Oracle® Identity Manager

Password Synchronization Module for Microsoft Active Directory
Installation and Configuration Guide

Release 9.0.4

E10179-01

May 2007

ORACLE®

Oracle Identity Manager Password Synchronization Module for Microsoft Active Directory Installation and Configuration Guide, Release 9.0.4

E10179-01

Primary Authors: Don Gosselin, Lyju Vadassery

Contents

Preface

Oracle Identity Manager Password Synchronization Module for Microsoft Active Directory Installation and Configuration Guide provides information about installing and configuring the Oracle Identity Manager Password Synchronization Module for Microsoft Active Directory. This guide also provides instructions for upgrading an existing installation of the module.

> **Note:** Some parts of the product and documentation still refer to the original Thor company name and Xellerate product name and will be rebranded in future releases.

Audience

This guide is intended for users who want to install and configure the Oracle Identity Manager Password Synchronization Module for Microsoft Active Directory.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at

http://www.oracle.com/accessibility/

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Related Documents

For more information, refer to the following documents in the Oracle Identity Manager documentation library:

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation Guide for JBoss*
- *Oracle Identity Manager Installation Guide for Oracle Containers for J2EE*
- *Oracle Identity Manager Installation Guide for WebLogic*
- *Oracle Identity Manager Installation Guide for WebSphere*
- *Oracle Identity Manager Administrative and User Console Guide*
- *Oracle Identity Manager Administrative and User Console Customization Guide*
- *Oracle Identity Manager Design Console Guide*
- *Oracle Identity Manager Tools Reference Guide*
- *Oracle Identity Manager Audit Report Developer Guide*
- *Oracle Identity Manager Best Practices Guide*
- *Oracle Identity Manager Globalization Guide*
- *Oracle Identity Manager Glossary of Terms*

The following document is available in the Oracle Identity Manager Connector Pack documentation library:

- *Oracle Identity Manager Connector Framework Guide*

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connector Pack Release 9.0.4 documentation library, visit Oracle Technology Network at

`http://www.oracle.com/technology/documentation/index.html`

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in the Oracle Identity Manager Password Synchronization Module for Microsoft Active Directory?

This chapter provides an overview of the updates made to the software and documentation for the Microsoft Active Directory connector in release 9.0.4 of the Oracle Identity Manager connector pack.

> **See Also:** The 9.0.3 release of this guide for information about updates that were new for the 9.0.3 release

The updates discussed in this chapter are divided into the following categories:

- Software Updates

  These include updates made to the password synchronization module.

- Documentation-Specific Updates

  These include major changes made to the documentation for the password synchronization module. These changes are not related to software updates.

> **See Also:** *Oracle Identity Manager Release Notes*

Software Updates

This section discusses updates made to this release of the password synchronization module.

Change in Password Synchronization Functionality

The "Components for Connecting Oracle Identity Manager to Microsoft Active Directory" section on page 1-1 has been reworded. In addition, information about the revised functionality of the password synchronization module has been added in this section.

Determining the Release Number of the Password Synchronization Module

Instructions to determine the release number of the password synchronization module are given in the "Determining the Release Number of the Password Synchronization Module" section on page 1-2.

Support for OC4J

Earlier releases of the module supported the following application servers:

- JBoss Application Server
- BEA WebLogic
- IBM WebSphere

This release of the module also supports Oracle Containers for J2EE (OC4J).

Modifications to the Known Issues List

The following changes have been made in the Known Issues list in Chapter 5:

- The issue about the "looping password change" problem that could occur while using an earlier release of the password has been addressed in this release. The corresponding item has been removed. Part of the procedure to address this problem is described in "Step 7: Configuring the xlconfig.xml File After Installing the Connector" section on page 2-14.
- The item explaining the condition under which password synchronization fails has been modified. As opposed to what was previously stated, there is no workaround for this scenario.

Documentation-Specific Updates

The following documentation-specific updates have been made in this release of the guide:

- Information in the "Components for Connecting Oracle Identity Manager to Microsoft Active Directory" section on page 1-1 has been reworded.
- If you change the password of the Oracle Identity Manager administrator after you install the password synchronization module, then the module would stop working. A caution notice explaining this has been added after Step 12 in the "Step 3: Installing the Password Synchronization Module" section on page 2-3.
- If you change the password of the Oracle Identity Manager administrator after you install the password synchronization module, then the module would stop working. A caution notice explaining this has been added after Step 12 in the "Step 3: Installing the Password Synchronization Module" section on page 2-3.
- The procedure described in the "Step 4: Performing Postinstallation Steps for the Password Synchronization Module" section on page 2-6 has been modified.

1

Overview of the Password Synchronization Module

Oracle Identity Manager is an advanced user account provisioning system for automatically granting and revoking access to enterprise applications and managed systems. The modular architecture of Oracle Identity Manager can handle most IT requirements, without requiring changes to existing infrastructure, policies, or procedures.

This chapter contains the following sections:

Components for Connecting Oracle Identity Manager to Microsoft Active Directory

Oracle Identity Manager provides the following components to link with Microsoft Active Directory:

- Connector for Microsoft Active Directory
- Password synchronization module for Microsoft Active Directory

Depending on your specific needs, you can deploy one or both of these components to connect Oracle Identity Manager and Microsoft Active Directory. Deployed together (along with LDAP over SSL), the connector and the password synchronization module provide full, bidirectional synchronization of all user attributes, including passwords.

The connector for Microsoft Active Directory updates user account attributes bidirectionally. However, password changes are updated only when the password is changed through Oracle Identity Manager, and not when it is changed through Microsoft Active Directory.

In contrast, the password synchronization module for Microsoft Active Directory updates Oracle Identity Manager with passwords changed in Microsoft Active Directory. This is achieved as follows:

The password synchronization module intercepts a password change event in Microsoft Active Directory and sends the new password to Oracle Identity Manager. Now, if the password change in Oracle Identity Manager fails because, for example, the password does not meet the password policy, then the password change is not allowed in Microsoft Active Directory. However, if the password change in Oracle

Identity Manager succeeds, then the password change is allowed in Microsoft Active Directory.

The following table compares the functionality offered by both tools.

Functionality	Module	Connector
Updates Microsoft Active Directory with user account attributes (except for passwords) changed in Oracle Identity Manager	No	Yes
Updates Oracle Identity Manager with user account attributes (except for passwords) changed in Microsoft Active Directory	No	Yes
Updates Microsoft Active Directory with passwords changed in Oracle Identity Manager (requires LDAP over SSL)	No	Yes
Updates Oracle Identity Manager with passwords changed in Microsoft Active Directory	Yes	No

Files and Directories That Comprise the Password Synchronization Module

The installation files for the module are compressed in the following ZIP file on the installation media:

`Directory Servers/Microsoft Active Directory/Microsoft Active Directory Password Sync`

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
`setup_ad.exe`	This file is used to install the password synchronization module.
`set_ad.jar`	This JAR file is used during the installation process.
Files in the `com/oracle/xl/installer` directory	Each of these resource bundle files contains language-specific information that is used by the connector. **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the user interface of Oracle Identity Manager. These text strings include GUI element labels and messages displayed on the Administrative and User Console.
Files in the `jpclient/lib` directory	These are password synchronization library files.
Files in the `xlhome/ext` directory	These are third-party JAR files.
Files in the `xlhome/install` directory	These JAR files are required by the password synchronization module installer.

Determining the Release Number of the Password Synchronization Module

To determine the release number of an existing password synchronization module:

1. Extract the contents of the `xliADSync.jar` file. This file is copied into the *`ADSYNC_HOME`*`/lib` directory after you perform the installation process described in Chapter 2.
2. Open the `manifest.mf` file in a text editor. The `manifest.mf` file is one of the files bundled inside the `xliADSync.jar` file.

   In the `manifest.mf` file, the release number of the connector is displayed as the value of the `Version` property.

2

Deploying the Password Synchronization Module

This guide covers two scenarios:

- Upgrading an existing instance of the password synchronization module to the current version

  To implement this option, follow the instructions provided in Chapter 3.

- Deploying the password synchronization module

  To implement this option, follow the instructions provided in this chapter.

Deploying the password synchronization module involves performing the following general procedures:

- Step 1: Preparing to Install the Password Synchronization Module
- Step 2: Enabling Password Policies for Microsoft Active Directory
- Step 3: Installing the Password Synchronization Module
- Step 4: Performing Postinstallation Steps for the Password Synchronization Module
- Step 5: Configuring the Password Synchronization Module
- Step 6: Configuring the Password Synchronization Module for SSL Communication
- Step 7: Configuring the xlconfig.xml File After Installing the Connector

Step 1: Preparing to Install the Password Synchronization Module

To prepare for installation, first verify that the following deployment requirements are addressed:

- An instance of Oracle Identity Manager release 8.5.3.1 or later is installed, running, and visible to the computer hosting the Microsoft Active Directory domain controller on which you want to install the password synchronization module.

  See Also: Depending on the application server that you use, refer to one of the following guides:

  Oracle Identity Manager Installation Guide for JBoss

  Oracle Identity Manager Installation Guide for Oracle Containers for J2EE

  Oracle Identity Manager Installation Guide for WebLogic

  Oracle Identity Manager Installation Guide for WebSphere

- The connector for Microsoft Active Directory must be deployed.

  See Also: *Oracle Identity Manager Connector Guide for Microsoft Active Directory*

- If you are installing on a computer other than the host for the application server, then you must know the host name and port number of the computer hosting that application server. In addition, the remote host must be able to ping the application server host using both IP address and host name.
- Suppose you use IBM WebSphere to host your Oracle Identity Manager installation. Then on the computer where you are installing the password synchronization module, you must install an instance of the IBM WebSphere Application Client that is compatible with the installed version of IBM WebSphere.

  Note: This step does not apply if the application server hosting the Oracle Identity Manager server to which Active Directory will connect is either JBoss Application Server or BEA WebLogic.

- The computer on which you are installing the password synchronization module meets the requirements listed in the following table.

Item	Requirement
Microsoft Active Directory	Active Directory Server
Host operating system	Any one of the following: ■ Microsoft Windows 2000 with Service Pack 4 or later ■ Microsoft Windows Server 2003

Note: You must install a separate instance of the password synchronization module on each Active Directory domain controller for which you require password synchronization to the user account stores managed by Oracle Identity Manager.

The installation files for the password synchronization module are compressed in the following directory on the installation media:

```
Directory Servers/Microsoft Active Directory/Microsoft Active Directory Password
Sync
```

After verifying the deployment requirements, copy the ZIP file to a directory on the Oracle Identity Manager server. Extract the contents of the ZIP file into this directory.

See Also: The "Files and Directories That Comprise the Password Synchronization Module" section on page 1-2 for more information about the files in the installation media ZIP file

Step 2: Enabling Password Policies for Microsoft Active Directory

To enforce both the default Microsoft Windows password policy and the custom password policy, you must enable the "Passwords must meet complexity

requirements" policy setting. This section describes the procedure to enable this policy setting.

> **Note:** If you do not want to enforce the default password policy, then you must ensure that the "Passwords must meet complexity requirements" policy setting is disabled.
>
> A custom password policy is enforced, regardless of whether the "Passwords must meet complexity requirements" policy setting is disabled or enabled.

To enable the "Passwords must meet complexity requirements" policy setting:

1. On the Microsoft Windows computer hosting the Active Directory domain controller on which you are installing the password synchronization module, start the Domain Security Policy application.

   To do this, on the Microsoft Windows computer, click the **Start** menu, **Programs**, **Administrative Tools,** and **Domain Security Policy.**

2. If you are using Microsoft Active Directory 2003, then directly proceed to the next step.

   If you are using Microsoft Active Directory 2000, then select **Window Settings** on the left pane of the Domain Security Policy application window and then proceed to the next step.

3. Select **Security Settings,** expand **Account Policies,** and then click **Password Policy.**

4. Double-click **Passwords must meet complexity requirements.** The Password Must Meet Complexity Requirements Properties dialog box is displayed.

5. In the dialog box, select **Define this policy setting,** select **Enabled,** and then click **OK.**

Step 3: Installing the Password Synchronization Module

To install the password synchronization module:

1. On the computer hosting the Active Directory domain controller where you are installing the password synchronization module:

   a. Open Microsoft Windows Explorer.

   b. Navigate to the temporary directory into which you extract the contents of the installation media ZIP file.

   c. Double-click the `setup_ad.exe` file to start the installer.

   d. Specify a language.

2. Click **Next.**

3. On the Target Directory page, you can either accept the default installation directory or specify the path to the directory in which you want install the module. For example, you can specify a path similar to the following:

   ```
   C:/OracleProvisioningAD
   ```

   Alternatively, you can use the **Browse** button to navigate to the installation directory.

4. Click **Next.**

   The installer creates a directory named `adsynch` inside the installation directory that you specify. Then, it copies the password synchronization module components into the `adsynch` directory and creates certain directories inside the `adsynch` directory.

   Note: From this point onward, this guide refers to the directory *`user_specified_install_directory`*`/adsynch` as *`ADSYNC_HOME`*.

5. On the Application Server page, specify the application server that hosts the Oracle Identity Manager server to which the Active Directory domain controller will connect. Then, click **Next.**

   Note: If you specify IBM WebSphere as the application server, then perform the next step. Otherwise, directly proceed to Step 7.

6. On the WebSphere Directory page, specify the path to the directory where the IBM WebSphere Application Client is installed, on the computer where you are installing the module. Then, click **Next.**
7. On the JRE page, specify the JRE option that you want to use with the module. The following choices are available:
   - JRE bundled with Oracle Identity Manager
   - An existing JRE 1.4.2 installation on the computer where you are installing the password synchronization module. The following table lists the appropriate JRE version for the supported application servers.

Application Server	Required JRE	Comments
JBoss Application Server	Sun JRE 1.4.2_09 or later	However, all versions of Sun JRE 1.5 are *not* supported.
BEA WebLogic	Sun JRE 1.4.2_09 or later	However, all versions of Sun JRE 1.5 are *not* supported.
IBM WebSphere	IBM JRE 1.4.2_*x*	Available as part of the IBM WebSphere Application Client installation that is compatible with IBM WebSphere on the server on which Oracle Identity Manager is installed
OC4J	SunJRE 1.4.2_09 or later	However, all versions of Sun JRE 1.5 are *not* supported.

   For an existing JRE installation, you must specify the path to the installation. Then, click **Next**.

8. On the System Administration page, specify the account name and password required to log in to the Oracle Identity Manager server.

   The default account for login is `xelsysadm`.

   After specifying the required information, click **Next.**

9. On the Application Server Configuration page, specify the following:

- The host name or IP address of the application server computer hosting Oracle Identity Manager
- The naming port associated with the application server. The following table lists the default naming ports for the supported application servers.

Application Server	Default Naming Port
JBoss Application Server	1099
BEA WebLogic	7001
IBM WebSphere	2809
OC4J	12401

If the application server for Oracle Identity Manager uses a nondefault naming port, then use that port number and consult your system administrator for additional guidance.

After you specify the required information, click **Next.**

10. On the Summary page, verify that the installation directory for the module, which you specify on the Target Directory page, is correctly displayed.

    If you need to change the installation directory, click **Back** until you reach the Target Directory page, make the required changes, and then proceed through the installation sequence again.

    When the installation directory is displayed correctly, click **Install.**

11. The Complete page displays a message indicating successful installation.

    Click **Finish** to close the installer.

12. Restart the computer.

Caution: Do not change the Oracle Identity Manager administrator password after you install the password synchronization module. If you change the password after installation, then the password synchronization module would stop working.

If you change the password, then you must reinstall the password synchronization module.

Files Copied During Password Synchronization Module Installation

The following table lists the installation locations for the key components of the password synchronization module.

File	Description
Windows_System32_Directory/Adsync.dll	This file is registered as a listener for password changes to the Active Directory Domain controller. Whenever an Active Directory password is changed, this file calls the Change Password script named `ChangePassword.cmd`.

File	Description
ADSYNC_HOME/config/xlconfig.xml	This file contains all the user-configurable settings for the password synchronization module. Users can edit this file after installing the module. For details, refer to the "Step 5: Configuring the Password Synchronization Module" section on page 2-7.
ADSYNC_HOME/lib/xliADSync.jar	This JAR file contains the class files required by the Change Password script.
ADSYNC_HOME/ChangePassword.cmd	This script, which is called by adsync.dll in response to a password change, uses the required classpath and command-line parameters to call the ChangePassword class, which is in the xliADSync.jar file.
ADSYNC_HOME/wsChangePassword.cmd	This is the version of the Change Password script that is used by IBM WebSphere.
ADSYNC_HOME/lib/xliADSync.ear	This file contains the class files required by the version of the Change Password script used by IBM WebSphere.

Step 4: Performing Postinstallation Steps for the Password Synchronization Module

After you install the password synchronization module, perform the following steps:

1. Copy the following files from the *OIM_home*\ext directory to the *ADSYNC_HOME*/ext directory on the computer where you installed the password synchronization module:
   - javagroups-all.jar or jgroups-all.jar
   - oscache-2.0.2-22Jan04.jar or oscache.jar
2. Copy all the JAR files from the *OIM_Design_Console_installation_dir*/lib directory on the computer hosting the Oracle Identity Manager Design Console to the *ADSYNC_HOME*\lib directory on the computer where you install the password synchronization module.
3. Depending on the application server used, perform one of the following steps:
   - For JBoss Application Server, copy the *JBoss_home*/client/jbossall-client.jar to the *ADSYNC_HOME*/ext directory.
   - For BEA WebLogic, copy the *BEAWebLogic_home*/weblogic81/server/lib/weblogic.jar into the *ADSYNC_HOME*/ext directory.
   - For IBM WebSphere, extract and copy the xlDataObjectBeans.jar file into the *ADSYNC_HOME*/lib directory as follows:

     a. Use the following URL to connect to the IBM WebSphere administrative console:

     ```
     http://localhost:9090/admin
     ```

     b. Use the Oracle Identity Manager administrator account credentials to log in.

     c. Click **Applications**, and then click **Enterprise Applications**.

d. Select **Xellerate**.

e. Click **Export**.

f. Save the `Xellerate.ear` file to a temporary directory.

g. Extract the `xlDataObjectBeans.jar` file from the `Xellerate.ear` file.

h. Copy the `xlDataObjectBeans.jar` file into the *ADSYNC_HOME*`/lib` directory.

Note: Ensure that you extract and copy the `xlDataObjectBeans.jar` file, not the `xlDataObjects.jar` file.

- For OC4J, copy the following files into the *ADSYNC_HOME*`/ext` directory:

  OC4J_home`/j2ee/home/oc4jclient.jar`
  OC4J_home`/j2ee/home/lib/ejb.jar`

4. If you plan to run Oracle Identity Manager on a clustered application server, then:

   a. Establish a trust relationship between the virtual server that represents the Oracle Identity Manager cluster and the computer hosting the Active Directory domain controller on which you install the password synchronization module.

   b. Add the host name of the virtual server to the `hosts` file of the computer hosting the Active Directory domain controller on which you install the password synchronization module.

   c. Edit the `xlconfig.xml` file associated with the password synchronization module you install. This file is located in the *ADSYNC_HOME*`/config` directory.

   In the `xlconfig.xml` file, change the value of the `<java.naming.provider.url>` tag to the fully qualified host name of the virtual server.

   Note: Each instance of the `xlconfig.xml` file is in the `config` directory. This directory is in the root installation directory for the component with which the configuration file is associated. For example, the path of the `xlconfig.xml` file associated with the password synchronization module is as follows:

   ADSYNC_HOME`/config`

   After you update the value of the `<java.naming.provider.url>` tag in the `xlconfig.xml` file associated with the password synchronization module, save and close the file.

Step 5: Configuring the Password Synchronization Module

After you complete installation of the password synchronization module, you can configure it by editing the `xlconfig.xml` file, which is located in the *ADSYNC_HOME*`/config` directory.

To configure the parameters in the xlconfig.xml file, first open the file by using any text editor. The following table lists the elements you can configure within the <ADsync> tag in the xlconfig.xml file.

Tag Within the <ADSync> Tag	Description
<UserMatch> </UserMatch>	The MatchingMethod parameter specifies how Oracle Identity Manager matches an Oracle Identity Manager user to the Active Directory ID passed to the adsync.dll file. The first of the following three options is the default. Use it when all the login IDs in Oracle Identity Manager match all the Active Directory user IDs. When the login IDs in Oracle Identity Manager and the Active Directory IDs do not match, then use one of the remaining options. ■ **UserID:** The Active Directory user ID matches the Oracle Identity Manager user login. ■ **UDF:** The Active Directory user ID matches the UDF specified in the <FieldName> attribute. ■ **ResourceField:** The Active Directory user ID matches the <FieldName> attribute in the process form of the Oracle Identity Manager user to whom a resource object specified by the <ResourceObject> attribute is provisioned.
<Result> </Result>	This optional configuration element specifies where the result of the password change operation must be logged (apart from the adsync.log file). Values for the following parameters are provided as tags within the <Result> tag: ■ **UpdateUDF:** Set to True or False to update a status field in the Users form. ■ **FieldName:** Specify a field name when the UpdateUDF tag is set to True. For example, FieldName can be USR_UDF_STATUS. ■ **FailureValue:** This string goes into the status field if the password reset operation fails. ■ **SuccessValue:** This string goes into the status field if the password reset operation succeeds. ■ **AppendTimeStamp:** Set this to True or False to append a timestamp to the string in the status field.

The following sample XML code provides a listing of the original (default) contents of the <ADSync> tag:

```
<ADSync>
  <!--
  The Login section provides information about how the utility is authenticated.
  If UseSignature is true, then the username is used for authentication, using the
  signature-based login. The key in the "PrivateKey" alias is used.
  If UseSignature is false, then the username and password are used for
  authentication.
  -->
  <Login>
   <UseSignature>false</UseSignature>
   <Username>xelsysadm</Username>
   <Password encrypted="true">tPzEM127PIQxO64w2g7wgw==</Password>
  </Login>
  <!--
  The Active Directory name should match an Oracle Identity Manager username.
  If the MatchingMethod is UserID, the Active Directory username is assumed to be
```

```
  the Oracle Identity Manager user name.
  For UDF, FieldName must contain the name of the User Defined field that
  contains the active directory user ID.
  For ResourceField, process forms of the users who have ResourceObject
  specified are searched to find the required user. This can be used if
  Active Directory is provisioned as an account, but not a trusted source.
  -->
  <UserMatch>
   <!-- UserID, UDF and ResourceField -->
   <MatchingMethod>UserID</MatchingMethod>
   <FieldName>UD_ADUSER_LOGIN</FieldName>
   <ResourceObject>AD User</ResourceObject>
  </UserMatch>
  <!--
  If required, a UDF field can be updated with the result of the operation and
  Timestamp so that additional workflow can be started.
  -->
  <Result>
   <UpdateUDF>false</UpdateUDF>
   <FieldName>USR_UDF_ADPWDRES</FieldName>
   <SuccessValue>SUCCESS</SuccessValue>
   <FailureValue>FAIL</FailureValue>
   <AppendTimeStamp>true</AppendTimeStamp>
  </Result>
</ADSync>
```

After you make the required changes to the user-configurable tags in the `xlconfig.xml` file, save and close the file.

Step 6: Configuring the Password Synchronization Module for SSL Communication

Note: This is an optional step of the procedure.

However, the configuration of secure client operation (using SSL at the server) affects all clients. This means that if you use SSL to secure Oracle Identity Manager communication with the password synchronization module, then the Oracle Identity Manager Design Console and any other custom clients must also communicate with Oracle Identity Manager using SSL.

You can configure SSL to secure the transfer of password information from Microsoft Active Directory to Oracle Identity Manager. The procedure that you must follow depends on the application server that you use:

See Also: The "Step 8: Configuring SSL" section on page 2-14 of *Oracle Identity Manager Connector Guide for Microsoft Active Directory* for information about configuring SSL to secure data transfer from Oracle Identity Manager to Microsoft Active Directory.

- Configuring the Password Synchronization Module for SSL Communication on JBoss Application Server
- Configuring the Password Synchronization Module for SSL Communication on BEA WebLogic

After you configure the password synchronization module and the Design Console for SSL communication, you must check if SSL has been enabled for these clients by performing the following procedure:

- Validating SSL Communication for the Password Synchronization Module and the Design Console

Configuring the Password Synchronization Module for SSL Communication on JBoss Application Server

To configure password synchronization module for SSL communication on JBoss Application Server:

1. To export the Oracle Identity Manager Server certificate, change to the *OIM_home*/config directory and then enter the following command:

   ```
   Java_home/bin/keytool -export -file xlserver.cer -keystore .xlkeystore
   -storepass xellerate -alias xell
   ```

   A file named xlserver.cer is created in the config directory. This is the Oracle Identity Manager certificate file.

2. Copy the xlserver.cer file from the *OIM_home*/config directory to the *ADSYNC_HOME*/java/lib/security directory on the Microsoft Active Directory server.

   Note: You create the xlserver.cer file by performing Step 2 of the procedure described in the "Configuring the Design Console for SSL Communication on JBoss Application Server" section.

3. Change to the directory into which you copy the xlserver.cer file, and then enter the following command to import the certificate:

   ```
   keytool -import -alias alias -file xlserver.cer -keystore my_cacerts -storepass
   password -trustcacerts
   ```

   In this command:

   - *alias* is the alias for the certificate (for example, the server name)
   - *my_cacerts* is the full path and name of the certificate store (the default is cacerts)

     The actual certificate store location is *JBoss_home*/jre/lib/security/cacerts.
   - *password* is the keystore password

     Note: changeit is the default password for the cacerts file stored in the Sun JVM. This may change depending on the JVM that you are using.

4. In the command prompt window, when you are prompted to specify whether or not you want to trust this certificate, enter YES.

After you configure the password synchronization module for SSL communication, you must ensure that all other clients of Oracle Identity Manager, such as the Design Console, are configured for SSL communication.

See Also: *Oracle Identity Manager Design Console Guide* for information about configuring the Design Console for SSL communication

Configuring the Password Synchronization Module for SSL Communication on BEA WebLogic

To configure the password synchronization module for SSL communication on BEA WebLogic:

1. Open the BEA WebLogic console.
2. Enable the SSL listening port of BEA WebLogic as follows:
   a. Expand **Servers**, and then click the name of the server that you want to use.
   b. Click **Configuration**, and then click **General**.
   c. On the General tab, select the **SSL Listen Port Enabled** check box.

      The default SSL port, 7002, is enabled.
   d. Click **Apply**.
3. Configure the keystore in BEA WebLogic as follows:
   a. On the Keystores & SSL tab, specify the following values:

      Custom Identity Keystore: Specify the name and location of the keystore that you want to use. The following is the default keystore:

      WebLogic_home/server/lib/DemoIdentity.jks

      Type: Specify the type of the keystore.

      Passphrase and **Confirm Passphrase**: Specify the password for the keystore.
   b. Click **Change**.
   c. From the Keystores list, select Custom Identity And Java Standard Trust.
   d. Specify the following values:
      – **Custom Identity Key Store File Name**: Specify the fully qualified path to the identity keystore.
      – **Custom Identity Key Store Type**: Specify the type of the keystore.
      – **Custom Identity Key Store Pass Phrase** and **Confirm Custom Identity Key Store Pass Phrase**: Specify the password for the keystore.
   e. Click **Continue**.
   f. Specify the following values:

      Private Key Alias: Specify the alias that you have created for the identity keystore.

      Passphrase and **Confirm Passphrase**: Specify the password that is used to retrieve the private key from the keystore.
   g. Click **Finish**.
4. Restart BEA WebLogic for the changes to take effect.
5. Generate a signed certificate as follows:
   a. Navigate to the following directory:

```
JDK_used_by_WebLogic/jre/lib/security
```

b. Enter the following command to generate the certificate:

```
keytool -genkey -alias private_key_alias -keyalg RSA -keysize 1024 -dname
"DN_value" -keypass private_key_password -keystore identity_store_file
-storepass identity_store_file_password
```

In this command:

- *private_key_alias* is the alias that you want to use for the private key
- *private_key_password* is the password that toy want to use for the private key
- *DN_value* is the distinguished name (DN) for your organization

  The CN value in the DN must be the host name or IP address of the Oracle Identity Manager server. You can get the CN value from the <ADSYNC_HOME>/config/xlconfig.xml file. For example, suppose the value of the <java.naming.provider.url> tag is as follows:

  ```
  t3://oimserver:7001
  ```

  Then, the DN that you enter in the command must contain CN=oimserver.
- *identity_store_file* is the identity store that you want to use
- *identity_store_file_password* is the password of the identity store that you want to use

The following is a sample command:

```
keytool -genkey -alias adpwmod -keyalg RSA -keysize 1024 -dname
"CN=oimserver, OU=Identity, O=Acme Widgets Corp,L=RedwoodShores,
S=California, C=US" -keypass adpw_pass -keystore idstore.jks -storepass
idstorepass
```

c. Enter the following command to sign the certificate:

```
keytool -selfcert -alias private_key_alias -sigalg MD5withRSA -validity
2000 -keypass private_key_password -keystore identity_store_file -storepass
identity_store_file_password
```

d. Enter the following command to export the certificate

```
keytool -export -alias private_key_alias -file cert_file_name -keypass
private_key_password -keystore identity_store_file -storepass
identity_store_file_password
```

In this command, replace *cert_file_name* with the name that you want to use for the certificate file. For example, you can use adsslcert.pem as the name of the file.

6. Add the details of the keystore in BEA WebLogic as follows:

a. Open the BEA WebLogic console.

b. Click **Servers**, **Configuration**, and **Keystores & SSL**.

c. Click **Change**.

d. From the **KeyStores** list, select **Custom Identity and Java Standard Trust** and then click **Continue**.

e. Enter the following values:

- Custom Identity Key Store File Name: Enter the complete location of the identity store file, *identity_store_file*, that you generate in Step 2.

  For example:

  ```
  c:\bea814\jdk142_05\jre\lib\security\idstore.jks
  ```

- Custom Identity Key Store Type: Enter **JKS**.
- Custom Identity Key Store Passphrase: Enter the identity store file password, *identity_store_file_password*
- Private Key Alias: Enter the private key alias, *private_key_alias*
- Passphrase: Enter the private key password, *private_key_password*

f. Click **Finish**.

7. Restart the server for these changes to take effect.

After you configure BEA WebLogic for SSL, configure the password synchronization module for SSL communication as follows:

1. Copy the certificate file from the *JDK_used_by_WebLogic*/jre/lib/security directory to the JRE configured with the password synchronization module. This certificate file is created when you perform Step 2.d of the earlier procedure.

For example, if you are using the JRE bundled with the module, then copy the certificate file into the <*ADSYNC_HOME*>/java/lib/security directory.

2. Change to the directory into which you copy the certificate file, and then enter the following command to import the certificate:

```
keytool -import -alias private_key_alias -file cert_file_name -keystore
my_cacerts -storepass password -trustcacerts
```

In this command:

- *alias* is the alias for the certificate (for example, the server name)
- *my_cacerts* is the full path and name of the certificate store (the default is cacerts)

  The actual certificate store location is as follows:

  ```
  JBoss_home/java/jre/lib/security/cacerts
  ```

- *password* is the keystore password

  Note: changeit is the default password for the cacerts file stored in the Sun JVM. This may change depending on the JVM that you are using.

3. In the command prompt window, when you are prompted to specify whether or not you want to trust this certificate, enter YES.

4. Copy the *WebLogic_home*/license.bea file into the *ADSYNC_HOME* directory.

5. Add the *ADSYNC_HOME* directory path to the CLASSPATH environment variable.

To do this, you first enter a semicolon (;) at the end of the existing value of the CLASSPATH and then enter the *ADSYNC_HOME* directory path.

6. In the *ADSYNC_HOME*/config/xlconfig.xml file, search for the <java.naming.provider.url> tag and change the protocol value to t3s and the port value to the SSL port number.

For Example:

```
<java.naming.provider.url>t3s://solqe4:7002</java.naming.provider.url>
```

Step 7: Configuring the xlconfig.xml File After Installing the Connector

After you install the Microsoft Active Directory connector, you must make changes in the `xlconfig.xml` of the password synchronization to reflect the properties of the connector as follows:

1. Open the `xlconfig.xml` file.
2. In the file, search for the `<ADConnectorConfig>` tag.
3. Make the following changes in the child elements of the <ADConnectorConfig> tag:
   - `<Installed>` tag: Set the value to true.
   - `<ITResourceType>` tag: Specify the name of the IT resource type for the connector.
   - `<ITResourceName>` tag: Specify the name of the IT resource for the connector.
4. Save and close the file.

The following XML code shows sample values entered in the <ADConnectorConfig> section:

```
<ADConnectorConfig>
     <Installed>true</Installed>
     <ITResourceType>AD Server</ITResourceType>
     <ITResourceName>AD34</ITResourceName>
</ADConnectorConfig>
```

3

Upgrading the Password Synchronization Module

You can upgrade an existing password synchronization module to the current revision. To do this, perform the following procedures:

1. Refer to Chapter 4 for instructions on removing an earlier instance of the password synchronization module.
2. Verify that your environment is ready for the latest release of the password synchronization module by completing the procedure described in the "Step 1: Preparing to Install the Password Synchronization Module" section on page 2-1.
3. Complete the procedure described in the "Step 2: Enabling Password Policies for Microsoft Active Directory" section on page 2-2.
4. Complete the procedure described in the "Step 3: Installing the Password Synchronization Module" section on page 2-3 to install the password synchronization module on the computer hosting the Active Directory domain controller for which you want to implement password synchronization.
5. Complete the procedure described in the "Step 4: Performing Postinstallation Steps for the Password Synchronization Module" section on page 2-6 to copy the required files from the computer hosting Oracle Identity Manager to the computer on which you install the password synchronization module.

4

Removing the Password Synchronization Module

To remove an installed and configured instance of the password synchronization module:

1. Delete the module-related registry keys by performing the following steps:
   a. Run `regedit.exe`. This file is usually located in the Microsoft Windows registry
   b. Navigate to the following key:

      `HKEY_LOCAL_MACHINE | System | CurrentControlSet | Control | Lsa`

   c. Double-click the **Notification Packages** key.
   d. In the Edit Binary Value dialog box, delete **adsync** from the list of values, and then click **OK.**

      For example, suppose the original data string displayed in the Data column on the right pane of the Registry Editor application window is as follows:

      `FPNWCLNT RASSFM KDCSVC scecli adsync`

      After you delete **adsync** from the list of values, the data string would appear as follows:

      `FPNWCLNT RASSFM KDCSVC scecli`

   e. Navigate to the following key:

      `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\adsync`

   f. Delete this key along with all of its properties.
2. Restart the computer.
3. Delete the `ADSync.dll` file from the *`WINDOWS`*`\system32` directory.
4. Delete the *`ADSYNC_HOME`* directory.

5

Known Issues

The following is a known issue associated with this release of the password synchronization module:

- Password synchronization fails if you install the password synchronization module on a mapped device.

Index