

Oracle® Identity Manager

Connector Guide for Microsoft Active Directory Password
Synchronization

Release 9.1.1

E11218-06

July 2009

Oracle Identity Manager Connector Guide for Microsoft Active Directory Password Synchronization,
Release 9.1.1

E11218-06

Copyright © 2009, Oracle and/or its affiliates. All rights reserved.

Primary Author: Alankrita Prakash

Contributing Authors: Debapriya Datta, Devanshi Mohan, Lyju Vadassery

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. 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, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Contents

Audience.....	ix
Documentation Accessibility	ix
Related Documents	x
Documentation Updates	x
Conventions	x
Software Updates	xi
Documentation-Specific Updates.....	xiv

1 About the Connector

1.1	Connectors for Microsoft Active Directory	1-1
1.2	Guidelines on Using the Connector	1-3
1.3	Connector Architecture.....	1-4
1.3.1	Password Synchronization Process.....	1-4
1.3.1.1	First SPML Request Rejected	1-6
1.3.1.2	First SPML Request Accepted.....	1-6
1.3.1.3	Oracle Identity Manager Is Not Available.....	1-8
1.3.2	Password Synchronization Connector in a Multi-Domain Controller Environment	1-9
1.4	Roadmap for Deploying and Using the Connector	1-9

2 Deploying the Connector

2.1	Preinstallation.....	2-1
2.1.1	Verifying Deployment Requirements.....	2-1
2.2	Installation	2-1
2.2.1	Installing the Connector.....	2-2
2.2.2	Reconfiguring the Connector	2-8
2.3	Postinstallation	2-11
2.3.1	Enabling and Disabling Logging.....	2-12
2.3.2	Configuring the IT Resource for the Target System	2-13
2.3.2.1	Specifying a Value for the Allow Password Provisioning Parameter	2-15
2.3.3	Enabling the Strong Password Authentication (Password Complexity) Feature of Microsoft Active Directory	2-15
2.3.4	Configuring SSL.....	2-16
2.3.4.1	Configuring SSL on IBM WebSphere Application Server.....	2-16
2.3.4.1.1	Exporting the Certificate	2-16
2.3.4.1.2	Importing the Certificate	2-17
2.3.4.1.3	Additional Configuration Steps	2-18

2.3.4.2	Configuring SSL on JBoss Application Server	2-18
2.3.4.2.1	Generating Keys	2-19
2.3.4.2.2	Signing the Certificate	2-19
2.3.4.2.3	Exporting the Certificate	2-19
2.3.4.2.4	Importing the Certificate	2-20
2.3.4.2.5	Configuring the server.xml File	2-20
2.3.4.3	Configuring SSL on Oracle Application Server	2-21
2.3.4.3.1	Enabling SSL for HTTP Communication to Oracle HTTP Server	2-21
2.3.4.3.2	Exporting the Certificate	2-22
2.3.4.3.3	Importing the Certificate	2-23
2.3.4.4	Configuring SSL on Oracle WebLogic Server	2-23
2.3.4.4.1	Generating Keys	2-24
2.3.4.4.2	Signing the Certificate	2-24
2.3.4.4.3	Exporting the Certificate	2-24
2.3.4.4.4	Configuring Custom Identity Keystore in WebLogic Server	2-25
2.3.4.4.5	Importing the Certificate	2-26

3 Removing the Connector

3.1	Removing an Existing Installation of Release 9.1.0.1	3-1
3.2	Removing an Existing Installation of Release 9.1.1	3-2

4 Known Issues

A Special Characters Supported for Passwords

Index

List of Figures

1-1	Architecture of the Password Synchronization Connector	1-4
1-2	Sequence of Events That Occur During Password Synchronization	1-5
2-1	Installation Directory Page (Installation)	2-2
2-2	Active Directory Configuration Parameters Page (Installation)	2-3
2-3	Second Active Directory Configuration Parameters Page (Installation)	2-4
2-4	Oracle Identity Manager Configuration Parameters Page (Installation)	2-5
2-5	Configuration Parameters Page (Installation)	2-7
2-6	Summary Page (Installation)	2-7
2-7	Active Directory Configuration Parameters (Reconfiguration)	2-9
2-8	Oracle Identity Manager Configuration Parameters Page (Reconfiguration)	2-10
2-9	Configuration Parameters Page (Reconfiguration)	2-10
2-10	Second Active Directory Configuration Parameters Page (Reconfiguration)	2-11
3-1	Summary Page for Removing the Connector	3-2

List of Tables

1-1	Functionality of the User Management and Password Synchronization Connectors.....	1-3
2-1	Certified Deployment Configurations	2-1
2-2	Microsoft Active Directory Configuration Parameters	2-3
2-3	Oracle Identity Manager Configuration Parameters	2-5

Preface

This guide discusses the connector that is used to propagate password changes from Microsoft Active Directory to Oracle Identity Manager.

Audience

This guide is intended for resource administrators and target system integration teams.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. 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.

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at <http://www.fcc.gov/cgb/consumerfacts/trs.html>, and a list of phone numbers is available at <http://www.fcc.gov/cgb/dro/trsphonebk.html>.

Related Documents

For generic information about connectors, see *Oracle Identity Manager Connector Concepts* in the Oracle Identity Manager Connectors documentation library.

To access the Oracle Identity Manager documents mentioned as references in this guide, visit Oracle Technology Network. The following Oracle Technology Network page provides links to Oracle Identity Manager documentation:

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

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connectors 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.
<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 Oracle Identity Manager Connector for Microsoft Active Directory Password Synchronization?

This chapter provides an overview of the updates made to the software and documentation of the Microsoft Active Directory Password Synchronization connector in release 9.1.1.

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

- [Software Updates](#)

This section describes updates made to the connector software. This section also points out the sections of this guide that have been changed in response to each software update.

- [Documentation-Specific Updates](#)

This section describes major changes made to this guide. For example, the relocation of a section from the second chapter to the third chapter is a documentation-specific update. These changes are not related to software updates.

Software Updates

The following sections discuss software updates:

- [Software Updates in Release 9.1.0](#)
- [Software Updates in Release 9.1.0.1](#)
- [Software Updates in Release 9.1.1](#)

Software Updates in Release 9.1.0

The following are software updates in release 9.1.0:

- [Support for 32-Bit and 64-Bit Microsoft Windows](#)
- [Oracle Identity Manager Flag Field for Tracking Password Changes Is Automatically Created](#)
- [Support for Signature-Based Authentication](#)

Support for 32-Bit and 64-Bit Microsoft Windows

The password synchronization connector has separate installers for Microsoft Active Directory running on 32-bit and 64-bit Microsoft Windows.

Oracle Identity Manager Flag Field for Tracking Password Changes Is Automatically Created

An Oracle Identity Manager flag field is used to track password changes propagated by the connector. In earlier releases, you had to manually create this field in Oracle Identity Manager. From this release onward, the field is automatically created in Oracle Identity Manager when you install the Microsoft Active Directory User Management connector.

Support for Signature-Based Authentication

The password synchronization connector supports signature-based authentication. This is an alternative to password-based authentication for connecting to Oracle Identity Manager during password synchronization operations.

Information specific to signature-based authentication has been provided at various places in this guide.

Software Updates in Release 9.1.0.1

The following is a software update in release 9.1.0.1:

- [Single Installer for Both 32-Bit and 64-Bit Microsoft Windows](#)

Single Installer for Both 32-Bit and 64-Bit Microsoft Windows

A single installer has been developed for Microsoft Active Directory running on 32-bit and 64-bit Microsoft Windows. Corresponding changes have been made in this release of the guide.

Software Updates in Release 9.1.1

The following are software updates in release 9.1.1:

- [Architecture of the Connector Has Been Modified](#)
- [No Dependency on the Microsoft Active Directory User Management Connector](#)
- [Support for Password Propagation through SPML Web Service](#)
- [Support for Storing Configuration Parameters in the Registry](#)
- [Support for Retrying Password Propagation when Oracle Identity Manager is not Available](#)
- [No Requirement for Creating an Attribute in Microsoft Active Directory to Track Password Changes](#)
- [No Requirement for Reinstalling the Connector if the Account Used by the Connector for Logging in to Oracle Identity Manager is Changed](#)
- [Resolved Issues](#)
- [Additions to the List of Known Issues](#)

Architecture of the Connector Has Been Modified

The architecture of the password synchronization connector has been completely modified. Major changes made in the new, fault-tolerant architecture of the connector are discussed in the subsequent sections.

No Dependency on the Microsoft Active Directory User Management Connector

In earlier releases, you had to install the Microsoft Active Directory User Management connector before you could start using the password synchronization connector. From

this release onward, the password synchronization connector does not use any component of the user management connector. At the same time, password propagation from Microsoft Active Directory to Oracle Identity Manager can be configured to complement the features offered by the user management connector.

Support for Password Propagation through SPML Web Service

In earlier releases, the connector used the Oracle Identity Manager APIs for password propagation from Active Directory to Oracle Identity Manager. From this release onward, the connector uses SPML Web service for password propagation to Oracle Identity Manager.

Support for Storing Configuration Parameters in the Registry

The connector stores all configuration parameters of the connector in the Microsoft Windows Registry. This enables you to reconfigure the configuration parameters without reinstalling the connector. This feature also replaces the xlconfig.xml file that was used to store configuration parameters in earlier releases.

See ["Reconfiguring the Connector"](#) on page 2-8 for more information.

Support for Retrying Password Propagation when Oracle Identity Manager is not Available

In the earlier releases, if Oracle Identity Manager was not available, then the connector did not retry propagating the password to Oracle Identity Manager. From this release onward, the connector retries password propagation if Oracle Identity manager is not available.

See ["Connector Architecture"](#) on page 1-4 for more information.

No Requirement for Creating an Attribute in Microsoft Active Directory to Track Password Changes

In earlier releases, the connector required an attribute to be created in Microsoft Active Directory to act as a flag for tracking password changes initiated by Oracle Identity Manager. From this release onward, this attribute is not required.

No Requirement for Reinstalling the Connector if the Account Used by the Connector for Logging in to Oracle Identity Manager is Changed

In earlier releases, if you had changed the password of the account that the connector used to log in to Oracle Identity Manager during a password synchronization operation, then you had to reinstall the connector with the changed password. From this release onward, you can reconfigure the connector whenever you change the login credentials of the account that the connector uses for logging in to Oracle Identity Manager during a password synchronization operation. This eliminates the need for reinstalling the connector.

See ["Reconfiguring the Connector"](#) on page 2-8 for more information.

Resolved Issues

The following are issues resolved in release 9.1.1:

Bug Number	Issue	Resolution
7276037	IT resource name in the adsynch.log file was not localized.	This issue does not apply for this release of the connector. In this release, the IT resource name is not recorded in the log file.

Bug Number	Issue	Resolution
7272742 and 7293723	After you installed the connector, logging was automatically enabled. You could not disable it. In addition, you could not specify or change or the log level.	This issue has now been resolved. You can now enable and disable logging for the password synchronization connector. See "Enabling and Disabling Logging" on page 2-12 for more information.

Additions to the List of Known Issues

In the ["Known Issues"](#) on page 4-1 chapter, the following item has been added:

Bug 8361237

Information about events that occur during connector installation are recorded in the oimpwdsync.log file, which is located in the %TEMP% directory.

The oimpwdsync.log file is not deleted when you reinstall or reconfigure the password synchronization connector.

Documentation-Specific Updates

Major changes have been made in the structure of the guide. The objective of these changes is to synchronize the guide with the changes made to the connector and to improve the usability of information provided by the guide.

See ["Roadmap for Deploying and Using the Connector"](#) on page 1-9 for detailed information about the organization of content in this guide.

- In the [Deploying the Connector](#) chapter, the "Determining the Release Number of the Connector" section has been removed.
- In the [Known Issues](#) chapter:
 - Bug 7155390 has been removed as the bug had been resolved in release 9.1.0.1 of the connector.
 - Known issue has been added.
- In the ["Verifying Deployment Requirements"](#) section, changes have been made in the "Target systems and target system host platforms" row.

About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with external, identity-aware applications.

Oracle Identity Manager Connector for Microsoft Active Directory Password Synchronization captures passwords changed on the target system and propagates them to Oracle Identity Manager.

This guide discusses the password synchronization connector.

Note:

In this guide:

- Oracle Identity Manager Connector for Microsoft Active Directory Password Synchronization is also referred to as the **connector** or **password synchronization connector**.
 - The Microsoft Active Directory User Management connector is also referred to as the **user management connector**.
 - Microsoft Active Directory is also referred to as the **target system**.
-

This chapter contains the following sections:

- [Connectors for Microsoft Active Directory](#)
- [Guidelines on Using the Connector](#)
- [Connector Architecture](#)
- [Roadmap for Deploying and Using the Connector](#)

1.1 Connectors for Microsoft Active Directory

Oracle Identity Manager provides the following connectors for integration with Microsoft Active Directory:

- The **user management connector** can be configured to run in either the identity reconciliation (trusted source) mode or the account management (target resource) mode.

In the identity reconciliation mode, Microsoft Active Directory is used as the trusted source and users are directly created and modified on it. During reconciliation from the trusted source, the user management connector fetches

data about these target system users into Oracle Identity Manager. This data is used to create or update the corresponding OIM Users.

In the account management mode, Microsoft Active Directory is used as a target resource. During reconciliation from the target resource, the user management connector fetches into Oracle Identity Manager data about users created or modified directly on the target system. This data is used to add or modify resources allocated to OIM Users. In addition, the connector enables provisioning operations through which user data changes are propagated from Oracle Identity Manager to Microsoft Active Directory.

- The **password synchronization connector** propagates password changes from Microsoft Active Directory to Oracle Identity Manager.

Depending on your business requirements, you can deploy one or both of these connectors to integrate Oracle Identity Manager with Microsoft Active Directory.

[Table 1–1](#) describes the functionality of the user management and password synchronization connectors.

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

Table 1–1 Functionality of the User Management and Password Synchronization Connectors

Event	Action Performed by the Connector
Trusted source reconciliation from Active Directory	<p>Only user management connector installed: User data from Active Directory is matched with OIM Users</p> <p>Only password synchronization connector installed: NA</p> <p>Both user management and password synchronization connectors installed: The user management connector propagates user data changes (except for password changes) from Active Directory to the corresponding OIM Users. The password synchronization connector propagates password changes from Active Directory to the corresponding OIM Users.</p>
Target resource reconciliation from Active Directory	<p>Only user management connector installed: User data from Active Directory is matched with the Active Directory resource assigned to OIM Users</p> <p>Only password synchronization connector installed: NA</p> <p>Both user management and password synchronization connectors installed: The user management connector propagates user data changes (except for password changes) from Active Directory to the Active Directory resource assigned to OIM Users. The password synchronization connector propagates password changes from Active Directory to the corresponding OIM Users.</p>
OIM User's password changed	<p>Only user management connector installed and configured for the target resource mode: Depending upon the value of the Allow Password Provisioning IT resource parameter, the user management connector propagates to Active Directory and other resources allocated to the OIM User, password changes made to OIM Users.</p> <p>The Allow Password Provisioning parameter is an IT resource parameter for the user management connector. If you set this parameter to <i>yes</i>, then Oracle Identity Manager propagates the password change to all of the resources allocated (provisioned) to the OIM User. If you set this parameter to <i>no</i>, then Oracle Identity Manager does not propagate the password change to all of the resources allocated (provisioned) to the OIM User.</p> <p>Note: This applies only if pre-populate adapters have been configured to propagate passwords from OIM Users to the resources.</p> <p>Only password synchronization connector installed: NA</p> <p>Both user management (configured for target resource mode) and password synchronization connectors installed: Same as what happens when the user management connector is installed and configured for the target resource mode. The password synchronization connector is not used here as this is a provisioning operation.</p>
Password changed on Active Directory	<p>Only user management connector installed: Passwords changed on Active directory are not propagated to Oracle Identity Manager</p> <p>Only password synchronization connector installed: Passwords changed on Active directory are propagated to Oracle Identity Manager</p> <p>Both user management and password synchronization connectors installed: Passwords changed on Active directory are propagated to Oracle Identity Manager</p>

1.2 Guidelines on Using the Connector

The following are the guidelines on using the connector:

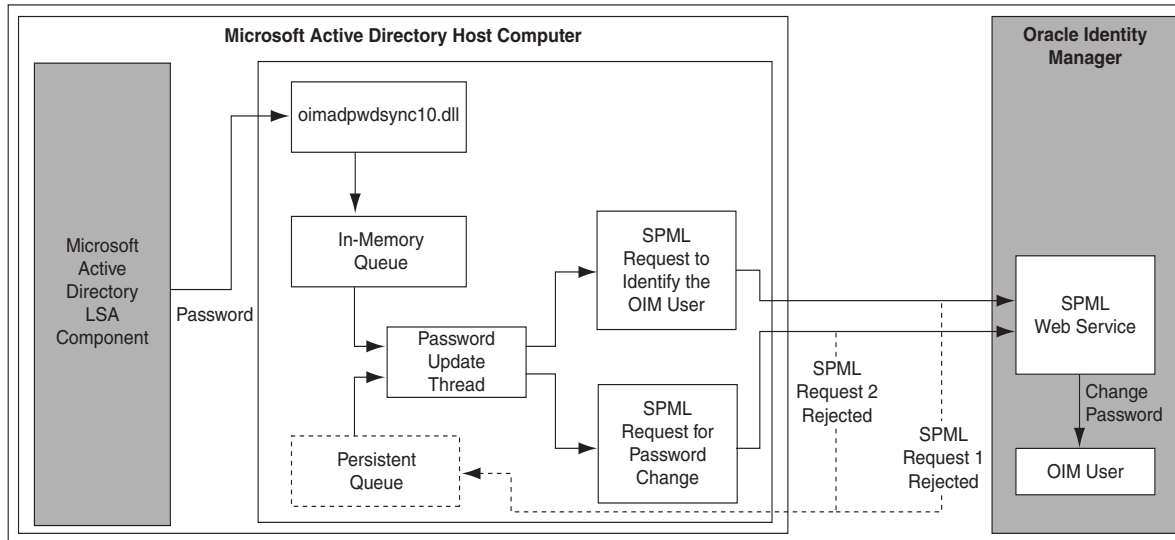
- If Microsoft Active Directory is the only authoritative source for passwords in your operating environment, then it is recommended not to propagate passwords from Oracle Identity Manager to Microsoft Active Directory.
- If Oracle Identity Manager is the only authoritative source for passwords in your operating environment, then *do not* install the password synchronization connector.

- If both Oracle Identity Manager and Microsoft Active Directory can function as authoritative sources for passwords in your operating environment, then the password policies set on Oracle Identity Manager and Microsoft Active Directory must be consistent.

1.3 Connector Architecture

The architecture of the connector is the blueprint for the functionality of the connector. [Figure 1–1](#) shows the architecture of the password synchronization connector.

Figure 1–1 Architecture of the Password Synchronization Connector

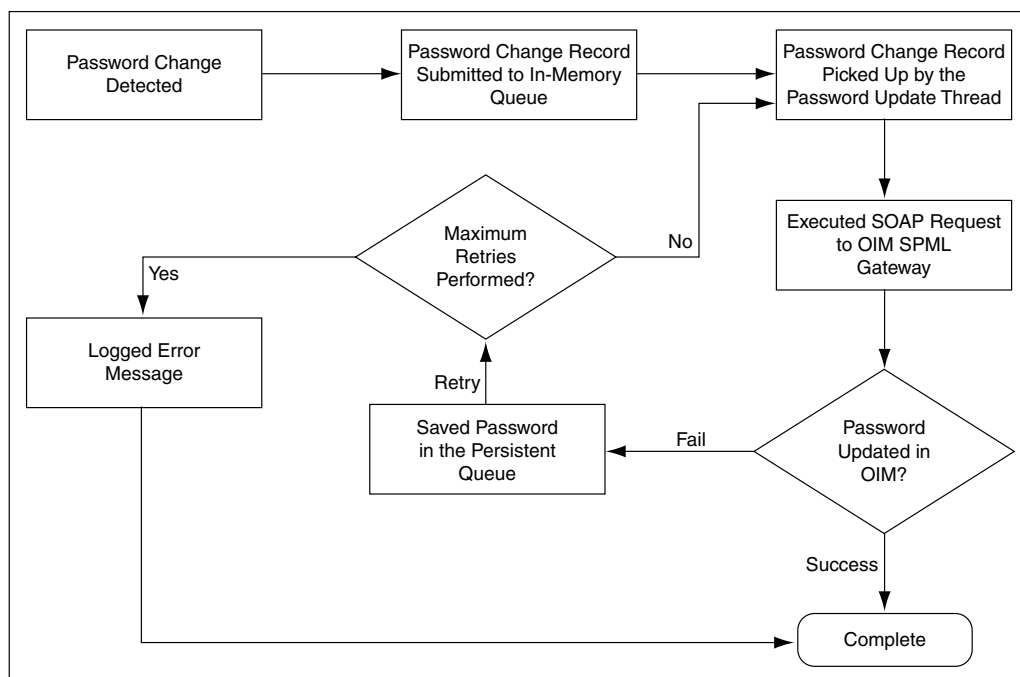


This section discusses the following topics:

- [Password Synchronization Process](#)
- [Password Synchronization Connector in a Multi-Domain Controller Environment](#)

1.3.1 Password Synchronization Process

[Figure 1–2](#) shows the sequence of events that occur when the password is propagated from the target system to Oracle Identity Manager.

Figure 1–2 Sequence of Events That Occur During Password Synchronization

The following is the sequence of events that take place during password synchronization:

1. A user changes the user's password on Microsoft Active Directory. The user can change the password in one of the following ways:
 - Using Microsoft Management Console
 - Pressing Ctrl+Alt+Del and then using the Change Password option on one of the client computers for the Microsoft Active Directory server
 - Using a third-party application or custom utility for changing passwords on Microsoft Active Directory

The password change is successful on Microsoft Active Directory only when the password clears all the password checks on Microsoft Active Directory.

2. The local security authority (LSA) component of Microsoft Windows intercepts the password change on Microsoft Active Directory and passes the password (in plain-text format) and required user information to the password filter (oimadpwdsync10.dll file). The oimadpwdsync10.dll file is one of the files copied to the target system when you install the password synchronization connector.
3. The password filter encrypts the password and user information in a password change record and stores this record in the password change record queue. This queue consists of password change records corresponding to each password change on Microsoft Active Directory. The password change record queue is held in memory, and it is also known as the in-memory queue.
4. The password update thread is created when the password filter is initialized. This thread performs the following tasks:
 - a. Picks up a password change record from the in-memory queue or persistent queue.

Note: The persistent queue is explained later in this section.

- b. Decrypts the password change record.
- c. Creates and sends an SPML request to Oracle Identity Manager in the form of a SOAP packet.

This SPML request contains the sAMAccountName of the target system user whose password must be updated on Oracle Identity Manager. On Oracle Identity Manager, the sAMAccountName value is compared with the OIM User attribute that you specify while installing the connector.

See Also: The "SPML Web Service" chapter in *Oracle Identity Manager Tools Reference* for detailed information about the SPML Web Service

The following sections discuss the processes associated with each event that may occur when the SPML request is sent:

Note: The update of a password on the target system does not depend on acceptance of the password by Oracle Identity Manager or the availability of Oracle Identity Manager.

- [First SPML Request Rejected](#)
- [First SPML Request Accepted](#)
- [Oracle Identity Manager Is Not Available](#)

1.3.1.1 First SPML Request Rejected

Oracle Identity Manager rejects the first SPML request if the corresponding OIM User matching the sAMAccountName of the target system user does not exist. If this event occurs, then the following error message is written to the Application log in the Microsoft Windows Event Log:

Unable to update sAMAccountName, the user does not exist in OIM

In addition, the following error message is written to the *TIME_STAMPOIMMain.log* file:

The user does not exist in OIM

See "[Enabling and Disabling Logging](#)" on page 2-12 for information about the connector log files.

1.3.1.2 First SPML Request Accepted

Oracle Identity Manager accepts the first SPML request if an OIM User matching the sAMAccountName of the target system user is found. After the OIM User is found:

1. The SPML Web service sends a success response to the password update thread.
2. The password update thread sends a second SPML request to the SPML Web service in Oracle Identity Manager. This request contains the password of the OIM User.

The following sections discuss processes associated with each event that may occur when the second SPML request is sent:

- [Second SPML Request Rejected](#)
- [Second SPML Request Accepted](#)
- [Oracle Identity Manager Is Not Available](#)

Second SPML Request Rejected

Oracle Identity Manager rejects the second SPML request for one of the following reasons:

- The password does not meet password policies set on Oracle Identity Manager

Note: Password policies set on the target system may not be consistent with password policies set on Oracle Identity Manager.

- The password contains special characters that are not supported by Oracle Identity Manager.
- The user ID of an OIM User contains characters in the non-native encoding of the Microsoft Active Directory system.

If Oracle Identity Manager rejects the second SPML request, then:

1. In both scenario, the following error message is written to the Application log in the Microsoft Windows Event Log:

Unable to update *USER_NAME_OF_THE_OIM_USER*. The OIM server rejected the setPasswordRequest. Please check the OIM server log for more details.

This error message is also recorded in the *TIME_STAMP*OIMMain.log file. In addition, the exception stack trace is recorded in the debug log file of Oracle Identity Manager. The stack trace provides details about the reason for the password change rejection. See ["Enabling and Disabling Logging"](#) on page 2-12 for information about the connector log files.

2. The SPML Web Service sends an SPML response indicating that the password update operation has failed.
3. The password change record (contains the password along with the user information in encrypted format) is stored in the persistent queue. This queue is located in the *ou=oimpwdsyncDOMAIN_NAME,BASE_DN* container of Microsoft Active Directory.
4. The password update thread increments the retry count for the password change record by one and resends SPML requests to Oracle Identity Manager.

Note: A value for the retry count is specified during connector installation.

5. If Oracle Identity Manager accepts the password change, then the password change record is removed from the persistent queue. The rest of the steps mentioned in this section are not performed.
6. If Oracle Identity Manager rejects the password change, then the password update thread keeps resending SPML requests until the retry count reaches the maximum number of retries.

If Oracle Identity Manager becomes unavailable after it rejects the password and before the maximum number of retries for a rejected password is reached, then:

- The password along with user information is stored in the persistent queue in encrypted format.
 - The password update thread attempts to update the password of the corresponding OIM User without incrementing the retry count. When Oracle Identity Manager becomes available, this retry attempt continues and the retry count resumes incrementing from this point onward.
7. When the retry count reaches the maximum number of retries:
- The password change record is deleted from the persistent queue.
 - The following error message is written to the Application log in the Microsoft Windows Event Log:

```
Unable to update USER_NAME_OF_THE_OIM_USER. The OIM server rejected the
setPasswordRequest. Please check the OIM server log for more details.
```

This error message is also recorded in the *TIME_STAMPOIMMain.log* file. In addition, the exception stack trace is recorded in the debug log file of Oracle Identity Manager. The stack trace provides details about the reason for the password change rejection. See ["Enabling and Disabling Logging"](#) on page 2-12 for information about the connector log file.

Second SPML Request Accepted

If Oracle Identity Manager accepts the second SPML request (containing the password change), then the password of the OIM User is updated successfully. The process ends here.

Oracle Identity Manager Is Not Available

See ["Oracle Identity Manager Is Not Available"](#) on page 1-8 for information about events that occur if Oracle Identity Manager is not available after the response to the first SPML request is received and before the second SPML request is sent.

1.3.1.3 Oracle Identity Manager Is Not Available

If Oracle Identity Manager is not available at the start of the password synchronization operation, then:

1. The following error message is written to the Application log in the Microsoft Windows Event Log:

```
Unable to update sAMAccountName. The OIM SPML Web Service is unreachable.
Please verify the availability of the web service or the configuration
parameters.
```

This error message is also recorded in the *TIME_STAMPOIMMain.log* file.

2. The password along with the user information is encrypted and stored in the persistent queue.
3. The password update thread picks up the password change record from the persistent queue and resends SPML requests to Oracle Identity Manager (without incrementing the retry count).
4. As long as Oracle Identity Manager is not available, Steps 2 and 3 are repeated until the first SPML request is sent to Oracle Identity Manager.

5. When Oracle Identity Manager becomes available, the first SPML request is sent. The next set of steps depends on which of the following events takes place:
 - [First SPML Request Rejected](#)
 - [First SPML Request Accepted](#)

1.3.2 Password Synchronization Connector in a Multi-Domain Controller Environment

In a multi-domain controller environment, if one of the domain controllers is unavailable and if a Password Change request is sent to it, then the Password Change request is re-routed to a domain controller that is available. The domain controller that is available then sends the password to the OIM User.

Note: The Password Change request that is stored in the memory queue of a domain controller is lost if that domain controller crashes. If this happens, then the Password Change request cannot be retrieved.

The following example illustrates how the connector works in a multi-domain controller environment:

Suppose the operating environment consists of two domain controllers, DC1 and DC2. If DC1 becomes unavailable and a user for example, John Doe, changes his password on the target system, then the connector on DC2 propagates the new password to the corresponding OIM User.

1.4 Roadmap for Deploying and Using the Connector

The following is the organization of information in the rest of this guide:

- [Chapter 2, "Deploying the Connector"](#) describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- [Chapter 3, "Removing the Connector"](#) describes the procedure to uninstall the connector.
- [Chapter 4, "Known Issues"](#) lists known issues associated with this release of the connector.
- [Appendix A, "Special Characters Supported for Passwords"](#) provides information about special characters that you can use in the Password field on the target system and Oracle Identity Manager.

Deploying the Connector

The procedure to deploy the connector can be divided into the following stages:

- [Preinstallation](#)
- [Installation](#)
- [Postinstallation](#)

2.1 Preinstallation

Preinstallation for the connector involves performing the procedure described in the following section.

2.1.1 Verifying Deployment Requirements

Before you install the connector, you must ensure that the following deployment requirements are addressed:

- The computer on which you are installing the connector meets the requirements listed in [Table 2–1](#).

Table 2–1 *Certified Deployment Configurations*

Item	Requirement
Target systems and target system host platforms	<p>The target system can be any one of the following:</p> <ul style="list-style-type: none">■ Microsoft Windows Server 2003 Active Directory installed on Microsoft Windows Server 2003 with SP2 and later service packs (x86 or x64)■ Microsoft Windows Server 2008 Active Directory installed on Microsoft Windows Server 2008 with SP2 and later service packs (x86 or x64)
	<ul style="list-style-type: none">■ An instance of Oracle Identity Manager release 9.1.0.0 or later along with the SPML Web service is installed, running, and accessible from the computer hosting the Microsoft Active Directory domain controller on which you want to install the connector.■ The target system host computer must be able to ping the application server host using both IP address and host name.

2.2 Installation

This section discusses the following topics:

- [Installing the Connector](#)
- [Reconfiguring the Connector](#)

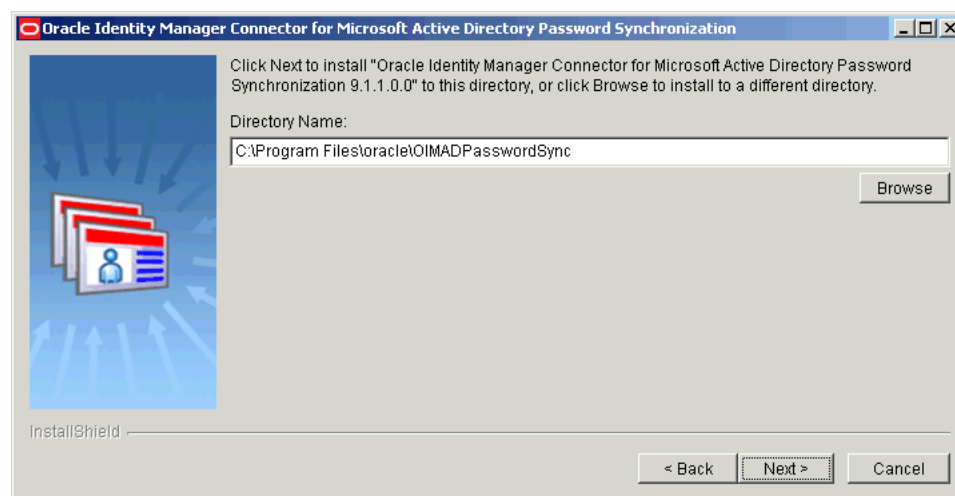
2.2.1 Installing the Connector

To install the connector:

1. On the Microsoft Active Directory host computer, run the installer as follows:
 - a. Copy the contents of the installation media to a temporary directory.
 - b. In the temporary directory, run the setup.exe file to start the installer.
2. On the Welcome page, click **Next**.
3. On the next page, click **Next**.
4. On the Installation Directory page, you can either accept the default installation directory or use the **Browse** button to specify the directory in which you want install the connector.

[Figure 2–1](#) shows the Installation Directory page.

Figure 2–1 Installation Directory Page (Installation)



5. Click **Next**.

If the installation directory that you specify (in the preceding step) exists, then the installer confirms if you want to overwrite the directory. Otherwise, the installer creates the installation directory.

6. On the Active Directory Configuration Parameters page, which displays the configuration parameters for Microsoft Active Directory, verify the values displayed in all fields.

If the values displayed on this page do not match the values for your current installation of Microsoft Active Directory, then change these values accordingly. Otherwise, you can proceed to the next step.

[Figure 2–2](#) shows the Active Directory Configuration Parameters page on which sample values have been specified.

Figure 2–2 Active Directory Configuration Parameters Page (Installation)

Table 2–2 describes each configuration parameter of Microsoft Active Directory.

Table 2–2 Microsoft Active Directory Configuration Parameters

Parameter	Description
Domain	Enter the domain name for the Microsoft Active Directory domain controller on which the connector is being installed. This value is typically the DNS domain name. Sample value: <code>example.com</code>
BaseDN	Enter the base DN of Microsoft Active Directory. This is the container where the connector searches for entries with changed passwords. The persistent queue, which is an <code>organizationUnit</code> , will be created within this container. Therefore, the base DN that you specify must be capable of holding <code>organizationalUnit</code> objects. Sample value: <code>DC=example,DC=com</code>
Port	Enter the port number at which LDAP for Microsoft Active Directory host computer is enabled. Default value: 389
Host	Enter the IP address (<i>not</i> the host name) of the Microsoft Active Directory host computer. Sample value: <code>172.20.55.120</code>

7. Click **Next**.
8. On the second Active Directory Configuration Parameters page, enter values for the following fields:
 - **User:** Enter the user name of an account that belongs to the Administrators group.
You can use any one of the following formats to enter the user name:
 - `USER_LOGIN@DOMAIN.COM`
 - `cn=USER_LOGIN,cn=USERS,dc=DOMAIN,dc=com`

Sample values:

john_doe@example.com

cn=admin, cn=Users, dc=example, dc=com

- **User Password:** Enter the password of the account that you entered in the **User** field.
- **Log File Path:** Enter the path to the directory where the log files must be generated.

Default value: `INSTALLATION_DIRECTORY\Logs`

`INSTALLATION_DIRECTORY` is the directory that you specify in Step 4.

See ["Enabling and Disabling Logging"](#) on page 2-12 for information about logging.

[Figure 2-3](#) shows the Microsoft Active Directory Information page on which sample values have been specified.

Figure 2-3 Second Active Directory Configuration Parameters Page (Installation)

9. Click **Next** to proceed with installation.
10. On the Oracle Identity Manager Configuration Parameters page, specify values for the configuration parameters of Oracle Identity Manager.

[Figure 2-4](#) displays the Oracle Identity Manager Configuration Parameters page on which sample values have been specified.

Figure 2–4 Oracle Identity Manager Configuration Parameters Page (Installation)

Oracle Identity Manager Configuration Parameters

Oracle Identity Manager Configuration Parameters
All fields marked with * are mandatory

Host*

oimhost

Port*

8080

Administrator Login*

admin

Administrator Password*

OIM User Attribute*

Users.User ID

OIM Application Server Type*

Weblogic

Use SSL*

☐ Yes

☒ No

Client Certificate Subject Name

InstallShield

< Back Next > Cancel

Table 2–3 describes each configuration parameter of Oracle Identity Manager.

Table 2–3 Oracle Identity Manager Configuration Parameters

Parameter	Description
Host	<p>Enter the host name (<i>not</i> the IP address) of the computer hosting Oracle Identity Manager.</p> <p>Note: The host name must be accessible from the Microsoft Active Directory host computer.</p> <p>Sample value: oimhost</p>
Port	<p>Enter the number of the port at which the Oracle Identity Manager SPML Web service is listening.</p> <p>Sample value: 8080</p>
Administrator Login	<p>Enter the user name of the account that will be used by the connector to login to Oracle Identity Manager during a password synchronization operation. This account must have the permissions required to change the password of OIM Users.</p>
Administrator Password	<p>Enter the password of the account that will be used by the connector to login to Oracle Identity Manager during a password synchronization operation.</p>

Table 2–3 (Cont.) Oracle Identity Manager Configuration Parameters

Parameter	Description
OIM User Attribute	<p>Enter the Metadata Column Code of the column in the USR table that you want to use to match OIM Users with users in the target system. During password synchronization, the sAMAccountName value of the user whose password is changed is compared against values in this column.</p> <p>Sample value (for predefined OIMUser fields): <code>Users.User ID</code></p> <p>For user-defined OIMUser fields, you can use the <code>USR_UDF_FIELD_NAME</code> format.</p> <p>Sample Value: <code>USR_UDF_USERNAME</code></p> <p>See the "Metadata Column Codes" appendix in <i>Oracle Identity Manager API Usage Guide</i> for information about the mapping between the physical column names and metadata column codes.</p>
OIM Application Server Type	<p>Select the name of the application server that hosts Oracle Identity Manager.</p> <p>Sample value: <code>JBoss</code></p>
Use SSL	<p>Select Yes, if you are going to configure SSL communication between Microsoft Active Directory and Oracle Identity Manager. Otherwise, select No .</p> <p>Default value: <code>Yes</code></p> <p>Note: It is recommended that you configure SSL to secure the transfer of SOAP messages from the target system to Oracle Identity Manager. See "Configuring SSL" on page 2-16 for information about enabling SSL.</p>
Client Certificate Subject Name	<p>Enter a value for this parameter only if <code>Use SSL</code> parameter has been set to <code>Yes</code> and client authentication is required by the application server.</p> <p>Enter a string that identifies the client certificate that must be used for SSL.</p> <p>Sample value: <code>TQL17</code></p> <p>Here, <code>TQL17</code> is the Issued To value in the certificate.</p>

11. Click Next.

12. On the Configuration Parameter Information page, enter values for the following fields:

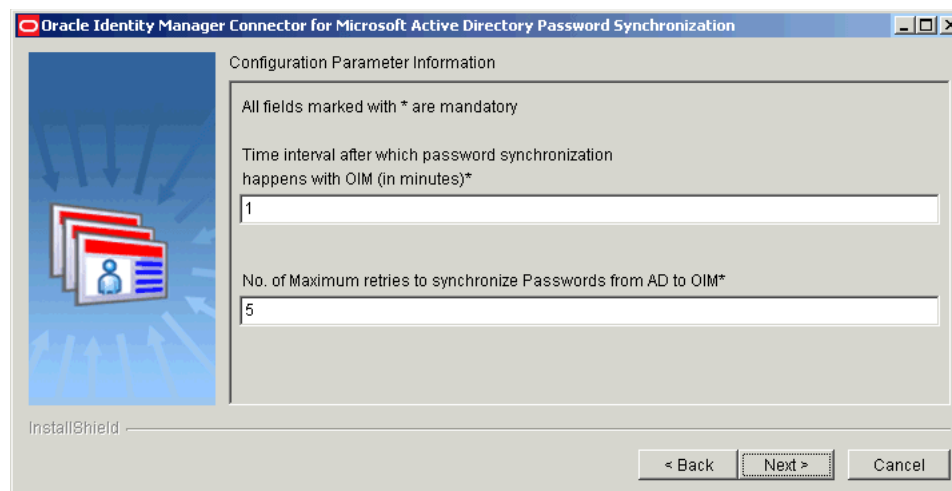
- **Time interval after which password synchronization happens with OIM (in minutes):** Enter an integer value in this field. This value represents the number of minutes the connector sleeps between processing password change events. The connector goes into the sleep mode after processing all the change events from the in-memory and persistent queues.

Default value: 1

- **No. of maximum retries to synchronize passwords from AD to OIM:** Enter an integer value. This value represents the number of times the connector tries to propagate the password before removing the password change record from the persistent queue.

Default value: 5

[Figure 2–5](#) is a screenshot of the Connector Configuration Parameters page on which sample values have been specified.

Figure 2–5 Configuration Parameters Page (Installation)

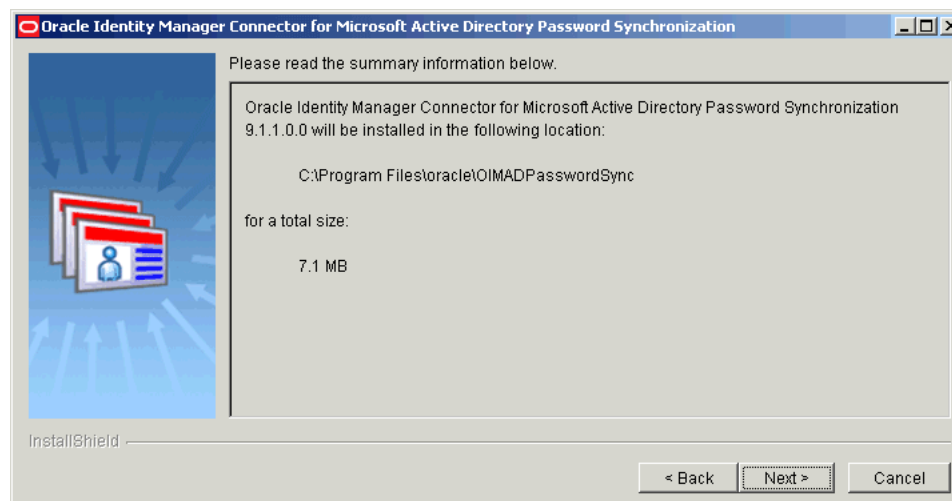
13. Click **Next**.

14. On the Summary Page, verify that the installation directory for the connector is displayed correctly and then click **Next** to install the connector.

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

Figure 2–6 shows the Summary page.

Note: If you are installing the connector on a 64-bit Microsoft Windows operating system, then before you proceed to the next step, copy the oimadpwdsync10.dll and orclmessages.dll files from the Windows\SysWOW64 directory to the WINDOWS\system32 directory.

Figure 2–6 Summary Page (Installation)

15. On the next page, click **Next** to restart your computer

You must restart the computer to initialize the oimadpwdsync10.dll file. If the oimadpwdsync10.dll file is not initialized, then the connector is not ready for propagating passwords changes from target system to Oracle Identity Manager.

Ensuring that the Connector is Ready for Propagating Passwords

In order to ensure that the connector is ready for propagating password changes from target system to Oracle Identity Manager, you must check if the oimadpwdsync10.dll file has been initialized.

To verify whether the oimadpwdsync10.dll file is initialized:

1. Enable logging for the *TIME_STAMPOIMMain.log* file by performing the procedure described in ["Enabling and Disabling Logging"](#) on page 2-12.
2. Check if the *TIME_STAMPOIMMain.log* file is generated in the path specified in the Log File Path field while performing Step 8 of ["Installing the Connector"](#) on page 2-2.

If the *TIME_STAMPOIMMain.log* file is generated, then the oimadpwdsync10.dll file is initialized. Otherwise, you must reinstall the connector.

2.2.2 Reconfiguring the Connector

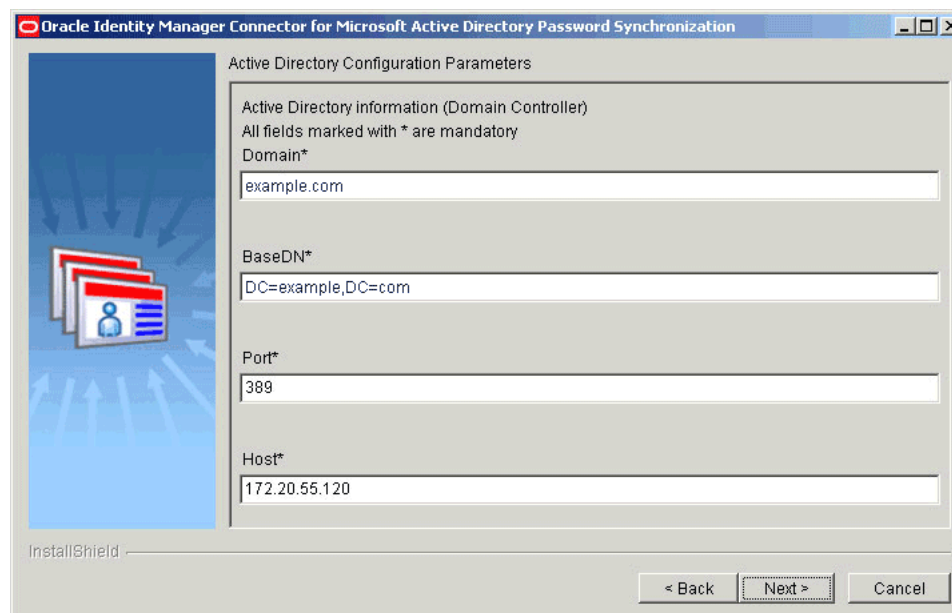
During connector installation, you specify a set of values for the configuration parameters of Microsoft Active Directory, Oracle Identity Manager, and the connector. After connector installation, if you want to change the values for any of the configuration parameters, then you must perform the procedure described in this section.

To reconfigure the connector:

1. On the Microsoft Active Directory host computer, run the setup.exe file located in the temp directory.
2. On the Welcome page, click **Next**.
3. On the Active Directory Configuration Parameters page, if required, modify values for any or all of the following parameters:
 - **Domain**
 - **BaseDN**
 - **Port**
 - **Host**

[Figure 2-2](#) shows the Active Directory Configuration Parameters page on which sample values have been specified.

Figure 2–7 Active Directory Configuration Parameters (Reconfiguration)



The screenshot shows a window titled "Oracle Identity Manager Connector for Microsoft Active Directory Password Synchronization". The main area is titled "Active Directory Configuration Parameters" and contains the following fields:

- Active Directory information (Domain Controller)**
All fields marked with * are mandatory
- Domain***: example.com
- BaseDN***: DC=example,DC=com
- Port***: 389
- Host***: 172.20.55.120

At the bottom, there are three buttons: "< Back", "Next >", and "Cancel". The "Next >" button is highlighted. The "InstallShield" logo is visible in the bottom left corner.

4. Click **Next**.
5. On the Oracle Identity Manager Configuration Parameters page, if required, modify values for any or all of the following parameters:
 - **Host**
 - **Port**
 - **OIM User Attribute**
 - **OIM Application Server Type**
 - **Use SSL**
 - **Client Configuration Subject Name**

Figure 2–4 displays the Oracle Identity Manager Configuration Parameters page on which sample values have been specified.

Figure 2–8 Oracle Identity Manager Configuration Parameters Page (Reconfiguration)

Oracle Identity Manager Configuration Parameters

Oracle Identity Manager Configuration Parameters
All fields marked with * are mandatory

Host*

oimhost

Port*

8080

OIM User Attribute*

Users.User ID

OIM Application Server Type*

Weblogic

Use SSL*

☐ Yes

☒ No

Client Certificate Subject Name

InstallShield

< Back Next > Cancel

6. Click **Next**.
7. On the Configuration Parameter Information page, if required, modify values for any or all of the following fields:
 - **Time interval after which password synchronization happens with OIM (in minutes)***
 - **No. of Maximum retries to synchronize Passwords from AD to OIM***

Figure 2–5 is a screenshot of the Configuration Parameters page on which sample values have been specified.

Figure 2–9 Configuration Parameters Page (Reconfiguration)

Configuration Parameter Information

All fields marked with * are mandatory

Time interval after which password synchronization happens with OIM (in minutes)*

1

No. of Maximum retries to synchronize Passwords from AD to OIM*

5

InstallShield

< Back Next > Cancel

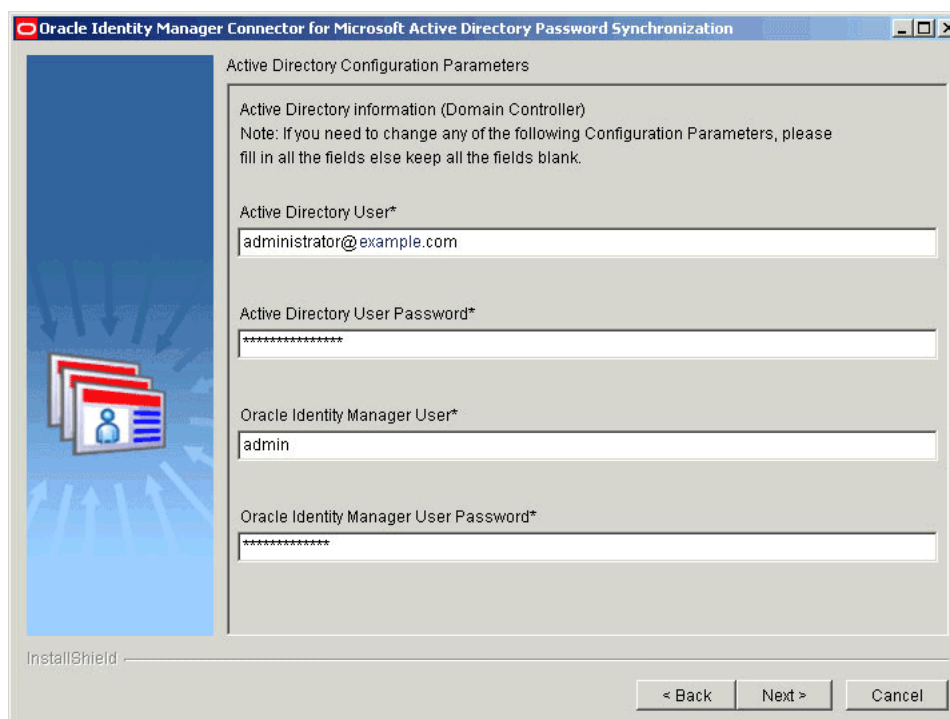
8. Click **Next** to continue with reconfiguring the connector.
9. On the second Active Directory Configuration Parameters page, if you want to modify the value of any field, then you must enter values for all fields displayed on that page. Otherwise, leave all the fields blank and proceed to the next step.

The following fields are displayed on the Second Active Directory Configuration Parameters page:

- **Active Directory User**
- **Active Directory User Password**
- **Oracle Identity Manager User**
- **Oracle Identity Manager User Password**

Figure 2–10 is a screenshot of the second Active Directory Configuration Parameters page on which sample values have been specified.

Figure 2–10 Second Active Directory Configuration Parameters Page (Reconfiguration)



10. On the Second Active Directory Configuration Parameters page, click **Next**.
11. On the next page, click **Finish** to complete the procedure for reconfiguring the connector.

2.3 Postinstallation

The following steps must be performed after the connector is installed:

- [Enabling and Disabling Logging](#)
- [Configuring the IT Resource for the Target System](#)
- [Enabling the Strong Password Authentication \(Password Complexity\) Feature of Microsoft Active Directory](#)

- [Configuring SSL](#)

2.3.1 Enabling and Disabling Logging

Log files contain information about events that occur during password synchronization. You can use the log files to determine the cause of any errors that may occur during password synchronization events.

This connector provides three log files. Each log file name is prefixed with *TIME_STAMP*, which represents the time at which the log file was created.

The following is the list of log files for this connector and their description:

Note: You cannot rename the log files. In addition, you cannot specify or change the log level for log files. The default log level is *DEBUG*.

- *TIME_STAMP_PasswordChange.log*

This file stores information about whether the connector is enabled. In the *TIME_STAMP_PasswordChange.log* file name, *TIME_STAMP* represents the time at which the log file was created in the YearMonthDayHourMinuteSecondMillisecond format.

Sample value: 200931801311828_PasswordChange.log

The *TIME_STAMP_PasswordChange.log* file is generated every time the oimadpwdsync10.dll file is initialized. The oimadpwdsync10.dll file is initialized when you restart the computer hosting the connector.

- *TIME_STAMPOIMMain.log*

This file stores information about events that occur while the password change records stored in the in-memory queue and persistent queue are being processed. In the *TIME_STAMPOIMMain.log* file name, *TIME_STAMP* represents the time at which the log file was created in the YearMonthDay format.

Sample value: 20093180IMMain.log

The *TIME_STAMPOIMMain.log* file is generated every time the password update thread is created.

- *TIME_STAMP_adsi_debug.log*

This file stores information about the events that occur from the time the password is changed in Microsoft Active Directory till the time the password change is saved to the in-memory queue. In the *TIME_STAMP_adsi_debug.log* file name, *TIME_STAMP* represents the time at which the log file was created in the YearMonthDayHourMinuteSecondMillisecond format.

Sample value: 2009318212319187_adsi_debug.log

The *TIME_STAMP_adsi_debug.log* file is generated every time a password change event occurs.

To enable or disable logging:

By default, logging is disabled for the password synchronization connector. After connector installation, if you want to enable logging, or disable logging after it has been enabled, then perform the procedure described in this section.

Note: The procedure described in this section must be performed on the target system host computer.

1. From the **Start** menu, click **Run**.
2. In the Run dialog box, type `regedit`.
3. In the Registry Editor window, on the left navigation pane:
 - If you want to enable or disable logging of events to the `TIME_STAMP_PasswordChange.log` file, then:
 - a. Navigate to the following key:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\oimpwdsync\ADConfig`
 - b. On the right pane, double-click the **Log** value.
 - If you want to enable or disable logging of events to the `TIME_STAMPOIMMain.log` file, then:
 - a. Navigate to the following key:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\oimpwdsync\OIMConfig`
 - b. On the right pane, double-click the **OIMLog** value.
 - If you want to enable or disable logging of events to the `TIME_STAMP_adsi_debug.log` file, then:
 - a. Navigate to the following key:
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\oimpwdsync\ADConfig`
 - b. On the right pane, double-click the **Log** value.
4. In the Edit String dialog box:
 - If you want to disable logging, then in the Value data field, enter `N`.
 - If you want to enable logging, then in the Value data field, enter `Y`.
5. Click **OK**.
6. If you have enabled or disabled logging of events to the `TIME_STAMP_PasswordChange.log` file, then restart the computer for the changes to take effect.

2.3.2 Configuring the IT Resource for the Target System

Note: If you have installed a user management connector release that is earlier than release 9.1.1, then you must set the value of the **AD Sync installed** parameter to `no`. For example, if you have installed the user management connector release 9.1.0, then you must set the value of the **AD Sync installed** parameter to `no`.

The ADITResource IT resource is created in Oracle Identity Manager when you install the user management connector. The **Allow Password Provisioning** parameter is a parameter of the user management connector.

If you want to use the target system as the trusted source for passwords, then set the **Allow Password Provisioning** parameter to `no`. When you set the value of this parameter to `no`, the user management connector does not propagate password changes from Oracle Identity Manager to the target system.

If you set the **Allow Password Provisioning** parameter to `yes`, then:

- When a Microsoft Active Directory resource is provisioned to an OIM User:
 1. An account is created on Microsoft Active Directory.
 2. The password of the account is detected by the connector and sent to Oracle Identity Manager.
 3. On Oracle Identity Manager, the password is compared with the current password of the Active Directory resource. Because both passwords are the same, no further action is taken.
 4. If password history policy is set, then an exception for the SPML request (sent by the password synchronization connector) is encountered. You can ignore this exception.
- When the password of the Microsoft Active Directory resource is changed on Oracle Identity Manager:
 1. The password is sent to Microsoft Active Directory by the user management connector.
 2. The updated password is detected by the connector and sent to Oracle Identity Manager.
 3. On Oracle Identity Manager, the password is compared with the current password of the Active Directory resource. Because both passwords are the same, no further action is taken.
 4. If password history policy is set, then an exception for the SPML request (sent by the password synchronization connector) is encountered. You can ignore this exception.
- When the password is changed on Microsoft Active Directory:
 1. The updated password is detected by the connector and sent to Oracle Identity Manager.
 2. On Oracle Identity Manager, the password is compared with the current password of the Active Directory resource. Because both passwords are different, the password of the Microsoft Active resource on Oracle Identity Manager is updated.
 3. The updated password is detected by the user management connector and sent to Microsoft Active Directory.
 4. The password of the Microsoft Active Directory is modified, even though this is the same password that was set by the user.
 5. The password of the account is detected by the password synchronization connector and sent to Oracle Identity Manager.
 6. On Oracle Identity Manager, the password is compared with the current password of the Active Directory resource. Because both passwords are the same, no further action is taken.

7. If password history policy is set on Oracle Identity Manager, then an exception for the SPML request (sent by the password synchronization connector) is encountered. You can ignore this exception.

2.3.2.1 Specifying a Value for the Allow Password Provisioning Parameter

Note: Perform the procedure described in this section only if the user management connector is installed.

You can specify a value for the Allow Password Provisioning parameter as follows:

1. Log in to the Administrative and User Console.
2. Expand **Resource Management**.
3. Click **Manage IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter ADITResource and then click **Search**.
5. Click the edit icon for the IT resource.
6. From the list at the top of the page, select **Details and Parameters**.
7. Depending on how you want the user management connector and password synchronization connector to function, enter a value of either *yes*, or *no* for the **Allow Password Provisioning** parameter.
8. If you have installed a user management connector release that is earlier than release 9.1.1, then you must set the value of the **AD Sync installed** parameter to *no*.

2.3.3 Enabling the Strong Password Authentication (Password Complexity) Feature of Microsoft Active Directory

Note: You must use an administrator account to perform the procedures described in this section.

Microsoft Active Directory provides the Strong Password Authentication feature through the implementation of a password filter. To use this password filter along with the connector, follow the instructions for enabling the "Passwords must meet complexity requirements" policy setting by visiting the Microsoft Web site at

<http://www.microsoft.com/technet/>

After you enable this policy setting, password changes in Microsoft Active Directory are checked against the Strong Password Authentication requirements before they are passed on to the connector.

2.3.4 Configuring SSL

Note: It is strongly recommended that you configure SSL communication between the connector and Oracle Identity Manager in your production environment.

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 connector, then the Oracle Identity Manager Design Console and any other custom clients must also communicate with Oracle Identity Manager using SSL.

To secure the propagation of passwords from Microsoft Active Directory to Oracle Identity Manager, you must configure SSL. The procedure that you must follow depends on the application server on which Oracle Identity Manager is running:

See Also: The "Configuring SSL" section of *Oracle Identity Manager Connector Guide for Microsoft Active Directory User Management* for information about configuring SSL to secure data transfer from Oracle Identity Manager to Microsoft Active Directory

- [Configuring SSL on IBM WebSphere Application Server](#)
- [Configuring SSL on JBoss Application Server](#)
- [Configuring SSL on Oracle Application Server](#)
- [Configuring SSL on Oracle WebLogic Server](#)

2.3.4.1 Configuring SSL on IBM WebSphere Application Server

The following sections provide information about enabling SSL communication when Oracle Identity Manager is running on IBM WebSphere Application Server:

- [Exporting the Certificate](#)
- [Importing the Certificate](#)
- [Additional Configuration Steps](#)

2.3.4.1.1 Exporting the Certificate

Note: The procedure described in this section must be performed on the IBM WebSphere Application Server host computer.

To export the IBM WebSphere Application Server certificate:

1. In a terminal window, change to the `WEBSPPHERE_HOME\AppServer\java\jre\bin` directory.
2. Run the following command:

```
keytool -export -alias default -file CERT_FILE_NAME -keypass  
DEFAULT_TRUST_STORE_PASSWORD -keystore DEFAULT_IDENTITY_STORE -storepass  
DEFAULT_IDENTITY_STORE_PASSWORD -storetype pkcs12 -provider  
com.ibm.crypto.provider.IBMJCE
```

In this command:

- *CERT_FILE_NAME* is the complete path and name of the certificate file.
- *DEFAULT_TRUST_STORE_PASSWORD* is the password of the default trust store trust.p12.
- *DEFAULT_IDENTITY_STORE* is the complete path and name of the default identity store key.p12.
- *DEFAULT_IDENTITY_STORE_PASSWORD* is the password of the default identity store key.p12.

The following is a sample command:

```
keytool -export -alias default -file C:\mycertificates\webasp.cer -keypass WebAS
-keystore C:\Program
Files\IBM\WebSphere\AppServer\profiles\AppSrv06\etc\key.p12 -storepass WebAS
-storetype pkcs12 -provider com.ibm.crypto.provider.IBMJCE
```

When you run the command, the application server certificate is generated in the *WEBSphere_HOME*\AppServer\java\jre\bin directory.

2.3.4.1.2 Importing the Certificate

Note: The procedure described in this section must be performed on the Microsoft Active Directory host computer.

To import the application server certificate:

1. Copy the certificate (exported in "[Exporting the Certificate](#)" on page 2-16) to any directory on the Microsoft Active Directory host computer.
2. Click **Start** and then click **Run**.
3. Enter the following command, and then click **OK**:

```
mmc
```

The Microsoft Management Console is displayed.
4. From the **File** menu, select **Add/Remove Snap-in**.
5. In the Add/Remove Snap-in dialog box, click **Add**.
6. In the Add Standalone Snap-in dialog box, select **Certificates**, and then click **Add**.
7. In the certificates snap-in dialog box, select **Computer account**, and then click **Next**.
8. In the Select Computer dialog box, accept the defaults, and then click **Finish**.
9. In the Add Standalone Snap-in dialog box, click **Close**.
10. In the Add/Remove Snap-in dialog box, click **OK**.
11. In the Console Root window, on the left pane, expand **Certificates (Local Computer)** under the Console Root folder.
12. Expand **Trusted Root Certification Authorities**, right-click **Certificates**, select **All Tasks**, and then click **Import**.

The Certificate Import Wizard is displayed.
13. On the Welcome to the Certificate Import Wizard page, click **Next**.

14. On the File to Import page, you can either specify the path to the directory in which you copied the exported certificate, or use the **Browse** button to specify the directory in which you copied the exported certificate.
15. Click **Next**.
16. On the Certificate Store page, select **Place all certificates in the following store**, and click **Next**.
17. On the Completing the Certificate Import Wizard, click **Finish**.
A message indicating that the import was successful is displayed.
18. Click **OK** to close the Certificate Import Wizard dialog box.

2.3.4.1.3 Additional Configuration Steps

Note: The procedure described in this section must be performed on the IBM WebSphere Client host computer.

You must extract and copy the xlDataObjectBeans.jar file located in the `OIM_DC_HOME\xlclient\ext` directory to the `WEBSPHERE_HOME\profiles\PROFILE_NAME\installedApps\NODE_NAME\OIM-xell-WS.ear\spmlws.war\WEB-INF\lib` directory.

Here:

- `OIM_DC_HOME` is the directory in which you install the Oracle Identity Manager Design Console
- `WEBSPHERE_HOME` is the home directory of WebSphere
- `PROFILE_NAME` is the name of the application server profile being used
- `NODE_NAME` is the name of the node which the application server profile uses

2.3.4.2 Configuring SSL on JBoss Application Server

The following sections provide information about enabling SSL communication when Oracle Identity Manager is running on JBoss application server:

- [Generating Keys](#)
- [Signing the Certificate](#)
- [Exporting the Certificate](#)

Note: The procedure described in the preceding sections must be performed on the JBoss Application Server host computer.

- [Importing the Certificate](#)

Note: The procedure described in the preceding section must be performed on the Microsoft Active Directory host computer.

- [Configuring the server.xml File](#)

Note: The procedure described in the preceding sections must be performed on the JBoss Application Server host computer.

2.3.4.2.1 Generating Keys

Generate keys by using the `keytool` command. The following `keytool` command generates an identity keystore. `jbossserver.jks`:

```
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 -storetype jks
```

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 you want to use for the private key.
- `DN_VALUE` is the distinguished name (DN) for your organization.
The common name (CN) value in the DN must be the host name of the Oracle Identity Manager server.
- `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 serverjboss -keyalg RSA -keysize 1024 -dname "CN=myhost"
-keypass welcome -keystore E:\jboss-4.0.3SP1\server\jbossserver.jks -storepass
welcome -storetype jks
```

2.3.4.2.2 Signing the Certificate

Use the following `keytool` command to sign the certificate that you created:

```
keytool -selfcert -alias PRIVATE_KEY_ALIAS -sigalg MD5withRSA -validity 2000
-keypass PRIVATE_KEY_PASSWORD -keystore IDENTITY_STORE_FILE -storepass
IDENTITY_STORE_FILE_PASSWORD
```

Note: It is recommended that you use trusted certificate authorities, for example, VeriSign or Thawte, for signing certificates.

The following is a sample command:

```
keytool -selfcert -alias serverjboss -sigalg MD5withRSA -validity 2000 -keypass
welcome -keystore E:\jboss-4.0.3SP1\server\jbossserver.jks -storepass welcome
```

2.3.4.2.3 Exporting the Certificate

Use the following `keytool` command to export the certificate from the identity keystore to a file:

```
keytool -export -alias PRIVATE_KEY_ALIAS -file CERT_FILE_NAME -keypass
PRIVATE_KEY_PASSWORD -keystore IDENTITY_STORE_FILE -storepass
```

```
IDENTITY_STORE_FILE_PASSWORD -storetype jks -provider sun.security.provider.Sun
```

In this command, replace *CERT_FILE_NAME* with the name that you want to use for the certificate file.

The following is a sample command:

```
keytool -export -alias serverjboss -file E:\jboss-4.0.3SP1\server\jbossserver.cert  
-keypass welcome -keystore E:\jboss-4.0.3SP1\server\jbossserver.jks -storepass  
welcome -storetype jks -provider sun.security.provider.Sun
```

2.3.4.2.4 Importing the Certificate

To import the application server certificate:

1. Copy the certificate (exported in ["Exporting the Certificate"](#) on page 2-19) to any directory on the Microsoft Active Directory host computer.
2. Click **Start** and then click **Run**.
3. Enter the following command, and then click **OK**:

```
mmc
```

The Microsoft Management Console is displayed.

4. From the **File** menu, select **Add/Remove Snap-in**.
5. In the Add/Remove Snap-in dialog box, click **Add**.
6. In the Add Standalone Snap-in dialog box, select **Certificates**, and then click **Add**.
7. In the certificates snap-in dialog box, select **Computer account**, and then click **Next**.
8. In the Select Computer dialog box, accept the defaults, and then click **Finish**.
9. In the Add Standalone Snap-in dialog box, click **Close**.
10. In the Add/Remove Snap-in dialog box, click **OK**.
11. In the Console Root window, on the left pane, expand **Certificates (Local Computer)** under the Console Root folder.
12. Expand **Trusted Root Certification Authorities**, right-click **Certificates**, select **All Tasks**, and then click **Import**.

The Certificate Import Wizard is displayed.

13. On the Welcome to the Certificate Import Wizard page, click **Next**.
14. On the File to Import page, you can either specify the path to the directory in which you copied the exported certificate, or use the **Browse** button to specify the directory in which you copied the exported certificate.
15. Click **Next**.
16. On the Certificate Store page, select **Place all certificates in the following store**, and click **Next**.
17. On the Completing the Certificate Import Wizard, click **Finish**.
A message indicating that the import was successful is displayed.
18. Click **OK** to close the Certificate Import Wizard dialog box.

2.3.4.2.5 Configuring the server.xml File

Copy the following entry to the `server.xml` file located in the `OIM_HOME\jboss-4.0.3SP1\server\default\deploy\jbossweb-tomcat55.sar` directory:

```
<Connector port="8443" address="${jboss.bind.address}"
    maxThreads="100" strategy="ms" maxHttpHeaderSize="8192"
    emptySessionPath="true"
    scheme="https" secure="true" clientAuth="false"
    sslProtocol="TLS"
    keystoreFile="E:\jboss-4.0.3SP1\server\jbossserver.jks"
    keystorePass="welcome"
    truststoreFile="E:\jboss-4.0.3SP1\server\jbossserver.jks"
    truststorePass="welcome"/>
```

After you have performed the preceding steps, restart the server for the changes to take effect.

2.3.4.3 Configuring SSL on Oracle Application Server

The following sections provide information about enabling SSL communication when Oracle Identity Manager is running on Oracle Application Server.

- [Enabling SSL for HTTP Communication to Oracle HTTP Server](#)
- [Exporting the Certificate](#)
- [Importing the Certificate](#)

2.3.4.3.1 Enabling SSL for HTTP Communication to Oracle HTTP Server

By default, the Oracle HTTP Server is configured with SSL and the SSL certificate store is located at `ORACLE_HOME\Apache\Apache\conf\ssl.wlt\default\`. The `listen` parameter in the `ORACLE_HOME\Apache\Apache\conf\ssl.conf` file points to the SSL port being used by the Oracle HTTP Server.

A custom wallet and certificate should be created for the Oracle HTTP Server.

Creating Custom Wallet and Certificate for Oracle HTTP Server

Perform the following steps to create a custom wallet and certificate for Oracle HTTP Server:

1. To create a custom wallet, run the following command:

```
orapki wallet create -wallet WALLET_LOCATION -auto_login
```

In this command, `WALLET_LOCATION` is the path to the directory where the wallet is created.

2. To add a self-signed certificate to the wallet, run the following command:

```
orapki wallet add -wallet WALLET_LOCATION -dn CN=HOST_NAME -keysize 2048
-self_signed -validity 3650
```

When prompted, enter the Wallet password.

This creates a self-signed certificate with a validity of 3650 days. The distinguished name of the subject is `CN=HOST_NAME`. Here `HOST_NAME` is the host name of the machine. The key size for the certificate is 2048 bits.

Note: Ensure that you obtain the certificate from an appropriate Certificate Authority.

3. To export the self-signed certificate, run the following command:

```
orapki wallet export -wallet WALLET_LOCATION -dn 'CN=HOST_NAME' -cert  
WALLET_LOCATION/b64certificate.txt
```

In this command, the value of *HOST_NAME* must be same as the value of *HOST_NAME* specified in Step 2.

4. Edit the ssl.conf file located in the *ORACLE_HOME*/Apache/Apache/conf/ as follows:

- a. In a text editor, open the ssl.conf file and find the following entry:

SSLWallet file:

- b. Enter *WALLET_LOCATION* (specified in Step 1) as the value of the SSLWallet file: entry.

The following is a sample value of the SSLWallet file: entry:

```
SSLWallet  
file:/home/testoc4j/OIM9102/product/10.1.3.1/OracleAS_1/Apache/Apache/conf/  
ssl.wlt/default
```

- c. Save and close the updated ssl.conf file.

5. Restart Oracle Application Server.

2.3.4.3.2 Exporting the Certificate

To export the application server certificate from the *WALLET_LOCATION* directory that you specified in Step 1 of ["Creating Custom Wallet and Certificate for Oracle HTTP Server"](#) on page 2-21, perform the following steps after you have started Oracle Wallet Manager:

Note: the default Oracle wallet directory is
ORACLE_HOME\Apache\Apache\conf\ssl.wlt\default\ewallet.p12

1. Depending on the operating system used, perform one of the following steps to start Oracle Wallet Manager:
 - For Microsoft Windows, click **Start, Programs, ORACLE-HOME_NAME, Integrated Management Tools, and Wallet Manager**.
 - For UNIX, in a terminal window, change to the *ORACLE_HOME*/bin directory and then enter the *owm* command.
2. Open the *WALLET_LOCATION* directory by using Oracle Wallet Manager.
3. Enter the wallet password (that you specified in Step 2 of ["Creating Custom Wallet and Certificate for Oracle HTTP Server"](#) on page 2-21) as the store password when prompted.
4. Right-click **Certificate (Ready)** and click **Export User Certificate**.
5. Enter *server.cert* as the file name and save the file.

The connector uses this certificate to trust Oracle Application Server.

See Also: The "Secure Sockets Layer" section in *Oracle Application Server Administrator's Guide* for more information about Oracle Wallet Manager

2.3.4.3.3 Importing the Certificate

To import the application server certificate:

1. Copy the certificate (exported in Step 3 of ["Creating Custom Wallet and Certificate for Oracle HTTP Server"](#) on page 2-21) to any directory on the Microsoft Active Directory host computer.
2. Click **Start** and then click **Run**.
3. Enter the following command, and then click **OK**:

```
mmc
```

The Microsoft Management Console is displayed.
4. From the **File** menu, select **Add/Remove Snap-in**.
5. In the Add/Remove Snap-in dialog box, click **Add**.
6. In the Add Standalone Snap-in dialog box, select **Certificates**, and then click **Add**.
7. In the certificates snap-in dialog box, select **Computer account**, and then click **Next**.
8. In the Select Computer dialog box, accept the defaults, and then click **Finish**.
9. In the Add Standalone Snap-in dialog box, click **Close**.
10. In the Add/Remove Snap-in dialog box, click **OK**.
11. In the Console Root window, on the left pane, expand **Certificates (Local Computer)** under the Console Root folder.
12. Expand **Trusted Root Certification Authorities**, right-click **Certificates**, select **All Tasks**, and then click **Import**.

The Certificate Import Wizard is displayed.
13. On the Welcome to the Certificate Import Wizard page, click **Next**.
14. On the File to Import page, you can either specify the path to the directory in which you copied the exported certificate, or use the **Browse** button to specify the directory in which you copied the exported certificate.
15. Click **Next**.
16. On the Certificate Store page, select **Place all certificates in the following store**, and click **Next**.
17. On the Completing the Certificate Import Wizard, click **Finish**.

A message indicating that the import was successful is displayed.
18. Click **OK** to close the Certificate Import Wizard dialog box.

2.3.4.4 Configuring SSL on Oracle WebLogic Server

The following sections provide information about enabling SSL communication when Oracle Identity Manager is running on Oracle WebLogic Server:

- [Generating Keys](#)
- [Signing the Certificate](#)
- [Exporting the Certificate](#)
- [Configuring Custom Identity Keystore in WebLogic Server](#)

Note: The procedure described in the preceding sections must be performed on the Oracle WebLogic Server host computer.

■ [Importing the Certificate](#)

Note: The procedure described in the preceding section must be performed on the Microsoft Active Directory host computer.

2.3.4.4.1 Generating Keys

Generate private/public certificate pairs by using the keytool command provided. The following command creates an identity keystore:

```
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 -storetype jks
```

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 you want to use for the private key.
- *DN_VALUE* is the distinguished name (DN) for your organization.
The common name (CN) value in the DN must be the host name of the Oracle Identity Manager server.
- *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 that creates an identity key store (support.jks):

```
keytool -genkey -alias support -keyalg RSA -keysize 1024 -dname "CN=oimserver"  
-keypass weblogic -keystore C:\bea\user_projects\domains\oim\support.jks  
-storepass support -storetype jks
```

2.3.4.4.2 Signing the Certificate

Use the following command to sign the certificate that you created.

```
keytool -selfcert -alias PRIVATE_KEY_ALIAS -sigalg MD5withRSA -validity  
2000 -keypass PRIVATE_KEY_PASSWORD -keystore IDENTITY_STORE_FILE -storepass  
IDENTITY_STORE_FILE_PASSWORD -storetype jks
```

Note: It is recommended that you use trusted certificate authorities, for example, VeriSign or Thawte, for signing certificates.

The following is a sample command:

```
keytool -selfcert -alias support -sigalg MD5withRSA -validity 2000 -keypass  
weblogic -keystore C:\bea\user_projects\domains\oim\support.jks -storepass support  
-storetype jks
```

2.3.4.4.3 Exporting the Certificate

Use the following command to export the certificate from the identity keystore to a file:

```
keytool -export -alias PRIVATE_KEY_ALIAS -file CERT_FILE_NAME -keypass
PRIVATE_KEY_PASSWORD -keystore IDENTITY_STORE_FILE -storepass
IDENTITY_STORE_FILE_PASSWORD -storetype jks -provider sun.security.provider.Sun
```

In this command, replace *CERT_FILE_NAME* with the complete path and name of the certificate file.

The following is a sample command:

```
keytool -export -alias support -file
C:\bea\user_projects\domains\oim\supportcert.pem -keypass weblogic -keystore
C:\bea\user_projects\domains\oim\support.jks -storepass support -storetype jks
-provider sun.security.provider.Sun
```

2.3.4.4.4 Configuring Custom Identity Keystore in WebLogic Server

To configure the custom identity keystore:

1. In the WebLogic Server Administration Console, click **Servers, Configuration**, and then click **General**.
2. Select **SSL listen port enabled**. The default port is 7002.
3. In the Administrative Console, click **Servers**.
4. On the **Configuration** tab, click the server name in the Name column of the table.
5. On the **Keystores** tab:
 - a. In the Change Center section, click **Lock & Edit** to enable modification to the settings on the page.
 - b. From the **Keystores** box, select **Custom Identity and Custom Trust**, and then click **Continue**.
 - c. In the **Custom Identity Keystore** and **Custom Trust Keystore** fields, enter `C:\bea\user_projects\domains\oim\support.jks` as the custom identity keystore file name.
 - d. In the **Custom Identity Keystore Type** field, enter `JKS`.
 - e. In the **Custom Identity Keystore Passphrase** and **Confirm Custom Identity Keystore Passphrase** fields, enter the password of the custom identity keystore.
6. On the **SSL** tab:
 - a. In the Change Center section, click **Lock & Edit** to enable modification to the settings on the page.
 - b. From the **Identity and Trust Location** box, select **Keystores**.
 - c. In the **Private Key Alias** field, enter `support` as the private key alias.
 - d. In the **Private Key Passphrase** and **Confirm Private Key Passphrase** fields, enter the password, for example, `support`.
7. Restart the server for the changes to take effect.

Note: For a clustered installation, repeat all the steps for each of the participating nodes in the cluster, and then restart the cluster.

2.3.4.4.5 Importing the Certificate

To import the application server certificate:

1. Copy the certificate (exported in ["Exporting the Certificate"](#) on page 2-24) to any directory on the Microsoft Active Directory host computer.
2. Click **Start** and then click **Run**.
3. Enter the following command, and then click **OK**:

```
mmc
```

The Microsoft Management Console is displayed.
4. From the **File** menu, select **Add/Remove Snap-in**.
5. In the Add/Remove Snap-in dialog box, click **Add**.
6. In the Add Standalone Snap-in dialog box, select **Certificates**, and then click **Add**.
7. In the certificates snap-in dialog box, select **Computer account**, and then click **Next**.
8. In the Select Computer dialog box, accept the defaults, and then click **Finish**.
9. In the Add Standalone Snap-in dialog box, click **Close**.
10. In the Add/Remove Snap-in dialog box, click **OK**.
11. In the Console Root window, on the left pane, expand **Certificates (Local Computer)** under the Console Root folder.
12. Expand **Trusted Root Certification Authorities**, right-click **Certificates**, select **All Tasks**, and then click **Import**.

The Certificate Import Wizard is displayed.
13. On the Welcome to the Certificate Import Wizard page, click **Next**.
14. On the File to Import page, you can either specify the path to the directory in which you copied the exported certificate, or use the **Browse** button to specify the directory in which you copied the exported certificate.
15. Click **Next**.
16. On the Certificate Store page, select **Place all certificates in the following store**, and click **Next**.
17. On the Completing the Certificate Import Wizard, click **Finish**.

A message indicating that the import was successful is displayed.
18. Click **OK** to close the Certificate Import Wizard dialog box.

Removing the Connector

This chapter describes the procedure to remove the connector installation for release 9.1.0.1 and 9.1.1. This chapter discusses the following topics:

- [Removing an Existing Installation of Release 9.1.0.1](#)
- [Removing an Existing Installation of Release 9.1.1](#)

3.1 Removing an Existing Installation of Release 9.1.0.1

To remove an existing installation of the release 9.1.0.1 connector:

1. Delete the connector-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. Delete the `Adsync.dll` file from the `Windows\system32` directory.
3. If you have installed the connector on a 64-bit Microsoft Windows operating system, then delete the `Adsync.dll` file from the `Windows\SysWOW64` directory.
4. Delete the `ADSYNC_HOME` directory.
5. Restart the computer.

3.2 Removing an Existing Installation of Release 9.1.1

To remove an existing installation of the release 9.1.1 connector:

1. Delete the persistent queue container from Active Directory. You can find the location of the persistent queue container in the prepAD.ldif file as a value of the `dn` entry.

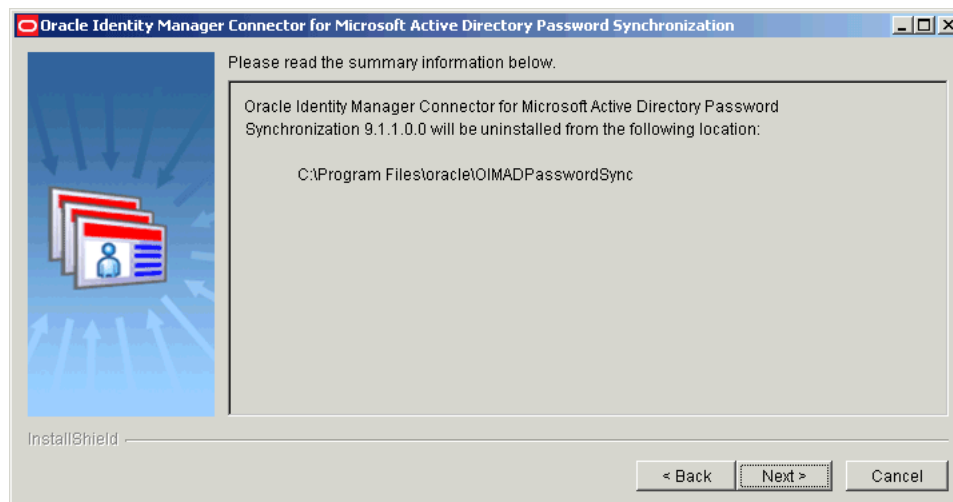
The prepAD.ldif file is located in the connector installation directory

2. From the **Start** menu, select **Settings**, and then click **Control Panel**.
3. From Control Panel window, double-click **Add or Remove Programs**.
4. In the Add or Remove Programs windows, select **Oracle Identity Manager Connector for Microsoft Active Directory Password Synchronization** from the list of currently installed programs, and then click **Change/Remove**.
5. On the Welcome page, click **Next**.
6. On the Summary page, verify that the location from where the connector will be removed is displayed correctly and then click **Next** to remove the connector.

Note: If you want to cancel the process of removing the connector, then click **Cancel**.

Figure 3–1 shows the Summary page for removing the connector.

Figure 3–1 Summary Page for Removing the Connector



7. On the next page, click **Next**.
8. On the subsequent page, click **Next**. This will restart your computer.
9. If you have installed the connector on a 64-bit Microsoft Windows operating system, then delete the oimadpwdsync10.dll and orclmessages.dll files from the Windows\system32 directory.

Known Issues

The following is the known issue associated with this release of the connector:

Bug 8361237

Information about events that occur during connector installation are recorded in the oimpwdsync.log file, which is located in the %TEMP% directory.

The oimpwdsync.log file is not deleted when you reinstall or reconfigure the password synchronization connector.

Special Characters Supported for Passwords

There are some restrictions on the special characters that you can use in the Password field on both Oracle Identity Manager and Microsoft Active Directory. For information about the supported special characters, refer to the "Special Characters Supported for Passwords" appendix in *Oracle Identity Manager Connector Guide for Microsoft Active Directory User Management*.

Index

A

account management mode
 See target resource reconciliation
Allow Password Provisioning parameter, 1-3, 2-14
architecture of the connector, 1-4

B

BEA WebLogic Server, 2-23

C

certified deployment configuration, 2-1
changing log levels, 2-12
complex passwords, 2-15
configurations, certified, 2-1
configuring SSL, 2-16
 BEA WebLogic Server, 2-23
 IBM WebSphere Application Server, 2-16
 additional configuration steps, 2-18
 exporting certificate, 2-16
 importing certificate, 2-17
 JBoss Application Server, 2-18
 configuring the server.xml file, 2-20
 exporting certificate, 2-19
 generating keys, 2-19
 importing certificate, 2-20
 signing the certificate, 2-19
 Oracle Application Server, 2-21
 enabling SSL for HTTP communication, 2-21
 exporting certificate, 2-22
 importing certificate, 2-23
 Oracle WebLogic Server
 exporting certificate, 2-24
 generating keys, 2-24
 importing certificate, 2-26
 signing the certificate, 2-24
connector architecture, 1-4

D

deinstalling
 See removing
deploying, 2-1
deployment configuration, certified, 2-1
deployment requirements, 2-1

deployment steps, 2-1
deployment use case, supported, 1-2
disabling logging, 2-12

E

enabling logging, 2-12
enabling strong password authentication, 2-15
exporting
 IBM WebSphere Application Server
 certificate, 2-16
 JBoss Application Server certificate, 2-19
 Oracle Application Server certificate, 2-22
 Oracle WebLogic Server certificate, 2-24

H

handling
 special characters, A-1

I

IBM WebSphere Application Server, 2-16
identity reconciliation mode
 See trusted source reconciliation
importing
 IBM WebSphere Application Server
 certificate, 2-17
 Oracle WebLogic Server certificate, 2-26
installation steps, 2-1
installing connector, 2-1, 2-2
issues, 4-1

J

JBoss Application Server, 2-18

K

known issues, 4-1

L

limitations, 4-1
log files, connector, 2-12
logging, 2-12

O

operating systems supported, 2-1
Oracle Application Server, 2-21

P

Password Complexity feature, 2-15
password synchronization process, 1-4
password synchronization process in a multi-domain
controller environment, 1-9
postdeployment steps, 2-11
postinstallation steps, 2-11
predeployment steps, 2-1
preinstallation steps, 2-1
prerequisites for connector deployment, 2-1
problems, 4-1

R

reconfiguring connector, 2-8
removing, 3-1, 3-2
removing the release 9.1.0.1 installation, 3-1
removing the release 9.1.1 installation, 3-2
requirements for connector deployment, 2-1

S

sequence of events, 1-5
first SPML request accepted, 1-6
Oracle Identity Manager is not available, 1-8
second SPML request accepted, 1-8
second SPML request rejected, 1-7
first SPML request rejected, 1-6
Oracle Identity Manager is not available, 1-8
special characters, handling, A-1
specifying the IT resource parameter value, 2-15
SSL configuring
See configuring SSL
stages of connector deployment
installation
installing connector, 2-1
postinstallation, 2-11
preinstallation, 2-1
strong password authentication feature, 2-15
supported
connector deployment use cases, 1-2
operating systems, 2-1
releases of Oracle Identity Manager, 2-1
target system host platforms, 2-1
target systems, 2-1

T

target resource reconciliation, 1-2, 1-3
target systems
host platforms supported, 2-1
supported, 2-1
trusted source reconciliation, 1-1, 1-3

U

user management connector modes
account management, 1-2, 1-3
identity reconciliation, 1-1, 1-3