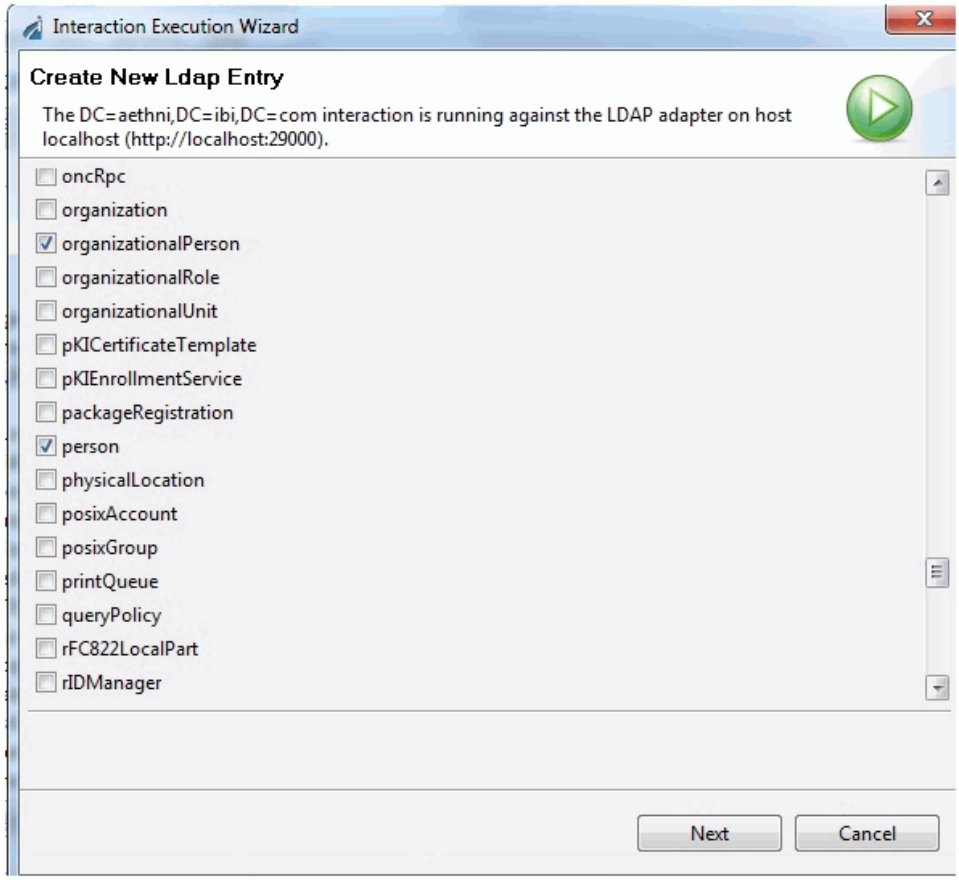
iWay Explorer allows you to introspect LDAP entries, generate XML schemas, and WSDL files for specific LDAP entries. In addition, iWay Explorer provides interactive dialogs for all LDAP operations, depending on the permission level of the user.

Creating New LDAP Entries

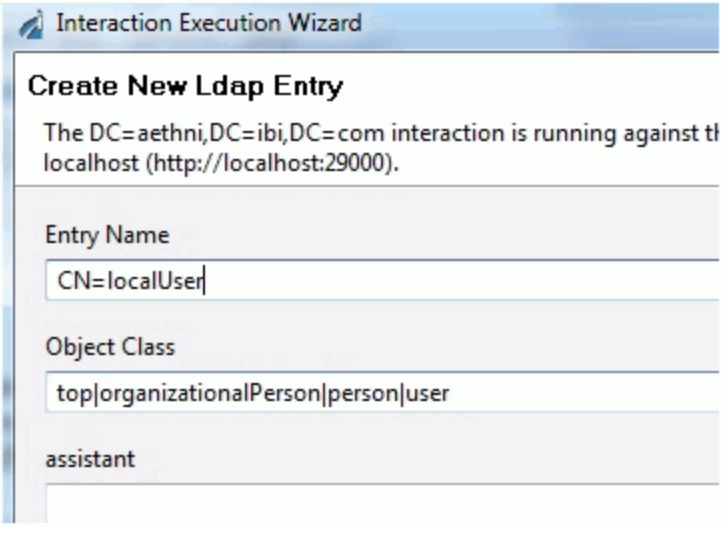
You can use this action to create a new LDAP entry.

Right-click an LDAP entry in the left pane and select *Create New Ldap Entry* from the context menu.

The Create New Ldap Entry dialog displays a list of objects available for creation at the selected entry level, as shown in the following image.



Select the desired objects and click *Next*. An interactive dialog with the available attributes is displayed, as shown in the following image.



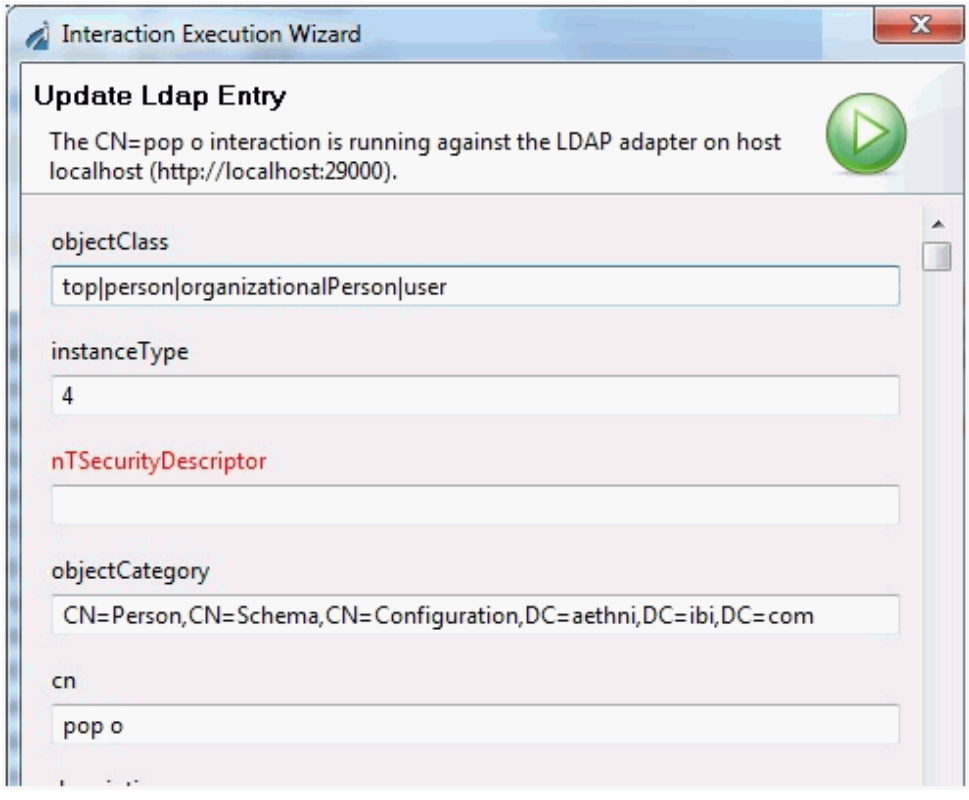
Provide values for the fields that correspond to the new LDAP entry and click *Create*.

Updating LDAP Entries

You can use this action to update a selected LDAP entry.

Right-click an LDAP entry in the left pane and select *Update Ldap Entry* from the context menu.

The Update Ldap Entry dialog opens, as shown in the following image.



Provide updated values for the fields that correspond to the LDAP entry and click *Update*.

Note: Some entries cannot be changed, such as the name or object class.

See *Understanding Active Directory Error Messages* on page 105 for Active Directory error codes, or RFC-4511 of the Internet Engineering Task Force, for more information on Active Directory or LDAP server error codes.

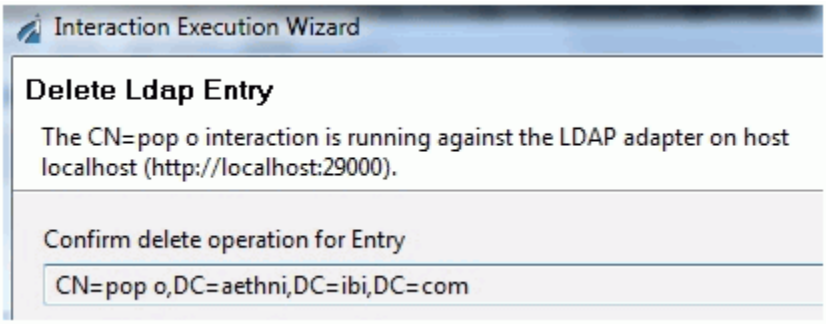
Deleting LDAP Entries

You can use this action to delete a selected LDAP entry.

Note: There is no undo option for the delete operation.

Right-click an LDAP entry in the left pane and select *Delete Ldap Entry* from the context menu.

The Delete Ldap Entry dialog opens, as shown in the following image.



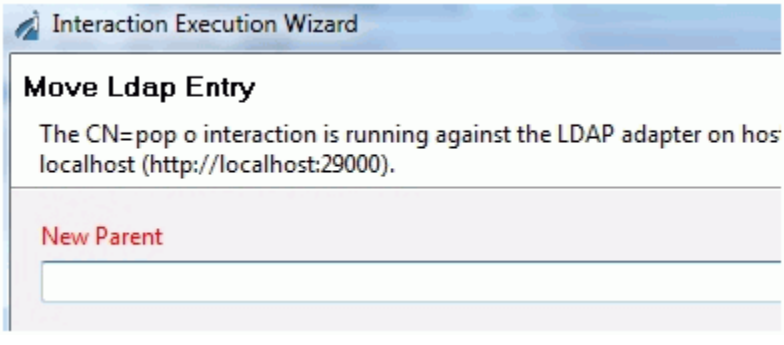
Click *Delete* to confirm the delete action.

Moving LDAP Entries

You can use this action to move a selected LDAP entry.

Right-click an LDAP entry in the left pane and select *Move Ldap Entry* from the context menu.

The Move Ldap Entry dialog opens, as shown in the following image.



Enter the new parent destination to move the selected LDAP entry.

Schema Location

By default, iWay Explorer stores the schemas it creates in subdirectories under the iWay home directory of the machine on which it is installed. However, using iWay Explorer, you can also export these schemas to any location that you specify on your file system.

The exact location of the schemas differs, depending on whether you deploy iWay Explorer with an iBSP.

When the adapter is used with an iBSP configuration, iWay Explorer stores the schemas in a subdirectory of the iWay installation directory, for example,

iWayHome`\config\base\wsdl\schemas\service\LDAP\`*LDAP_Target*

where:

LDAP_Target

Is the name of the connection (target) to the LDAP system that you defined using iWay Explorer. Under this directory, iWay Explorer creates subdirectories containing schemas.

Procedure: How to Generate a Schema for an LDAP Entry

To generate a schema for an LDAP entry using iWay Explorer:

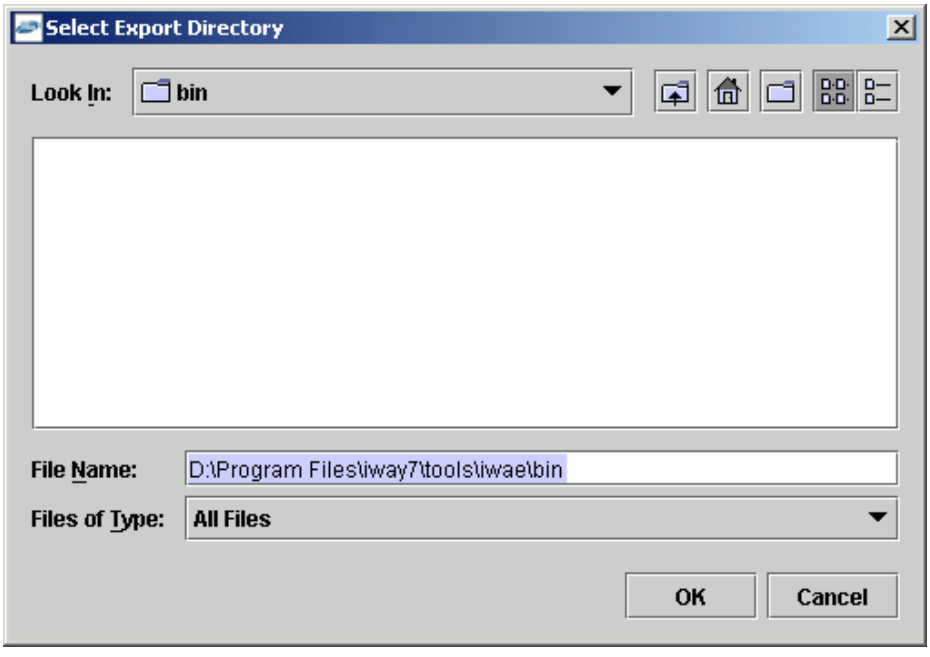
1. Connect to an LDAP target, as described in *Configuring and Managing Connections to an LDAP Server* on page 27.
2. Expand an available node.
3. Select a method under the expanded node.

   The XML request and response schemas are automatically generated for this method by iWay Explorer.
4. Click the *Request Schema* tab in the right pane.

   The XML request schema appears in the right pane.
5. Click the *Response Schema* tab in the right pane.

   The XML response schema appears in the right pane.
6. To export XML schemas, right-click a method in the left pane, and select *Export Schema(s)*.

The Select Export Directory dialog opens, as shown in the following image.



7. Navigate to a directory on your file system where you want to export the XML schemas.

   The file path is displayed in the File Name field.

8. Click *OK*.

   The XML request and response schemas are now exported to your local file system.

Chapter 7

Creating and Publishing iWay Business Services

This section describes how to create and publish iWay Business Services using iWay Explorer.

In this chapter:

- Understanding iWay Business Services
- Creating iWay Business Services

Understanding iWay Business Services

iWay Explorer provides web developers with a simple, consistent mechanism for extending the capabilities of the iWay Application Protocol Adapter for LDAP. The iWay Business Services Provider (iBSP) exposes functionality as web services. It serves as a gateway to heterogeneous back-end applications and databases.

A web service is a self-contained, modularized function that you can publish and access across a network using open standards. It is the implementation of an interface by a component and is an executable entity. For the caller or sender, a web service can be considered as a "black box" that may require input and delivers a result. Web services integrate within an enterprise as well as across enterprises on any communication technology stack, whether asynchronous or synchronous, in any format.

After you browse LDAP entries and create an XML schema, you can generate an iWay Business Service for the LDAP entry you wish to use with your adapter.

Naming Considerations

When you create a web service, iWay Explorer automatically uses the selected entry as the method name, since all methods can be called from the entry. This creates a conflict because these method names are not compatible in XML documents and issues with web clients can occur. It is a strongly recommended that all special characters (such as commas (,) equal signs (=), and so on) be removed from the name as the service is created.

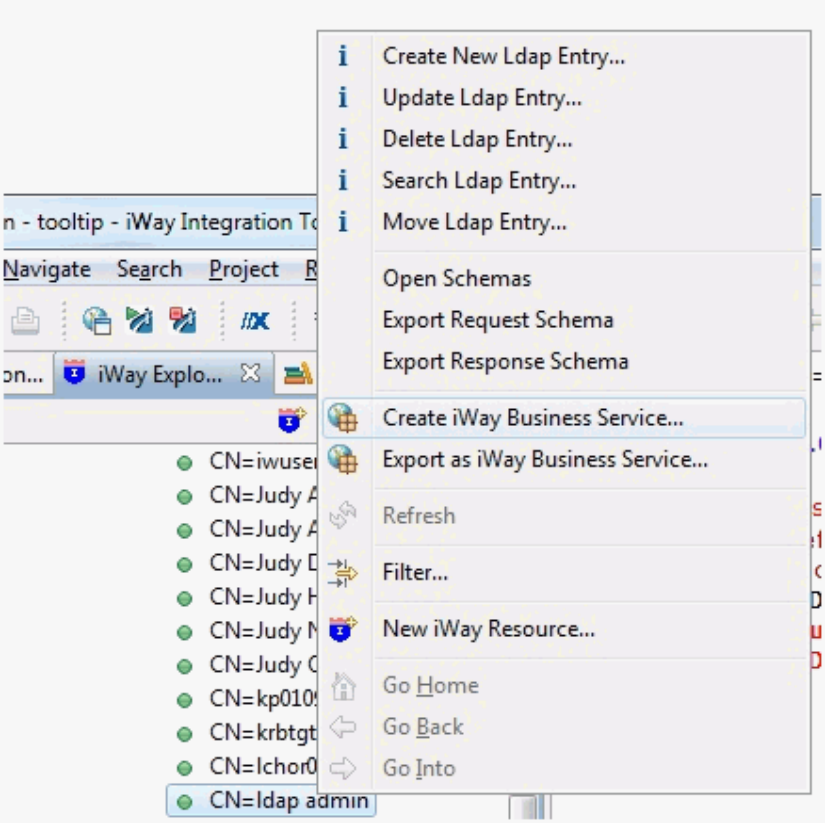
Creating iWay Business Services

This section describes how to create iWay Business Services.

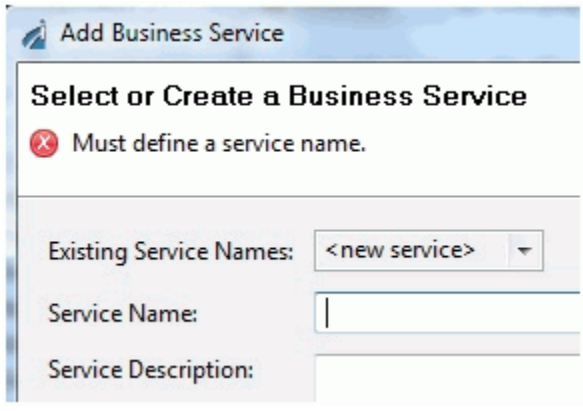
Procedure: How to Create iWay Business Services

To create iWay Business Services:

1. Connect to an LDAP target, as described in *Configuring and Managing Connections to an LDAP Server* on page 27.
2. In the left pane, expand the target node.
3. Locate and select an LDAP entry.
4. Right-click the method for the entry and select *Create iWay Business Service* from the context menu, as shown in the following image:



The Add Business Service dialog box opens, as shown in the following image.



Note: A service can contain multiple methods.

5. Perform the following steps:

   a. From the Existing Service Names drop-down list, select whether you want to create a new service name or use an existing service name. By default, *<new service>* is selected.

   b. In the Service Name field, type a descriptive name for the iWay Business Service.

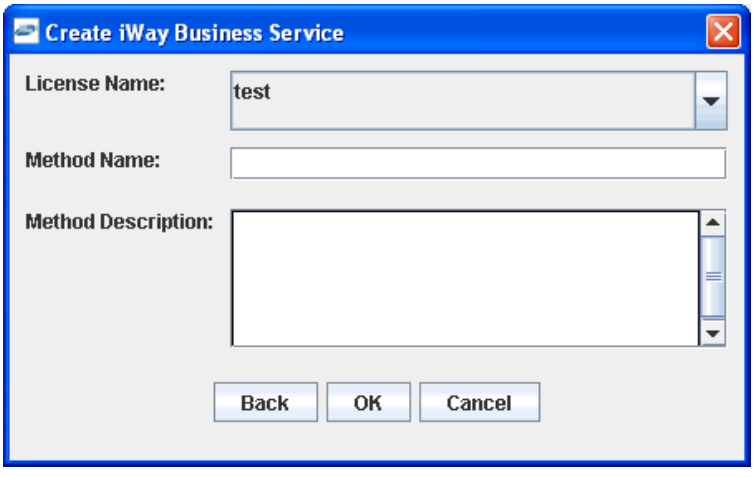
      For example:

      Note: Service names are case-sensitive and should not start with a number or a special character.

   c. In the Service Description field, type a brief description of the service (optional).

6. Click *Next*.

A second Create iWay Business Service dialog box opens and prompts you for additional information.

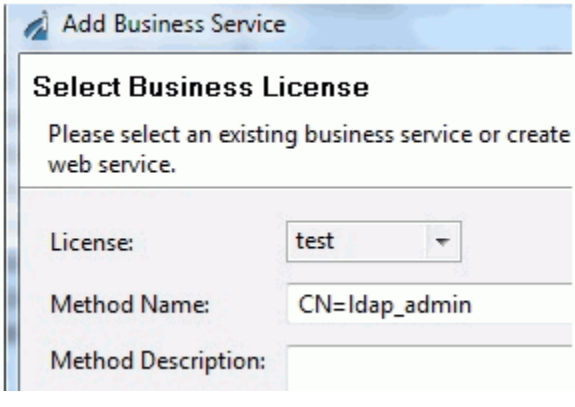


7. Perform the following steps:

   a. From the License Name drop-down list, select a license definition. By default, *test* is selected.

   b. In the Method Name field, type a descriptive name for the method. The name of the method you selected earlier is used as a default value for this field.

      The following image is an example of the default value based on the method you previously selected:

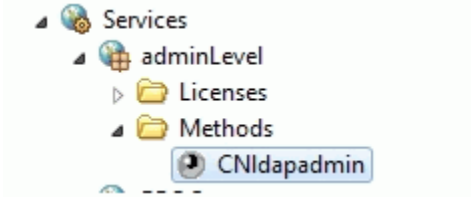


Remove all special characters and change the method name, as shown in the following example:

c. In the Method Description field, type a brief description of the method (optional).

8. Click *OK*.

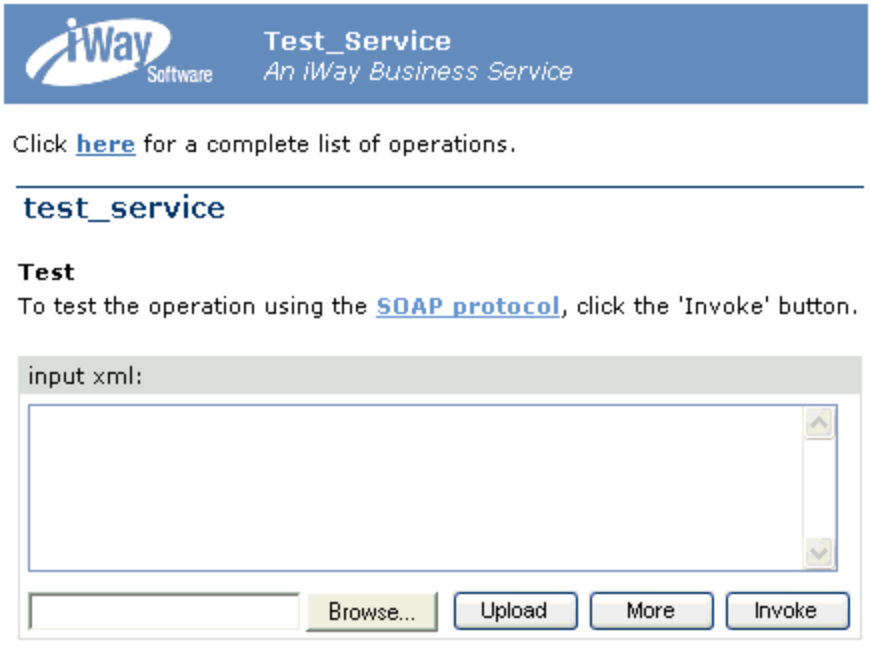
The iWay Business Services node expands in the left pane. The new iWay Business Service appears under the Services node, as shown in the following example:



The right pane displays the name of the expanded iWay Business Service and provides a hyperlink to the selected method.

9. Click the hyperlink for your service in the right pane.

An iWay Business Service test pane opens in a new window of your web browser, as shown in the following image.



10. Enter a sample XML input request document in the input area.
11. Click *Invoke*.

    The test response appears in the web browser.

Chapter 8

Configuring Events for LDAP

This section describes how to create ports and channels to extract events from an LDAP directory using iWay Explorer.

In this chapter:

- LDAP Event Handling Overview
- Creating an Event Port
- Creating a Channel

LDAP Event Handling Overview

Events are generated as a result of activity on an application system. You can use events to trigger an action in your application.

The iWay Application Protocol Adapter for LDAP supports event handling through the LDAP implementation of outbound messages. To create an iWay event, you must create a port and a channel using iWay Explorer. The following is a description of how ports and channels work.

- **Port.** A port associates a particular business object exposed by an adapter with a particular disposition. A disposition defines the protocol and location of the event data. The port defines the end point of the event consumption. For more information, see *Creating an Event Port* on page 75.
- **Channel.** A channel represents configured connections to particular instances of back-end or other types of systems. A channel binds one or more event ports to a particular listener managed by an adapter. For more information, see *Creating a Channel* on page 87.

Creating an Event Port

The following procedures describe how to create an event port using iWay Explorer.

When you use iWay Explorer with an iWay Business Services Provider (iBSP) implementation, the following port dispositions are available:

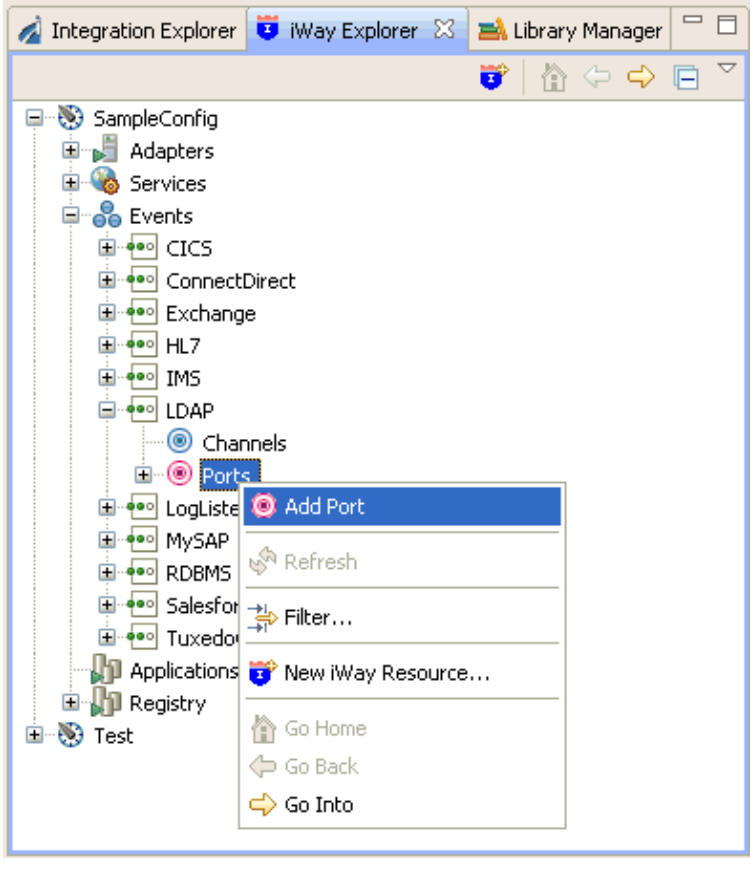
- **File.** The File disposition uses a file URL to specify the destination file name or directory where the event document will be written. During run time, the destination file name may require indexing to avoid overwriting.

- **iBSP.** The iBSP disposition enables an event to launch a business service method.
- **MSMQ.** The Microsoft Message Queue disposition supports public and private queues.
- **JMSQ.** The JMSQ disposition allows an event to be enqueued to a JMS queue.
- **SOAP.** The SOAP disposition allows an event to launch a business service specified by a WSDL file. A SOAP action is optional; "" is the default value.
- **HTTP.** The HTTP disposition uses an HTTP URL to specify an HTTP end point to which the event document is posted.
- **MQSeries.** The MQSeries disposition enables an event to be enqueued to an MQSeries queue. Both queue manager and queue name may be specified.

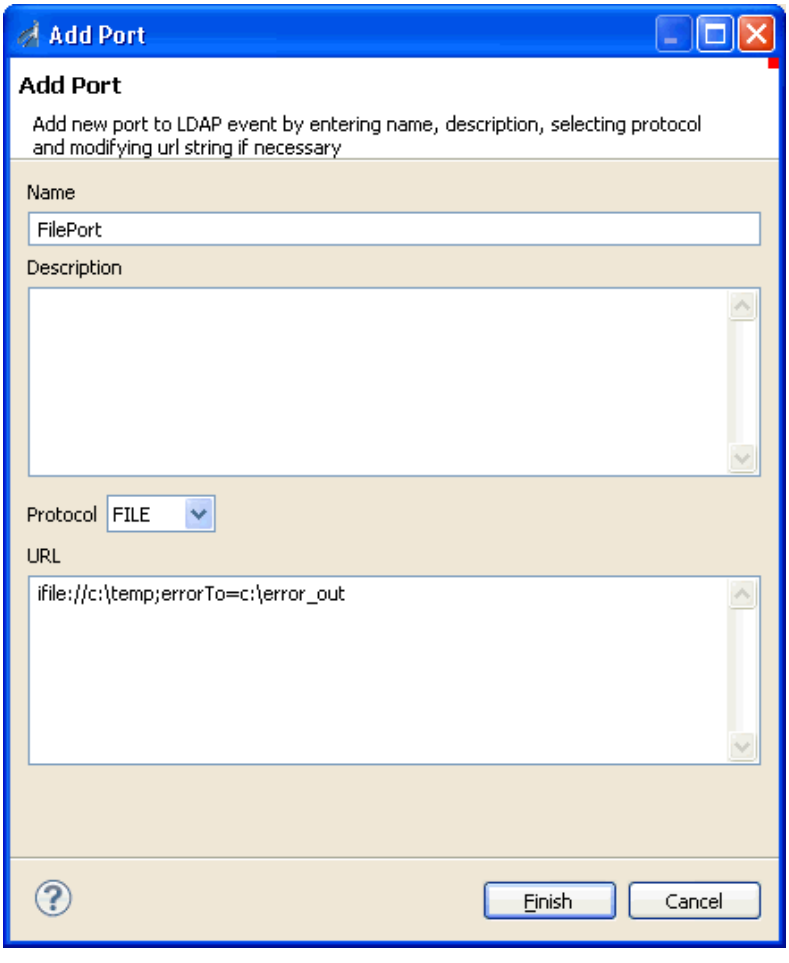
Procedure: How to Create a Port for the File Disposition

1. Connect to the Events node in iWay Explorer and expand the *LDAP* node.

2. Right-click the *Ports* node, and click *Add Port* from the menu.



The following image shows the Add Port dialog box where you can supply information about the port.



a. In the Name field, type a name for the port.

b. In the Description field, optionally type a brief description.

c. From the Protocol drop-down list, select *FILE*.

d. In the URL field, type a File destination to which event data is written.

When pointing the Events node in iWay Explorer to an iBSP deployment, specify the File destination using the following format:

```
ifile://[location];errorTo=[pre-defined port name or another
disposition url]
```

The following table describes the parameters for the File disposition.

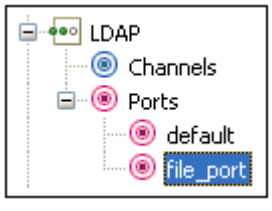
Parameter	Description
location	Destination and file name of the document where event data is written.
errorTo	Predefined port name or another disposition URL where error logs are sent. Optional.

For example:

```
ifile://D:\in\x.txt;errorTo=ifile://D:\error
```

3. Click *Finish* when you have supplied the values on the Add Port dialog box.

   The following image shows the port that you added, which appears beneath the Ports node in the Events area of iWay Explorer. In this example, the port is named file_port.



Procedure: How to Create a Port for the IBSE Disposition

1. Connect to the Events node in iWay Explorer and expand the *LDAP* node.
2. Right-click the *Ports* node, and click *Add Port* from the menu.

   The Add Port dialog box opens.
3. Supply the values for the fields on the dialog box as follows.
   a. In the Name field, type a name for the port.
   b. In the Description field, optionally type a brief description.
   c. From the Protocol drop-down list, select *IBSE*.
   d. In the URL field, type an iBSE destination using the following format:

   ```
   ibse:[svcName].[mthName];responseTo=[pre-defined port name or
   another disposition url];errorTo=[pre-defined port name or another
   disposition url]
   ```

The following table describes the parameters for the IBSE disposition.

Parameter	Description
svcName	Name of the business service created with iBSE.
mthName	Name of the method created for the business service.
responseTo	Location where responses to the business service are posted. Predefined port name or another full URL. Optional.
errorTo	Location where error documents are sent. Predefined port name or another full URL. Optional.

4. Click *Finish* when you have supplied the values on the Add Port dialog box.

   The port that you added is displayed beneath the Ports node.

Procedure: How to Create a Port for the MSMQ Disposition

1. Connect to the Events node in iWay Explorer and expand the *LDAP* node.
2. Right-click the *Ports* node, and click *Add Port* from the menu.

   The Add Port dialog box opens.
3. Supply the values for the fields on the dialog box as follows.
   a. In the Name field, type a name for the port.
   b. In the Description field, optionally type a brief description.
   c. From the Protocol drop-down list, select *MSMQ*.
   d. In the URL field, type an MSMQ destination in the following format:

```
msmq://[machineName]/private$/[qName];errorTo=[pre-defined port
name or another disposition url]
```

   The following table describes the parameters for the MSMQ disposition.

Parameter	Description
machineName	Name of the machine on which the Microsoft Message Queuing system is running.

Parameter	Description
queue type	For private queues, type *Private$*. Private queues are queues that are not published in the Active Directory. They appear only on the local computer that contains them. Private queues are accessible only by Microsoft Message Queuing applications that recognize the full path name or format name of the queue.
qName	Name of the private queue where messages are placed.
errorTo	Location where error documents are sent. Predefined port name or another full URL. Optional.

4. Click *Finish* when you have supplied the values on the Add Port dialog box.

   The port that you added is displayed beneath the Ports node.

Procedure: How to Create a Port for the JMSQ Disposition

1. Connect to the Events node in iWay Explorer and expand the *LDAP* node.
2. Right-click the *Ports* node, and click *Add Port* from the menu.

   The Add Port dialog box opens.
3. Supply the values for the fields on the dialog box as follows.
   a. In the Name field, type a name for the port.
   b. In the Description field, optionally type a brief description.
   c. From the Protocol drop-down list, select *JMSQ*.
   d. In the URL field, type a Java Message Service (JMS) destination.

      When pointing the Events node in iWay Explorer to an iBSP deployment, use the following format:

```
jmsq:[myQueueName]@[myQueueFac];jndiurl=[myurl];jndifactory=
[myfactory];user=[user];password=[xxx];errorTo=[pre-defined port
name or another disposition url]
```

      The following table describes the parameters for the JMSQ disposition.

Parameter	Description
myQueueName or jmsqueue	Name of a queue to which events are emitted.

Parameter	Description
myQueueFac or jmsfactory	A resource that contains information about the JMS Server.
jndiurl	The URL used to contact the JNDI provider. The syntax of this URL depends on the JNDI provider that is used. This value corresponds to the following standard JNDI property: `java.naming.provider.url`
jndifactory	Is JNDI context.INITIAL_CONTEXT_FACTORY, which is provided by the JNDI service provider.
user	User ID associated with this queue.
password	Password for the user ID.
errorTo	Location where error logs are sent. Optional. Predefined port name or another disposition URL. The URL must be complete, including the protocol.

4. Click *Finish* when you have supplied the values on the Add Port dialog box.

   The port that you added is displayed beneath the Ports node.

Procedure: How to Create a Port for the SOAP Disposition

1. Connect to the Events node in iWay Explorer and expand the *LDAP* node.
2. Right-click the *Ports* node, and click *Add Port* from the menu.

   The Add Port dialog box opens.
3. Supply the values for the fields on the dialog box as follows.
   a. In the Name field, type a name for the port.
   b. In the Description field, optionally type a brief description.
   c. From the Protocol drop-down list, select *SOAP*.
   d. In the URL field, type a SOAP destination, using the following format:

```
soap:[wsdl-url];soapaction=[myaction];method=[web service
method];namespace=[namespace];responseTo=[pre-defined port name or
another disposition url];errorTo=[pre-defined port name or another
disposition url]
```

The following table describes the parameters for the SOAP disposition.

Parameter	Description
wsdl-url	The URL to the WSDL file that is required to create the SOAP message, for example, `http://localhost:7001/ibsp/IBSPServlet/test/webservice.ibs?wsdl` where: *webservice* Is the name of the web service that you created using Business Service Explorer. To find this value, navigate to the Business Service Explorer node and open the *Service Description* hyperlink in a new window. The WSDL URL appears in the Address field. You can also open the WSDL file in a third-party XML editor (for example, Altova XMLSpy®) and view the SOAP request settings to find this value.
soapaction	The method called by the SOAP disposition, for example, *webservice.method@test@@* where: *webservice* Is the name of the web service that you created using Business Service Explorer. *method* Is the method being used. *test* Is the license that is being used by the web service. To find this value, navigate to the Business Service Explorer node and open the *Service Description* hyperlink in a new window. Perform a search for *soapAction*.

Parameter	Description
method	The web service method that you are using. You can find this value in the WSDL file.
namespace	The XML namespace that you are using. You can find this value in the WSDL file.
responseTo	The location to which responses are posted, which can be a predefined port name or another URL. Optional.
errorTo	The location to which error logs are posted, which can be a predefined port name or another URL. Optional.

4. Click *Finish* when you have supplied the values on the Add Port dialog box.

   The port that you added is displayed beneath the Ports node.

Procedure: How to Create a Port for the HTTP Disposition With an IBSP Deployment

1. Connect to the Events node in iWay Explorer and expand the *LDAP* node.
2. Right-click the *Ports* node, and click *Add Port* from the menu.

   The Add Port dialog box opens.
3. Supply the values for the fields on the dialog box as follows.
   a. In the Name field, type a name for the port.
   b. In the Description field, optionally type a brief description.
   c. From the Protocol drop-down list, select *HTTP*.
   d. In the URL field, type an HTTP destination, using the following format

   ```
   http://[myurl];responseTo=[pre-defined port name or another
   disposition url]
   ```

   where:

   `myurl`

   Is the URL target for the post operation, for example,

   `http://myhost:1234/docroot`

   `responseTo`

   Is the location to which responses are posted, if desired.

4. Click *Finish* when you have supplied the values on the Add Port dialog box.

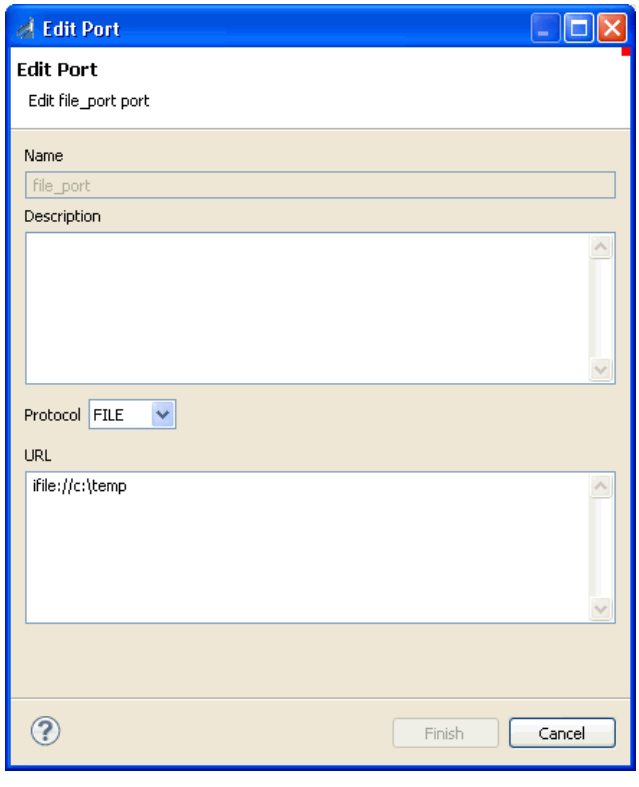
   The port that you added is displayed beneath the Ports node.

Procedure: How to Edit a Port

After you create a port, you can edit the information that you provided during the creation procedure.

1. Expand the *Ports* node in the Events area of iWay Explorer to locate the name of the port that you want to edit, for example, *file_port*.
2. Right-click the port, and click *Edit* from the menu.

   The Edit Port dialog box opens. It displays the values that you supplied when you created the port.



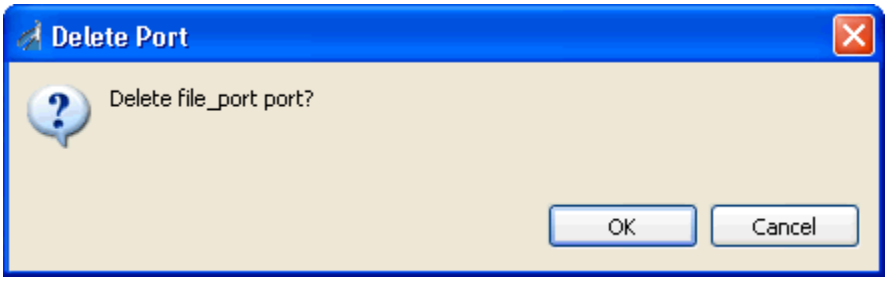
3. Use the fields on the dialog box to modify the properties as desired. You cannot change the name of the port.
4. Click *Finish* when you have completed your edits.

The modified properties are applied to the port.

Procedure: How to Delete a Port

1. Expand the *Ports* node in the Events area of iWay Explorer to locate the name of the port that you want to delete, for example, *file_port*.
2. Right-click the port, and click *Delete* from the menu.

   iWay Explorer displays a prompt, asking you to confirm the deletion of the selected port, as shown in the following image.



3. Click *OK* to proceed with the deletion.

Using the Default Port

When using iWay Explorer to connect to an application system and listen for events, a default port is available.

You can use the default port for testing purposes or when you do not want to route event data to a specific port that you have configured. The default port is enabled when you start a channel that does not have a specific port assigned to it.

The default event data is a file disposition that writes to an out.xml file in the following output directory:

```
ifile://./eventOut/out.xml
```

Procedure: How to Modify the Default Port Output Directory

1. In the ibse\WEB-INF\lib directory, open the ibse.jar file, and locate the dispositioninfo.xml file.
2. Using a text editor, locate the following lines in the dispositioninfo.xml file:

```
<?xml version="1.0" encoding="UTF-8"?>
<dispositioninfo pref="built-in" defaultPortURL="ifile://./eventOut/
out.xml">
```

3. Change the default output directory to a new location of your choice.

   You can also change the name and type of the default output file.

4. Save your changes, and redeploy iBSP.

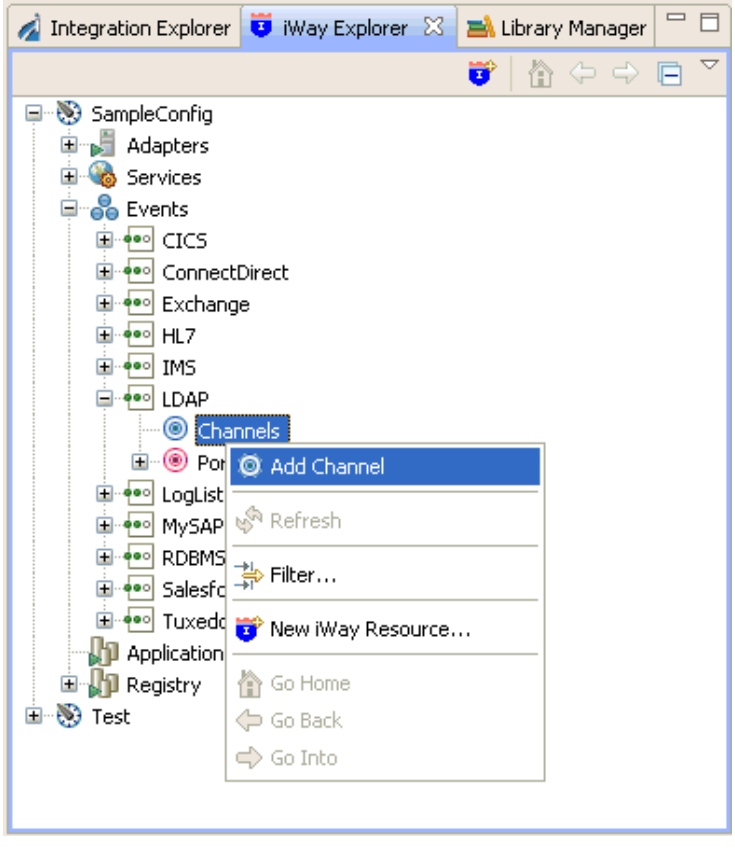
Creating a Channel

A channel binds a port to a listener managed by iWay Application Protocol Adapter for LDAP. A defined port must be associated with a channel in order for you to listen for events that take place in an LDAP system.

The procedures in this topic describe how to create, edit, or delete a channel using the Events node in iWay Explorer.

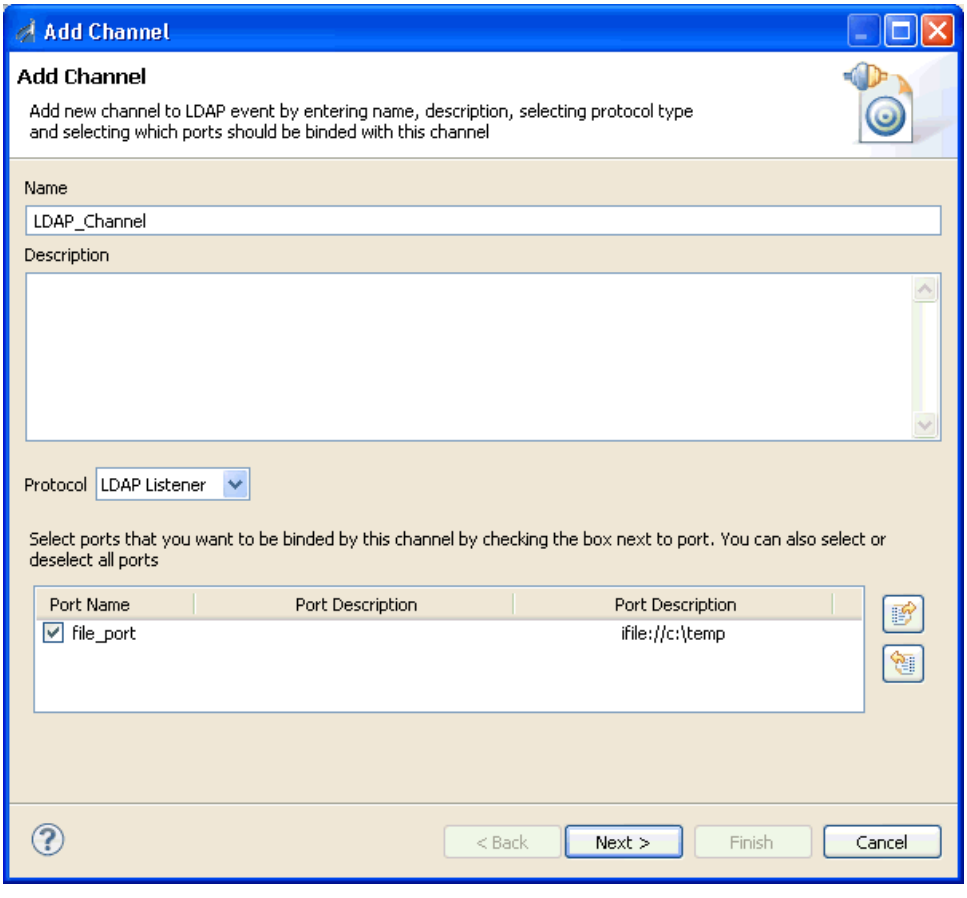
Procedure: How to Create a Channel

1. Connect to the Events node in iWay Explorer and expand the *LDAP* node.



2. Right-click the *Channels* node, and click *Add Channel* from the menu.

   The following image shows the Add Channel dialog box that opens, where you supply information about the channel.



   a. In the Name field, type a name for the channel, for example, LDAP_Channel.

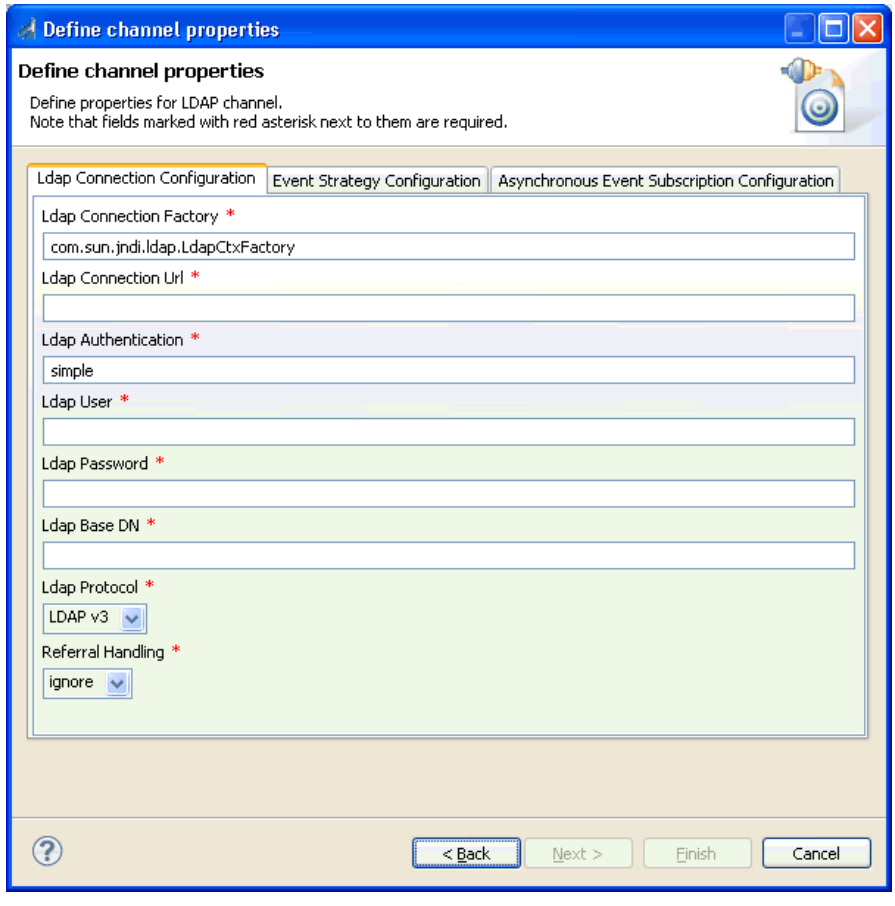
   b. In the Description field, optionally type a brief description (optional).

   c. From the Protocol drop-down list, select *LDAP Listener*.

   d. Under Port Name, select the check box for each port that this channel will bind to the listener.

3. Click *Next*.

The Define channel properties dialog box opens, as shown in the following image.



The following tabs are available:

- **Ldap Connection Configuration tab**

  For more information, see *Configuring the Ldap Connection Configuration Tab* on page 93.

- **Event Strategy Configuration tab**

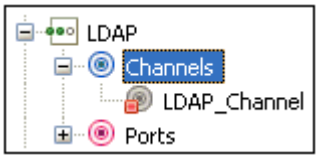
  For more information, see *Configuring the Event Strategy Configuration Tab* on page 96.

- **Asynchronous Event Subscription Configuration tab**

  For more information, see *Configuring the Asynchronous Event Subscription Configuration Tab* on page 98.

4. Click *Finish* when you are done.

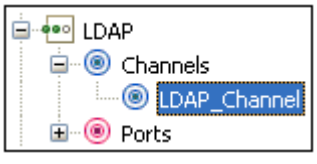
   The following image shows the channel that you added, which appears beneath the Channels node in the Events area of iWay Explorer. In this example, the channel is named LDAP_Channel.



   You are ready to start the channel to listen for events.

5. Right-click the channel, for example, *LDAP_Channel*, and click *Start* from the menu.

   The channel is now active and will listen for events on the LDAP system based on the configuration settings that were specified for the channel.



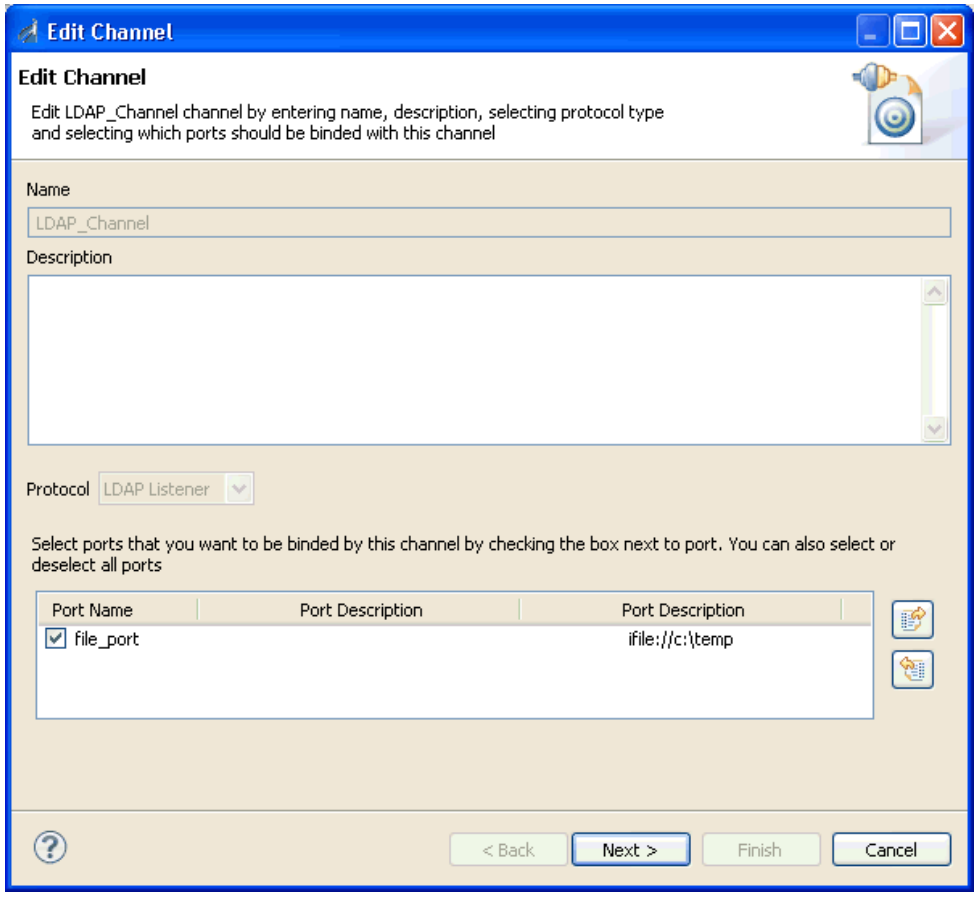
6. To stop the channel at any time, right-click the channel, and click *Stop* from the menu.

Procedure: How to Edit a Channel

After you create a channel, you can edit the information that you provided during the creation procedure.

1. In the Events node of iWay Explorer, locate the name of the channel that you want to edit, for example, *LDAP_Channel*.
2. Right-click the channel, and click *Edit* from the menu.

The Edit Channel dialog box opens. It displays the values that you supplied when you created the channel.



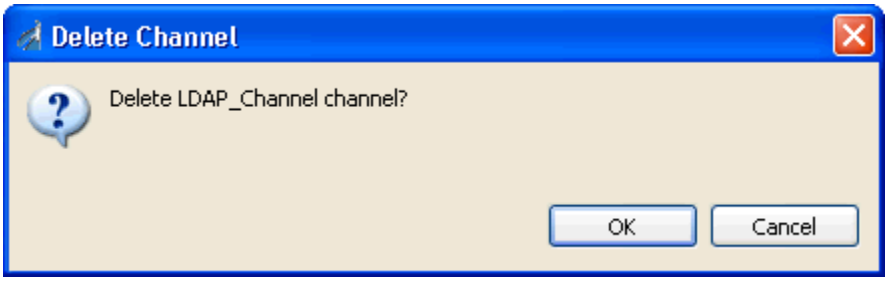
3. Use the fields on the dialog box to modify the properties as desired. You cannot change the name of the channel or its protocol.
4. Click *Next* on the Edit Channel dialog box to open the Define Channel Properties dialog box.
5. Use the tabs and fields on this dialog box to modify the properties as desired.
6. Click *Finish* on the Define Channel Properties dialog box when you have made your edits.

   The modified properties are applied to the channel.

Procedure: How to Delete a Channel

1. Expand the *Channels* node in the Events area of iWay Explorer to locate the name of the channel that you want to delete, for example, *LDAP_Channel*.
2. Right-click the channel, and click *Delete* from the menu.

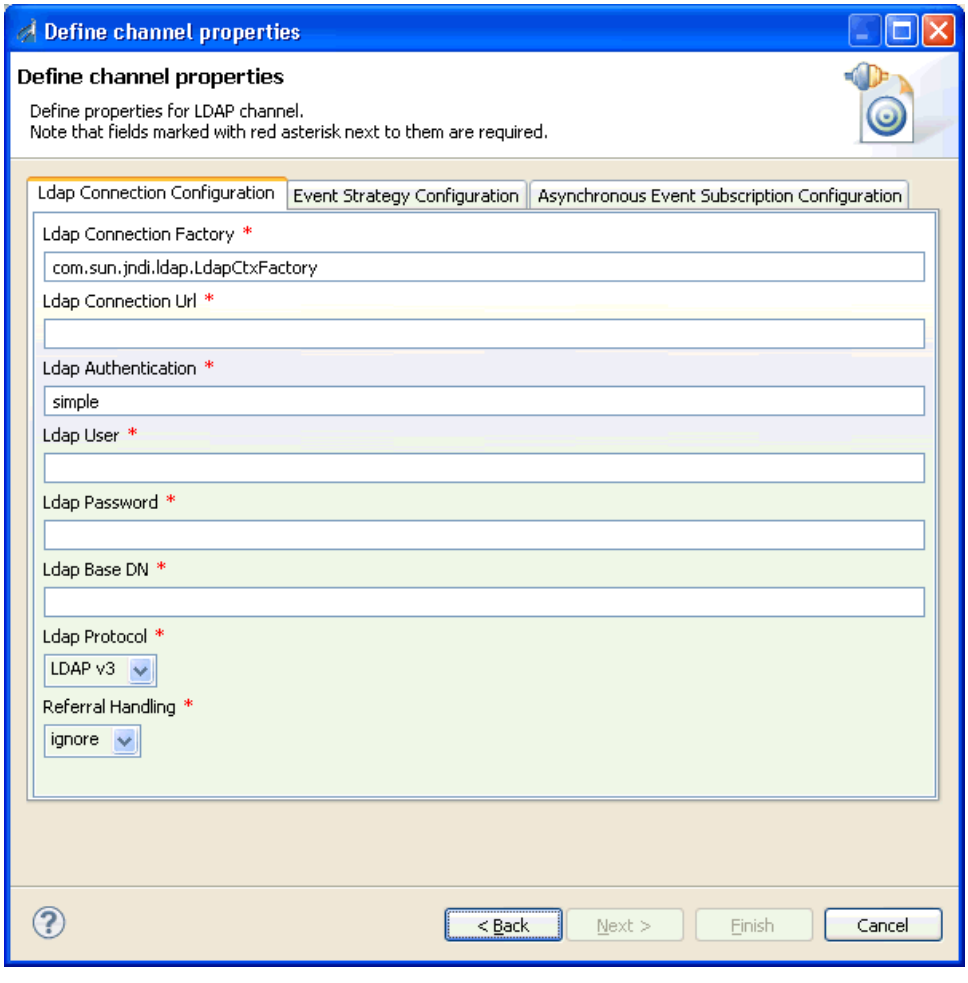
   iWay Explorer displays a prompt, asking you to confirm the deletion of the selected channel, as shown in the following image.



3. Click *OK* to proceed with the deletion.

Configuring the Ldap Connection Configuration Tab

This section describes how to configure the Ldap Connection Configuration tab during the channel configuration process, which is shown in the following image.



The parameters available in the Ldap Connection Configuration tab are listed and described in the following table:

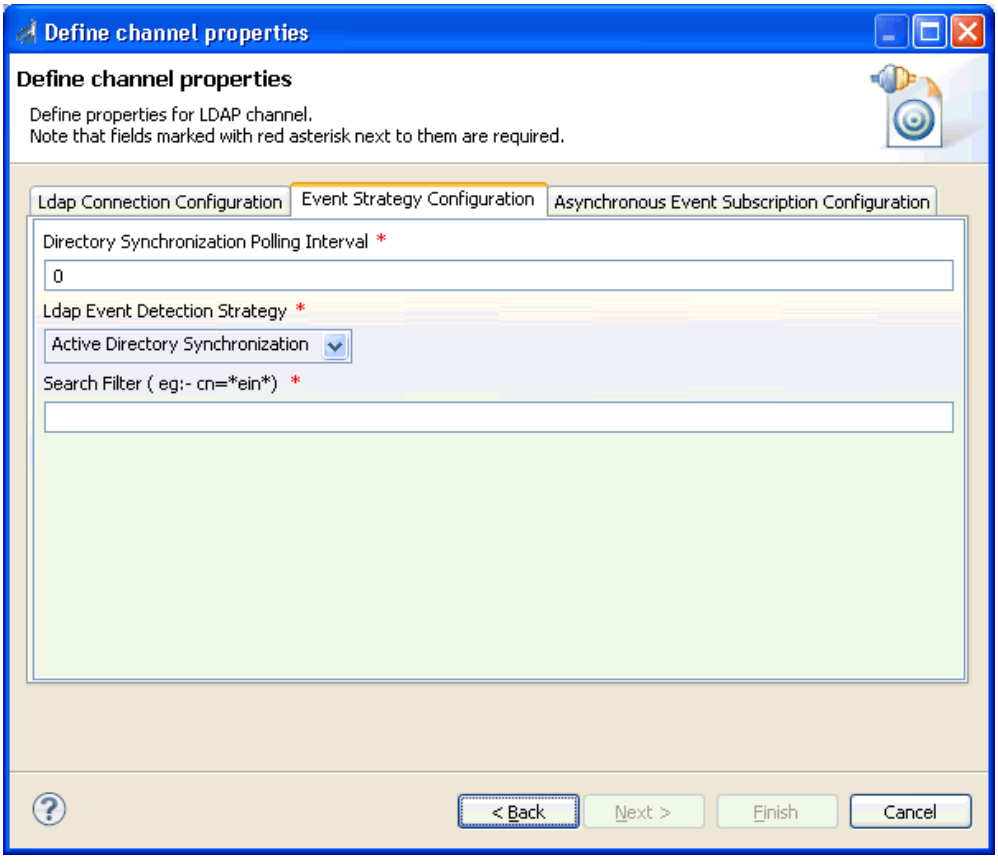
Parameter	Description
Ldap Connection Factory	The connection factory class that is used to access the LDAP server. The default connection factory implementation is com.sun.jndi.ldap.LdapCtxFactory, as provided by Java SDK.

Ldap Connection Url	The connection URL that is used to identify the LDAP server and connection context. This URL can use the following formats:
	❑ For unsecured access:
	`LDAP://machinename.network:portnumber`
	where:
	machinename
	Is the name of the system hosting the LDAP server.
	network
	Is the network of the LDAP server (such as *mycompany.com*).
	portnumber
	Is the port number of the LDAP server.
	❑ For secured access:
	`LDAPS://machinename.network:sslportnumber`
	where:
	machinename
	Is the name of the system hosting the LDAPS Directory Server.
	network
	Is the network of the LDAPS Directory Server (such as *mycompany.com*).
	sslportnumber
	Is the SSL port number of the LDAPS Directory Server.

Parameter	Description
Ldap Authentication	The authentication mechanism that is used to connect to the LDAP server. Currently, the adapter supports User ID and Password authentication of the *simple* bind standard.
Ldap User	The user password used that is used to access the LDAP server.
Ldap Password	A valid password that is associated with the user name.
Ldap Base DN	The relative entry point of the LDAP tree. If this field is empty, then the root DN is used.
Ldap Protocol	Currently, the adapter supports LDAP version 2 and LDAP version 3, as per target server requirements. Select one of the following LDAP versions from the drop down list: ❑ LDAP v3 (default) ❑ LDAP v2
Referral Handling	Select one of the following options from the drop-down list: ❑ ignore (default) ❑ follow

Configuring the Event Strategy Configuration Tab

This section describes how to configure the Event Strategy Configuration tab during the channel configuration process, which is shown in the following image.



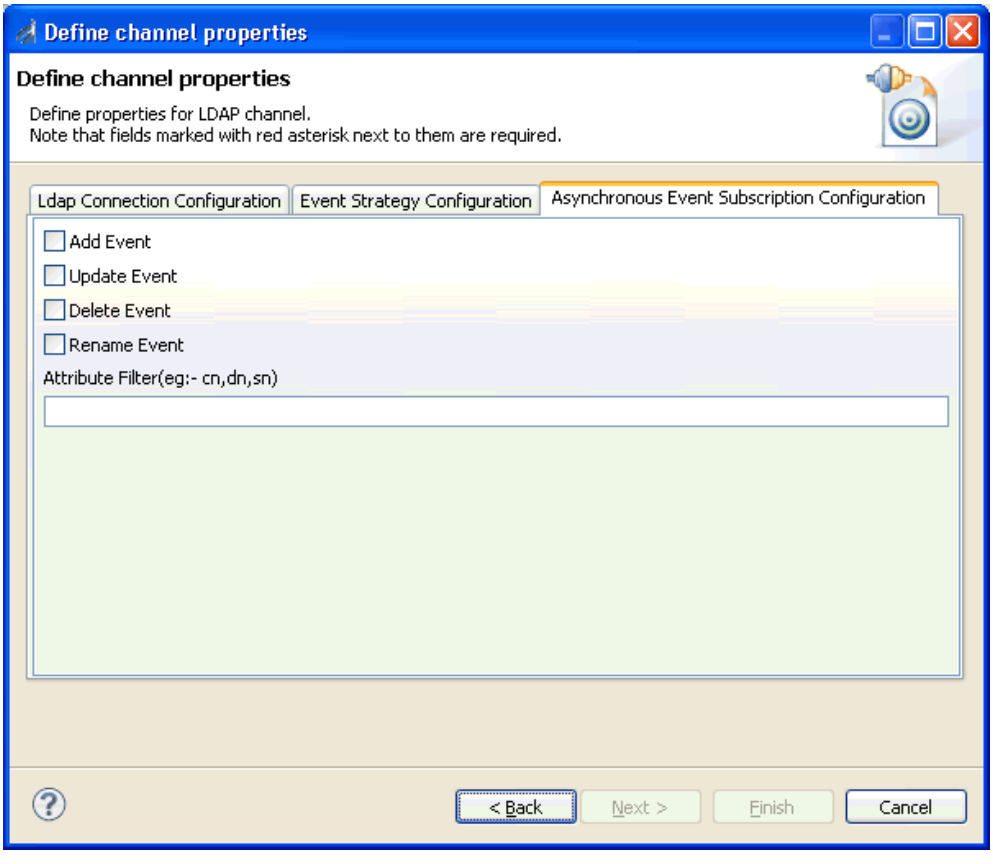
The parameters available in the Event Strategy Configuration tab are listed and described in the following table:

Parameter	Description
Directory Synchronization Polling Interval	Active Directory synchronization requires periodic polling to check for changes to the LDAP directory. The polling interval defaults to 0 seconds.

Parameter	Description
Ldap Event Detection Strategy	Select one of the following options from the drop-down list: ❑ **Active Directory Synchronization** Active Directory Synchronization is the directory synchronization mechanism that is provided by Active Directory Server and the only way events are captured from Active Directory. This strategy can also be used for any other LDAP provider types that support directory synchronization. ❑ **Asynchronous Ldap Notification** The asynchronous LDAP notification strategy registers event listeners with the LDAP server. Most servers other than Active Directory Server, support this protocol. This does not involve any polling and the notifications are in real-time. **Note:** Active Directory Server event capture is only supported when using the LDAP version 3 protocol.
Search Filter	Sets a search filter, which is used to limit the scope of events captured (for example, cn=*ein*).

Configuring the Asynchronous Event Subscription Configuration Tab

This section describes how to configure the Asynchronous Event Subscription Configuration tab during the channel configuration process, which is shown in the following image.



The parameters available in the Asynchronous Event Subscription Configuration tab are listed and described in the following table:

Parameter	Description
Add Event	Any changes that involve Add operations to the LDAP directory entries are captured and the notifications will be broadcasted.
Update Event	Any changes that involve Update operations to the LDAP directory entries are captured and the notifications will be broadcasted.

Parameter	Description
Delete Event	Any changes that involve Delete operations to the LDAP directory entries are captured and the notifications will be broadcasted.
Rename Event	Any changes that involve Rename operations to the LDAP directory entries are captured and the notifications will be broadcasted.
Attribute Filter	Sets an attribute filter, which is used to limit the scope of events captured. For example, a configured channel may only be interested in events pertaining to all employees that belong to the Toronto division of a certain company (ou=Toronto).

Appendix A Configuring the Adapter in an iWay Environment

After you successfully configure the adapter to represent a particular adapter target, the adapter can be assigned to an iWay Service Manager channel.

In this appendix:

❑ Configuring the Adapter in iWay Service Manager

Configuring the Adapter in iWay Service Manager

Before configuring the adapter in iWay Service Manager, you must first create a target, which represents a connection to a backend system, using iWay Explorer. For more information on configuring targets and connections using iWay Explorer, see *Creating XML Schemas for LDAP* on page 51.

You configure the adapter in the iWay Service Manager console. The configuration process creates run-time connection and persistent data files within Service Manager. The configuration process interrogates the Service Manager repository entries that were built when the target and connection were created using iWay Explorer. The define adapter process creates the run-time repository based on the design-time repository.

Procedure: How to Define the Adapter

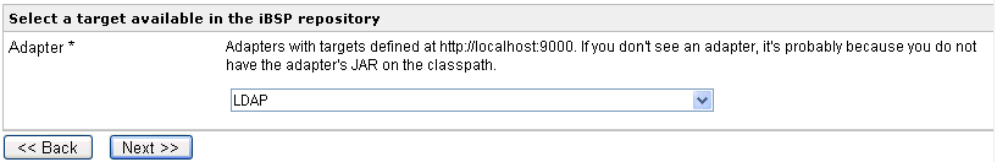
To define the adapter:

1. In the Service Manager console, select *Registry*, then *Adapters*.
2. Click *Add*.

   The iBSP URL pane opens, as shown in the following image.

3. Enter your iBSP URL, which is the location of the Service Manager repository, for example, http://localhost:9000. This field is required.
4. Click *Next*.

An adapter selection pane opens, as shown in the following image.



5. From the Adapter drop-down list, select an adapter (for example, LDAP), then click *Next*.
6. From the Target drop-down list, select a target you configured for the adapter in iWay Explorer, then click *Next*.

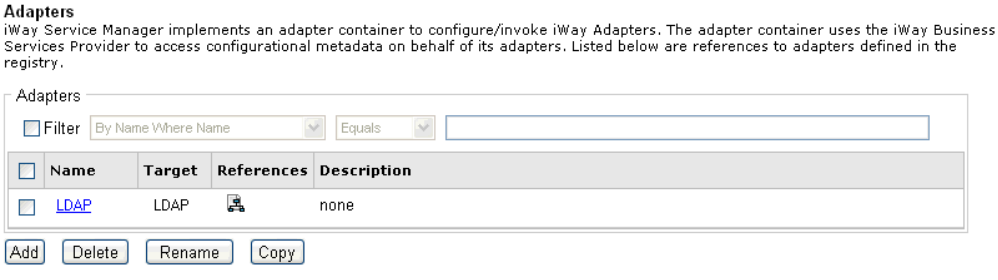
   The connection information associated with the target selected is displayed.

   a. Select whether to return an error document when an error occurs.

   b. Select whether an adapter connection will be reused between executes.

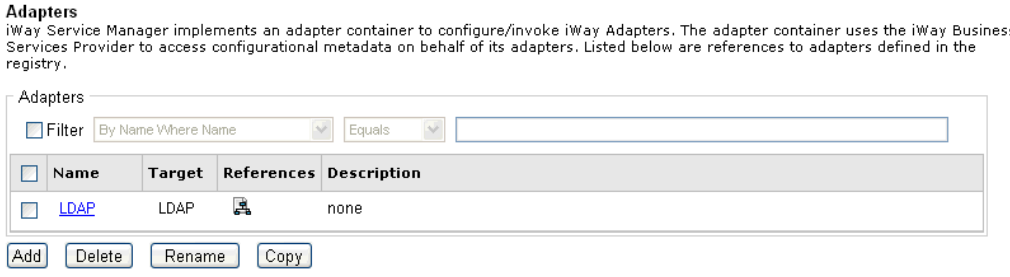
   c. Review the connection information you specified in iWay Explorer. You can change or update any information.
7. Click *Next*.
8. Provide a name and, optionally, a description, for the adapter, and click *Finish*.

   The adapter appears in the adapters list.



Procedure: How to Modify or Update an Adapter Connection

The following image shows the Adapter Defines pane which displays the name of the adapter and the description (optional).



To modify or update an adapter connection:

1. From the Adapters list, click the adapter reference you defined (for example, LDAP).

   The pane that displays the target connection information opens. You cannot change the name of the adapter or the target, but you can edit the connection information.

2. After you modify the connection information, click *Update Connection Properties*.
3. After you make changes or additions to the adapter target in iWay Explorer, click *Update Adapter Data*.
4. Click *Finish*.

Appendix B Understanding Active Directory Error Messages

This section lists and describes Active Directory error messages.

In this appendix:

- Error Messages

Error Messages

Each error message includes a code and a context number. For example:

- 525 - user not found
- 52e - invalid credentials
- 530 - not permitted to log on at this time
- 532 - password expired
- 533 - account disabled
- 701 - account expired
- 773 - user must reset password

Consider the following error message:

```
[LDAP: error code 49 - 80090308: LdapErr: DSID-0C0903AA, comment:
AcceptSecurityContext error, data 52e, v1772]
```

It can be decoded using the *data* part of the message.

Invalid credentials imply that the user ID or password is incorrect.

The following sample error codes are subject to change by Microsoft or its agents:

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 525, v893

HEX: 0x525 - user not found

DEC: 1317 - ERROR_NO_SUCH_USER (The specified account does not exist.)

NOTE: Returns when username is invalid.

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 52e, v893

HEX: 0x52e - invalid credentials

DEC: 1326 - ERROR_LOGON_FAILURE (Log on failure: unknown user name or bad password.)

NOTE: Returns when username is valid but password/credential is invalid. Will prevent most other errors from being displayed as noted.

80090308: LdapErr:DSID-0C09030B, comment: AcceptSecurityContext error, data 530, v893

HEX: 0x530 - not permitted to log on at this time

DEC: 1328 - ERROR_INVALID_LOGON_HOURS (Log on failure: account log on time restriction violation.)

NOTE: Returns only when presented with valid username and password/credential.

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 531, v893

HEX: 0x531 - not permitted to log on from this workstation

DEC: 1329 - ERROR_INVALID_WORKSTATION (Log on failure: user not allowed to log on to this computer.)

LDAP[userWorkstations:,multivalued list of workstation names>]

NOTE: Returns only when presented with valid username and password/credential.

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 532, v893

HEX: 0x532 - password expired

DEC: 1330 - ERROR_PASSWORD_EXPIRED (Log on failure: the specified account password has expired.)

LDAP[userAccountControl:<bitmask=0x00800000>] - PASSWORDEXPIRED

NOTE: Returns only when presented with valid username and password/credential.

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 533, v893

HEX: 0x533 - account disabled

DEC: 1331 - ERROR_ACCOUNT_DISABLED (Logon failure: account currently disabled.)

LDAP[userAccountControl:<bitmask=0x00000002>] ACCOUNTDISABLE

NOTE: Returns only when presented with valid username and password/credential.

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 701, v893

HEX: 0x701 - account expired

DEC: 1793 - ERROR_ACCOUNT_EXPIRED (The user's account has expired.)

LDAP[accountExpires:<value of -1, 0, or extremely large value indicates account will not expire>] - ACCOUNTEXPIRED

NOTE: Returns only when presented with valid username and password/credential.

80090308: LdapErr: DSID 0C09030B, comment: AcceptSecurityContext error, data 773, v893

HEX: 0x773 - user must reset password

DEC: 1907 - ERROR_PASSWORD_MUST_CHANGE (The user's password must be changed before logging on the first time.)

LDAP[pwdLastSet:<value of 0 indicates admin-required password change>] - MUST_CHANGE_PASSWD

NOTE: Returns only when presented with valid username and password/credential.

80090308: LdapErr: DSID-0C09030B, comment: AcceptSecurityContext error, data 775, v893

HEX: 0x775 - account locked out

DEC: 1909 - ERROR_ACCOUNT_LOCKED_OUT (the referenced account is currently locked out and may not be logged on to.)

LDAP[userAccountControl:<bitmask=0x00000010>] - LOCKOUT

NOTE: Returns even if invalid password is presented

Feedback

Customer success is our top priority. Connect with us today!

Information Builders Technical Content Management team is comprised of many talented individuals who work together to design and deliver quality technical documentation products. Your feedback supports our ongoing efforts!

You can also preview new innovations to get an early look at new content products and services. Your participation helps us create great experiences for every customer.

To send us feedback or make a connection, contact Sarah Buccellato, Technical Editor, Technical Content Management at *Sarah_Buccellato@ibi.com.*

To request permission to repurpose copyrighted material, please contact Frances Gambino, Vice President, Technical Content Management at *Frances_Gambino@ibi.com.*

Information Builders

iWay

iWay Application Protocol Adapter for LDAP User's Guide

Version 7.0.x and Higher

DN3502284.0418

Information Builders, Inc.
Two Penn Plaza
New York, NY 10121-2898