

## **Oracle® Identity Manager**

Password Synchronization Module for Microsoft Active Directory  
Installation and Configuration Guide

Release 9.0.2

**B32179-01**

September 2006

Oracle Identity Manager Password Synchronization Module for Microsoft Active Directory Installation and Configuration Guide, Release 9.0.2

B32179-01

Copyright © 2006, Oracle. All rights reserved.

Primary Authors: Don Gosselin, Lyju Vadassery

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

---

---

# Contents

<b>Preface</b> .....	v
Audience .....	v
Documentation Accessibility .....	v
Related Documents .....	vi
Documentation Updates .....	vii
Conventions .....	vii
<b>What's New in the Oracle Identity Manager Password Synchronization Module for Microsoft Active Directory?</b> .....	ix
Software Updates .....	ix
Documentation-Specific Updates.....	x
<b>1 Overview of the Password Synchronization Module</b>	
Components for Connecting Oracle Identity Manager to Microsoft Active Directory .....	1-1
Files and Directories That Comprise the Password Synchronization Module .....	1-2
<b>2 Deploying the Password Synchronization Module</b>	
Step 1: Preparing to Install the Password Synchronization Module .....	2-1
Step 2: Enabling Password Policies for Active Directory .....	2-2
Step 3: Installing the Password Synchronization Module .....	2-3
Files Copied During Password Synchronization Module Installation.....	2-5
Step 4: Performing Postinstallation Steps for the Password Synchronization Module.....	2-5
Step 5: Configuring the Password Synchronization Module .....	2-6
<b>3 Upgrading the Password Synchronization Module</b>	
<b>4 Removing the Password Synchronization Module</b>	
<b>5 Known Issues</b>	



---

---

# 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 set:

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation and Upgrade Guide for JBoss*
- *Oracle Identity Manager Installation and Upgrade Guide for WebLogic*
- *Oracle Identity Manager Installation and Upgrade Guide for WebSphere*
- *Oracle Identity Manager Installation and Upgrade Guide for Oracle Containers for J2EE*
- *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 Connector Guide for BMC Remedy User Management*
- *Oracle Identity Manager Connector Guide for CA-ACF2 Advanced*
- *Oracle Identity Manager Connector Guide for CA-Top Secret Advanced*
- *Oracle Identity Manager Connector Guide for Database Application Tables*
- *Oracle Identity Manager Connector Guide for Database User Management*
- *Oracle Identity Manager Connector Guide for IBM RACF*
- *Oracle Identity Manager Connector Guide for IBM RACF Advanced*
- *Oracle Identity Manager Connector Guide for IBM Lotus Notes and Domino*
- *Oracle Identity Manager Connector Guide for Microsoft Active Directory*
- *Oracle Identity Manager Password Synchronization Module for Microsoft Active Directory Installation and Configuration Guide*
- *Oracle Identity Manager Connector Guide for Microsoft Exchange 2000 and 2003*
- *Oracle Identity Manager Connector Guide for Microsoft Exchange 5.5*
- *Oracle Identity Manager Connector Guide for Microsoft Windows 2000*
- *Oracle Identity Manager Connector Guide for Microsoft Windows NT 4.0*
- *Oracle Identity Manager Connector Guide for Novell eDirectory*
- *Oracle Identity Manager Connector Guide for Novell GroupWise*
- *Oracle Identity Manager Connector Guide for Oracle e-Business Employee Reconciliation*
- *Oracle Identity Manager Connector Guide for Oracle e-Business User Management*
- *Oracle Identity Manager Connector Guide for Oracle Internet Directory*

- *Oracle Identity Manager Connector Guide for PeopleSoft Employee Reconciliation*
- *Oracle Identity Manager Connector Guide for PeopleSoft User Management*
- *Oracle Identity Manager Connector Guide for Siebel Enterprise Applications*
- *Oracle Identity Manager Connector Guide for RSA Authentication Manager*
- *Oracle Identity Manager Connector Guide for RSA ClearTrust*
- *Oracle Identity Manager Connector Guide for SAP CUA*
- *Oracle Identity Manager Connector Guide for SAP Employee Reconciliation*
- *Oracle Identity Manager Connector Guide for SAP Enterprise Portal*
- *Oracle Identity Manager Connector Guide for SAP User Management*
- *Oracle Identity Manager Connector Guide for Sun Java System Directory*
- *Oracle Identity Manager Connector Guide for UNIX SSH*
- *Oracle Identity Manager Connector Guide for UNIX Telnet*

## Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 9.0.1 connector documentation set, visit Oracle Technology Network at

<http://www.oracle.com/technology/documentation/index.html>

## Conventions

The following text conventions are used in this document:

<b>Convention</b>	<b>Meaning</b>
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	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 password synchronization module and documentation for Microsoft Active Directory in release 9.0.2 of the Oracle Identity Manager connector pack.

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

- [Software Updates](#)  
These include updates made to the connector software.
- [Documentation-Specific Updates](#)  
These include major changes made to the connector documentation. These changes are not related to software updates.

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

## Software Updates

This section discusses the following software updates implemented in this release of the connector.

### **Incorporation of Multilanguage Support**

In addition to English, this release of the connector supports the French and Japanese languages.

### **Change in Postinstallation Message**

The postinstallation message that prompts you to copy Oracle Identity Manager JAR files to the Microsoft Active Directory server has been changed to the following:

Please copy all the jar files from the Oracle Identity Manager installation's lib directory to <drive>:\<folder name>\adsynch\lib.

### **Additions to the Known Issues List**

The Known Issues list in [Chapter 5](#) contains an item explaining that password synchronization fails if you install the password synchronization module on a mapped device.

## Documentation-Specific Updates

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

- Step 4 has been added in the "[Step 2: Enabling Password Policies for Active Directory](#)" section on page 2-2.
- Steps 1 and 2 of the procedure described in the "[Step 4: Performing Postinstallation Steps for the Password Synchronization Module](#)" section on page 2-5 have been combined into a single step.
- In [Chapter 4, "Removing the Password Synchronization Module"](#):
  - The instruction for Microsoft Active Directory 2000 has been added to Step 2 of the procedure.
  - Step 4 has been added.

---



---

# 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](#)
- [Files and Directories That Comprise the Password Synchronization Module](#)

## 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

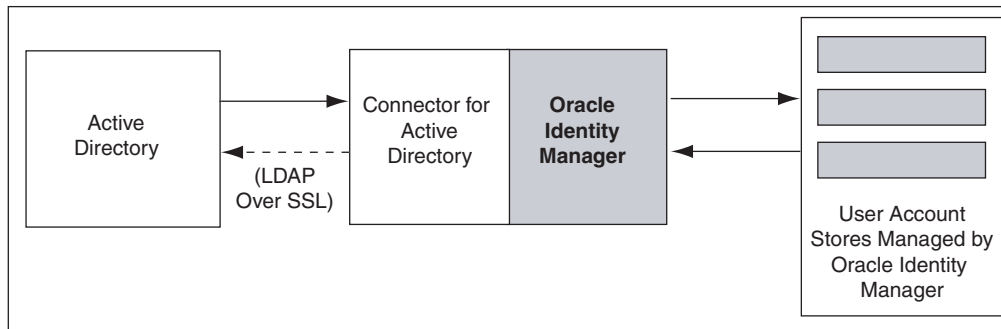
Depending on your specific needs, you can deploy one or both of these components to connect Oracle Identity Manager and Microsoft Active Directory. Deployed together (along with LDAP over SSL), the connector and the password synchronization module provide full, bidirectional synchronization of all user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

The following table compares the functionality offered by both tools.

Functionality	Module	Connector
Updates Microsoft Active Directory with user account attributes (except for passwords) changed by Oracle Identity Manager	No	Yes
Updates Oracle Identity Manager with user account attributes (except for passwords) changed by 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

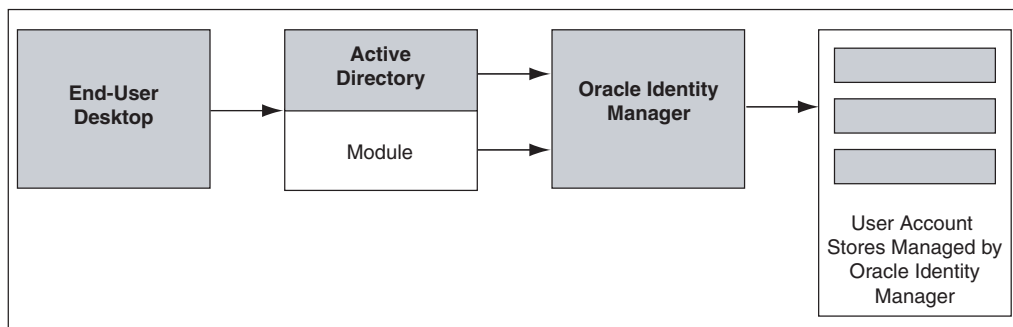
The connector for Microsoft Active Directory updates user account attributes bidirectionally. However, passwords are updated only when the password is changed through Oracle Identity Manager, and not when it is changed through Microsoft Active Directory.

The following figure illustrates the functionality of the connector for Microsoft Active Directory.



The password synchronization module for Microsoft Active Directory updates Oracle Identity Manager with passwords changed in Microsoft Active Directory.

The following figure illustrates the functionality of the password synchronization module for Microsoft Active Directory.



## 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 Rev 4.5.0.zip

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 jpcclient\lib directory	These are password synchronization library files.

<b>File in the Installation Media Directory</b>	<b>Description</b>
Files in the <code>x1home\ext</code> directory	These are external JAR files.
Files in the <code>x1home\install</code> directory	These JAR files are required by the password synchronization module installer.
<code>docs\B32179_01.pdf</code>	This guide, which provides instructions to deploy the connector.



---

---

# 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 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 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 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 and Upgrade Guide for JBoss*

*Oracle Identity Manager Installation and Upgrade Guide for WebLogic*

*Oracle Identity Manager Installation and Upgrade Guide for WebSphere*

*Oracle Identity Manager Installation and Upgrade Guide for Oracle Containers for J2EE*

- 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: <ul style="list-style-type: none"><li>■ Microsoft Windows 2000 with Service Pack 4 or later</li><li>■ Microsoft Windows Server 2003</li></ul>

---

---

**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 ZIP file on the installation media:

Directory Servers\Microsoft Active Directory\Microsoft Active Directory Password Sync Rev 4.5.0.zip

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 Active Directory

To enable password policies for Active Directory:

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 <i>not</i> supported.
BEA WebLogic	Sun JRE 1.4.2_09 or later	However, all versions of Sun JRE 1.5 are <i>not</i> 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

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 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

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.

## 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
<i>Windows_System32_Directory\Adsync.dll</i>	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 <code>ChangePassword.cmd</code> .
<i>ADSYNC_HOME\config\xlconfig.xml</i>	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 " <a href="#">Step 5: Configuring the Password Synchronization Module</a> " section on page 2-6.
<i>ADSYNC_HOME\lib\xliADSync.jar</i>	This JAR file contains the class files required by the Change Password script.
<i>ADSYNC_HOME\ChangePassword.cmd</i>	This script, which is called by <code>adsync.dll</code> in response to a password change, uses the required classpath and command-line parameters to call the <code>ChangePassword</code> class, which is in the <code>xliADSync.jar</code> file.
<i>ADSYNC_HOME\wsChangePassowrd.cmd</i>	This is the version of the Change Password script that is used by IBM WebSphere.
<i>ADSYNC_HOME\lib\xliADSync.ear</i>	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

Perform the following postinstallation 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. Depending on the application server that is used, copy one of the following files to the *ADSYNC\_HOME\ext* directory:
  - *JBoss\_home\client\jbossall-client.jar* (for JBoss Application Server)
  - *BEAWebLogic\_home\weblogic81\server\lib\weblogic.jar* (for BEA WebLogic)
3. 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.

4. If you plan to run Oracle Identity Manager on a clustered application server, then:
  - a. Establish a trust relationship between the computer hosting Oracle Identity Manager and the computer hosting the Active Directory domain controller on which you install the password synchronization module.
  - b. Add the host name of the computer hosting Oracle Identity Manager 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 `<java.naming.provider.url>` tag to the value stored in the tag in the `xlconfig.xml` file associated with the instance of the Design Console that you previously installed as part of the Oracle Identity Manager deployment.

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>	<p>The <code>MatchingMethod</code> parameter specifies how Oracle Identity Manager matches an Oracle Identity Manager user to the Active Directory ID passed to the <code>adsync.dll</code> 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.</p> <ul style="list-style-type: none"> <li>▪ <b>UserID:</b> The Active Directory user ID matches the Oracle Identity Manager user login.</li> <li>▪ <b>UDF:</b> The Active Directory user ID matches the UDF specified in the <code>&lt;FieldName&gt;</code> attribute.</li> <li>▪ <b>ResourceField:</b> The Active Directory user ID matches the <code>&lt;FieldName&gt;</code> attribute in the process form of the Oracle Identity Manager user to whom a resource object specified by the <code>&lt;ResourceObject&gt;</code> attribute is provisioned.</li> </ul>
<Result> </Result>	<p>This optional configuration element specifies where the result of the password change operation must be logged (apart from the <code>adsync.log</code> file). Values for the following parameters are provided as tags within the <code>&lt;Result&gt;</code> tag:</p> <ul style="list-style-type: none"> <li>▪ <b>UpdateUDF:</b> Set to <code>True</code> or <code>False</code> to update a status field in the Users form.</li> <li>▪ <b>FieldName:</b> Specify a field name when the <code>UpdateUDF</code> tag is set to <code>True</code>. For example, <code>FieldName</code> can be <code>USR_UDF_STATUS</code>.</li> <li>▪ <b>FailureValue:</b> This string goes into the status field if the password reset operation fails.</li> <li>▪ <b>SuccessValue:</b> This string goes into the status field if the password reset operation succeeds.</li> <li>▪ <b>AppendTimeStamp:</b> Set this to <code>True</code> or <code>False</code> to append a timestamp to the string in the status field.</li> </ul>

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.

---

## 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 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 2-5 to copy the required files from the computer hosting Oracle Identity Manager to the computer on which you install the password synchronization module.





---

## 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.



---

---

## Known Issues

The following are known issues associated with this release of the password synchronization module:

- Password synchronization fails if you install the password synchronization module on a mapped device. However, there is a workaround for this problem.



---

---

# Index

## B

---

BEA WebLogic, 2-2, 2-4

## C

---

components, 1-1, 1-2, 2-5  
configuring, 2-6

## D

---

deinstalling, 4-1  
deploying, 2-1

## F

---

files and directories, 1-2  
functionality, 1-1

## I

---

IBM WebSphere, 2-4  
installation  
  files, 2-5  
  media, 2-2  
  ZIP file, 2-2  
installing, 2-3  
issues, 5-1

## J

---

JBoss Application Server, 2-2, 2-4

## L

---

LDAP, 1-1

## O

---

operating systems supported, 2-2

## P

---

password policies, 2-2  
postdeployment, 2-5, 2-6  
postinstallation, 2-5  
predeployment steps, 2-1

preinstallation steps, 2-1  
problems, 5-1

## R

---

removing, 4-1

## S

---

SSL, 1-1  
supported operating systems, 2-2

## U

---

upgrading, 3-1

## Z

---

ZIP file on installation media, 2-2

