BEA AquaLogic® Interaction Identity Service - LDAP

Installation and Upgrade Guide

Version 2.2 MP2
Document Revised: June 1, 2008

Contents

Welcome to AquaLogic Interaction Identity Service - LDAP

AquaLogic Interaction Identity Service - LDAP enables you to import and synchronize users, associated profile information, and groups into the portal from an external LDAP source. User profile information can then be mapped to portal properties and stored in the database. At the time of login, the user's user name and password are passed to the LDAP source for purposes of authentication. This replaces native LDAP authentication.

This guide describes the following installation and setup steps in the order in which you should perform them:

1. Complete pre-installation procedures.
2. Install software on the remote server host computer.
3. Deploy the LDAP IDS package to an application server.
4. Register the remote server with the portal.
5. Tune configuration for deployment components.
6. This guide also includes procedures for uninstalling LDAP IDS software.

Typographical Conventions

This book uses the following typographical conventions.

Table 1-1 Typographical Conventions

Convention	Typeface	Examples/Notes
• File names • Folder names • Screen elements	**bold**	• Upload **Procedures.doc** to the portal. • The log files are stored in the **logs** folder. • To save your changes, click **Apply Changes**.
• Text you enter	`computer`	Type `Marketing` as the name of your community.
• Variables you enter	`computer with angle brackets (<>)`	Enter the base URL for the Remote Server. For example, `http://<my_computer>/`.
• New terms • Emphasis • Object example names	*italic*	• *Portlets* are Web tools embedded in your portal. • The URI *must* be a unique number. • The example Knowledge Directory displayed in Figure 5 shows the *Human Resources* folder.

BEA Documentation and Resources

This section describes other documentation and resources provided by BEA.

Table 1-2 BEA Documentation and Resources

Resource	Description
Installation Worksheet	This worksheet helps you to gather and record prerequisite information necessary for installing AquaLogic Interaction Identity Service - LDAP. It is available on edocs.bea.com and on the application CD.
Release Notes	These files are written for LDAP IDS administrators. They include information about new features and known issues in the release. They are available on edocs.bea.com and on the application CD.

Table 1-2 BEA Documentation and Resources

Resource	Description
Online Help	The online help is written for all levels of LDAP IDS users. It describes the user interface for LDAP IDS and gives detailed instructions for completing tasks in LDAP IDS. To access online help, click the help icon.
Developer Guides, Articles, API Documentation, Blogs, Newsgroups, and Sample Code	These resources are provided for developers on the BEA dev2dev site (dev2dev.bea.com). They describe how to build custom applications using AquaLogic User Interaction and how to customize AquaLogic User Interaction products and features.
Deployment Guide	This document is written for business analysts and system administrators. It describes how to plan your AquaLogic User Interaction deployment. It is available in electronic form (PDF) on edocs.bea.com.

Table 1-2 BEA Documentation and Resources

Resource	Description
AquaLogic User Interaction Support Center	The AquaLogic User Interaction Support Center is a comprehensive repository for technical information on AquaLogic User Interaction products. From the Support Center, you can access products and documentation, search knowledge base articles, read the latest news and information, participate in a support community, get training, and find tools to meet most of your AquaLogic User Interaction-related needs. The Support Center encompasses the following communities: **Technical Support Center** Submit and track support incidents and feature requests, search the knowledge base, access documentation, and download service packs and hotfixes. **User Group** Visit the User Group section to collaborate with peers and view upcoming meetings. **Product Center** Download products, read Release Notes, access recent product documentation, and view interoperability information. **Developer Center** Download developer tools and documentation, get help with your development project, and interact with other developers via BEA's dev2dev Newsgroups. **Education Services** Find information about available training courses, purchase training credits, and register for upcoming classes. If you do not see the Support Center when you log in to http://one.bea.com/support, contact ALUIsupport@bea.com for the appropriate access privileges.

Table 1-2 BEA Documentation and Resources

Resource	Description
dev2dev.bea.com	Download developer tools and documentation, get help with your development project, and interact with other developers via BEA's dev2dev Newsgroups.
Technical Support	If you cannot resolve an issue using the above resources, BEA Technical Support is happy to assist. Our staff is available 24 hours a day, 7 days a week to handle all your technical support needs. E-mail: ALUIsupport@bea.com Phone Numbers: U.S.A. +1 866.262.PLUM (7586) or +1 415.263.1696 Europe +44 1494 559127 Australia/NZ +61 2.9923.4030 Asia Pacific +61 2.9931.7822 Singapore +1 800.1811.202

Completing Pre-Installation Steps

This section describes the following pre-installation steps that will ensure a successful installation:

1. Download the most up-to-date documentation from edocs.bea.com.
2. Read the release notes for additional information on compatibility issues, known problems, and workarounds that might affect how you proceed with your deployment. Release notes are located at the top-level directory of the product package.
3. Provision host computers for your deployment and install prerequisite software. For details, see "Hardware and Software Requirements" on page 2-2.
4. Organize the information needed for the installation process by completing the *Installation Worksheet for AquaLogic Interaction Identity Service - LDAP 2.2*.

Hardware and Software Requirements

Note: For the most up-to-date list of supported software for your deployment, refer to the Interoperability page in the AquaLogic User Interaction Support Center.

The following table summarizes the hardware, operating system, and software requirements for LDAP IDS.

Caution: IPv6 is not supported. Verify that IPv6 is not enabled prior to installing LDAP IDS.

Table 2-1 Hardware and Software Requirements

Component	Requirement
LDAP IDS Host Computer	**Hardware** • 1.6 GHz or higher, with 2MB L2 cache • 1 GB memory • 2 GB disk space **Operating System** • AIX 5.3, on POWER3, POWER4, POWER5 • HP-UX 11i v2, on Itanium • Microsoft Windows Server 2003 SP1 or R2, on x86 • Red Hat Enterprise Linux 4 Update 3, on x86 • Solaris 8, 9, and 10, on SPARC • SUSE Enterprise Linux 9, on x86
Portal Software	AquaLogic Interaction 6.1.x and 6.5
Certified LDAP Vendors	Novell eDirectory, Lotus Notes, iPlanet/SunONE

CHAPTER 3

Installing AquaLogic Interaction Identity Service - LDAP

This section describes the following steps that allow for the successful installation and deployment of LDAP IDS:

1. Ensure that you have performed pre-installation procedures. For details, see “Completing Pre-Installation Steps” on page 2-1.
2. Install product files on the remote server host and the Image Service. For details, see “Installing LDAP IDS” on page 3-2.
3. Run a diagnostic test to verify successful installation. For details, see “Verifying Deployment” on page 3-3.

Installing LDAP IDS

LDAP IDS is implemented as a remote server in the context of the portal deployment; you install the product on a remote server host computer that can communicate with the portal. For host requirements, see "Hardware and Software Requirements" on page 2-2.

Note: For UNIX and Linux installations: the installer creates a new **pthome.xml** file in any install location that does not already contain the file. For that reason, you should install LDAP IDS in the same location as all other AquaLogic User Interaction components on the machine.

Note: For UNIX and Linux installations: the installation wizard is a graphical application. If you run it interactively, you must do so from an X-windows client. If you are running remotely, for example in an xterm, make sure the DISPLAY environment variable is set correctly.

To install product files:

1. Log in to the host computer using an administrator account that has access to the portal installation.
2. Map a connection to the Image Service directory.
3. Copy the LDAP IDS installation package to a location on the remote server host.
4. To launch the installer, double-click the **ALIIdentityServiceLDAP_v2-2.exe** file.
5. Complete the installation wizard pages as described in the following table.

Note: We recommend that you keep the default settings.

Table 3-1 Installation Wizard Pages

Wizard Page	Values
Introduction	Click **Next**.
Choose Server Type	Choose **Remote Server** to install files for LDAP IDS. Choose **Image Service** to install files for the Image Service.
Choose Installation Folder	Click **Next** to accept the default: Windows: **C:\bea\alui** UNIX and Linux**: /opt/bea/alui**

Table 3-1 Installation Wizard Pages

Wizard Page	Values
Specify Image Service Folder	Specify the location of your Image Service folder. **Note:** We recommend using: **\ptimages**
Application Port	Choose whether to use a secure HTTP protocol for the Web service (https) or a standard Web protocol (http). Also select your port number. The installer specifies the default port **11950**. Make sure to enter the SSL port number if using https.
Pre-Installation Summary	Verify the information in the panel and click **Install.**

6. Click **Done** to exit the installer.
7. (Windows only) Reboot your computer and start the LDAP IDS using **Administrative Tools | Services**.
8. (UNIX and Linux Only) You must set the PT_HOME environment variable, where PT_HOME is the root directory for installed AquaLogic User Interaction products, and restart LDAP IDS before verifying installation:

   a. Open a terminal window.

   b. Type the commands:

   ```
   source <pt_home>/pthome.sh
   <pt_home>/ptldapaws/2.2/bin/ptldapawsd.sh restart
   ```

Verifying Deployment

After you have deployed the LDAP IDS package, you can run a diagnostic utility to verify connectivity among deployment components.

To verify your deployment of the LDAP IDS package:

1. In a Web browser, open the URL for the remote server diagnostics utility, for example:

   http://<remoteserver>:<port>/ldapaws/install/index.html

2. Complete the steps as described in the utility summary page to verify the correct configuration of deployment components.

Registering LDAP IDS and Creating Related Portal Objects

After you have run the installation wizard and verified correct installation you must register, create, and implement LDAP IDS and its objects into the portal. This section includes information on the following topics:

- "Registering LDAP IDS" on page 4-2
- "Creating a Remote Authentication Source" on page 4-2
- "Creating a Remote Profile Source" on page 4-3

Registering LDAP IDS

The portal registers new identity services when you migrate them into the portal using the Migration Wizard. When you register the identity service, you import the remote server and Web services for the LDAP IDS.

Note: You must have administrative rights in the portal to deploy the migration packages for the Web Components and portlets.

To register LDAP IDS:

1. Log in to the portal as an administrator.
2. Click **Administration**.
3. In the Select Utilities menu, select **Migration - Import**.
4. Browse to the migration package. If you accepted installation defaults, the location is: **\\<LDAPIDSHostComputer>\bea\alui\ptldapaws\2.2\serverpackages\IdentityService-LDAP.pte**
5. Click **Load Package**.
6. Click **Finish**.

Creating a Remote Authentication Source

Create a remote authentication source to import users and groups from LDAP:

1. Log in to the portal as an administrator.
2. Click **Administration**.
3. Click the **LDAP IDS** folder.
4. From the Create Object menu, choose **Authentication Source - Remote**.
5. In the Choose Web Service dialog box, choose **LDAP IDS**.
6. Configure the authentication source as described in the online help.

Stay logged in to the portal with the LDAP IDS folder open for the next procedure.

Creating a Remote Profile Source

Create a remote profile source to import users’ profile information from LDAP. To create a remove profile source, in the LDAP IDS folder of the portal’s Administrative Object Directory:

1. From the Create Object menu, choose **Profile Source - Remote**.
2. In the Choose Web Service dialog box, choose **LDAP IDS**.
3. Configure the profile source as described in the online help.

Advanced Configuration

This section describes the following optional advanced procedures for LDAP configuration:

- "Configuring Logging" on page 5-1.
- "Configuring Application Server Session Settings" on page 5-3.
- "Configuring LDAP Server Settings" on page 5-3.
- "Using the LDAP IDS over SSL" on page 5-3.
- "Migrating Users from the Native LDAP Provider to the LDAP IDS" on page 5-5.

Configuring Logging

The **ldapws.war** file contains the **log4j.properties** file. The log4j.properties controls the logging settings for the application. You can open the log4j.properties file and edit it within the **ldapws.war** file.

There are two appenders defined:

- A1 is for the authentication source log
- A2 is for the profile source log

The default settings for the parameters in this file should be sufficient but there are several settings that you can change:

Table 5-1 Logging Settings

Files	Function
Append	Determines whether writes to the log file are appended at the end of the file, or if the file is overwritten. This should be set to true.
MaxFileSize	Specifies the maximum size a log file can be before it is rolled over into a new file if the appender is a **RollingFileAppender**. If you choose to roll over based on the date, the **MaxFileSize** setting does not take effect.
MaxBackupIndex	Sets the number of rolled-over files that are saved. The number of roll-over files you set for the **MaxBackupIndex** value depends on how much disk space you choose to devote to log files.
DatePattern	Determines the basis on which files are rolled over if the appender is a **DailyRollingFileAppender**. YYY-mm means the file is rolled over once a month. YYYY-mm-dd means the file is rolled over ever day. YYYY-mm-dd-HH rolls over every hour and so forth.
RollingFileAppender	If several synchronization jobs are run once a day use the **RollingFileAppender** so that the individual log files do not grow excessively large.
DailyRollingFIleAppender	In changing the **DailyRollingFileAppender** from **RollingFileAppender**, the **MaxFileSize** setting is ignored. This allows you to set the type of appender to either rollover based on date or size. If you use a **DailyRollingFileAppender** then you must look at the average size of the log created by a single synchronization run to determine what the total disk space is. If synchronizations are run once a week, then setting **MaxBackupIndex** to 10 provides approximately two months of job histories.

Configuring Application Server Session Settings

Within the **ldapws.war** file there is a **web.xml** file that contains settings for the application session. You can open this file and edit it within the ldapws.war file.

During large synchronizations, the portal must create database objects for all the users and groups returned by the LDAP IDS. This might cause session time-outs between the calls to GetGroups, GetUsers, and GetMembers.

You can avoid this time-out error by increasing the session-time-out value in the session-config object of **web.xml**.

Configuring LDAP Server Settings

LDAP servers allow you to set the maximum return size of a query result as well as the time limit for a query. If the LDAP IDS log file ever indicates a SizeLimitExceeded or TimeLimitExceeded error it is most likely that you need to adjust these values on the LDAP server. Different LDAP server administration consoles have these settings in different locations and you should contact your LDAP system administrator if you have questions about the location of the settings.

Using the LDAP IDS over SSL

In order to use the LDAP IDS over SSL there are two connections you must secure. This section includes the following topics:

- "Setting Up SSL Between the Portal and the Remote Server" on page 5-4.
- "Setting Up SSL Between the Remote Server and the LDAP Server" on page 5-4.

Setting Up SSL Between the Portal and the Remote Server

In order to connect to the LDAP IDS from the portal over SSL, you must connect to the remote server on an SSL port and import its trusted certificate.

From a Web browser on the portal server navigate to:
https://<remote_server>:<app_server_ssl_port>

If the computer hosting the portal does not already have a certificate from the remote server it prompts you with a Security Alert. Choose to view the certificate and install it to the Trusted Root Certification Authorities store.

When running the installer for LDAP IDS, choose https protocol and enter the SSL port for the application server. In the portal, when you configure the remote server object, use https and the SSL port.

Setting Up SSL Between the Remote Server and the LDAP Server

To connect to the LDAP server over SSL, import the certificate for the LDAP server into the **cacerts** file in the jre of the application server.

1. From a Web browser on the remote server navigate to: **https://<ldap_server>:<ldap_ssl_port>**. You should be prompted with a Security Alert.
2. Choose to view the certificate and import it.
3. Navigate to the **Tools | Internet Options** menu.
4. Select the **Content** tab and click **Certificates**.
5. Find the certificate for the LDAP server that you just imported and choose to export it as a DER encoded binary. Export it to the **<APP_SERVER_JAVA_HOME>/jre/lib/security** folder.
6. Use the java keytool to import this certificate to the **cacerts** file at **<APP_SERVER_JAVA_HOME>/jre/lib/security**.

   For instructions on using the keytool refer to the SunJava documentation.

   When you create the authentication source in the portal, enter 2 as the Security Mode. The standard SSL port is 636. If your LDAP server is using a different SSL port, enter this in the Alternate Port box.

Migrating Users from the Native LDAP Provider to the LDAP IDS

Plumtree Corporate Portal 5.0.x included a native LDAP provider. If you have been using the native LDAP provider, you may want to migrate your users to the LDAP IDS authentication source you created to preserve the MyPage and community settings.

Knowledge Base article DA_224007 “Migrating Users and Groups in 5.0.x Portals” discusses migrating users and groups in a 5.0.x portal. Read this article for instructions on the SQL commands needed to migrate the user information.

Uninstalling AquaLogic Interaction Identity Service - LDAP

To uninstall AquaLogic Interaction Identity Service - LDAP:

1. Remove the software from your remote server:
   - For Windows: Use the Windows Add/Remove Programs utility.
   - For UNIX and Linux: Use the **uninstall_ptldapaws** executable located at **<install_location>/uninstall/ptldapaws/2.2**.

   The uninstaller removes the war files and Java application files that were installed.
2. After the uninstallation process has completed, it is safe to delete the installation directory.

Upgrading AquaLogic Interaction Identity Service - LDAP

AquaLogic Interaction Identity Service - LDAP 2.2 installs with its own embedded application server. Therefore, installing it will not overwrite an existing LDAP IDS 2.x installation on another application server. You must uninstall the previous version, install the new version, and perform post-installation steps to complete upgrade.

Note: The following instructions also apply when you are upgrading from 2.2 to a 2.2 maintenance pack, or from an earlier 2.2 maintenance pack to a later one.

To upgrade from 2.x:

1. Uninstall the previous version. Refer to the installation guide for the previous version of LDAP IDS.
2. Run the installer as described in "Installing AquaLogic Interaction Identity Service - LDAP" on page 3-1.
3. Copy any template files you may have created from **<PT_HOME>/ptldapaws/<version>/settings/ldap/templates** to **<PT_HOME>/ptldapaws/2.2/settings/config/ldap/templates**.
4. Import the 2.x encryption key to your 2.2 installation:
   a. In a Web browser, open the remote server diagnostics utility, which can be found at: **http://<remoteserver>:<port>/ldapws/install/index.html**
   b. Complete the steps as described in the utility summary page in the diagnostics utility.

      At the encryption key import step, click **Import** and browse to the LDAPKeyStore file that was created for your version 2.x installation and select the key. The file can be

found at:
<JRE_HOME_FOR_YOUR_OLD_APP_SERVER>/lib/ext/LDAPKeyStore

5. In the portal, go to the remote server object for the LDAP IDS and change the port number to the one you set when you installed version 2.2 (or 2.2 maintenance pack).