Oracle® Identity Manager
Connector Guide for Microsoft Active Directory Password Synchronization

Release 9.1.1

E11218-28

February 2026

ORACLE®

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

E11218-28

Contents

3 Removing the Connector

4 Troubleshooting the Connector

5 Known Issues and Workarounds

List of Figures

List of Tables

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with Microsoft Active Directory.

Audience

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

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For information about installing and using Oracle Identity Manager, see the Oracle Identity Manager documentation library.

For generic information about connectors, see *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager.*

The following Oracle Technology Network page provides links to Oracle Identity Manager documentation:

http://download.oracle.com/docs/cd/E14571_01/im.htm

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, visit Oracle Technology Network at

http://download.oracle.com/docs/cd/E22999_01/index.htm

Conventions

The following text conventions are used in this document:

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

What's New in 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 9.1.1.5.

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 9.1.1.5](#)
- [Software Updates in Release 9.1.1.4](#)
- [Software Updates in Release 9.1.1](#)
- [Software Updates in Release 9.1.0.1](#)
- [Software Updates in Release 9.1.0](#)

Software Updates in Release 9.1.1.5

The following are software updates in release 9.1.1.5:

- [Support for New Version of the Connector](#)
- [Support for New Oracle Identity Manager Release](#)

Support for New Version of the Connector

From this release onward, version 9.1.1.5.16 of the connector is available for deployment. Be sure to download and apply mandatory patch 28353217 from `https://support.oracle.com` and to follow the readme instructions for proper deployment of this version of the connector.

ORACLE®

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

Support for New Oracle Identity Manager Release

From this release onward, the connector can be installed and used on a target system that can access a running instance of Oracle Identity Manager 11*g* release 1 (11.1.1). Where applicable, instructions specific to this Oracle Identity Manager release have been added in the guide.

See Certified Components for more information.

Software Updates in Release 9.1.1.4

The following are software updates in release 9.1.1.4:

- Support for Customizing the Location of OU
- Resolved Issues

Support for Customizing the Location of OU

From this release onward, you can customize the location of OU (Persistent Store) only while installing the connector. You can now create it under a different OU. However, once the OU is created, you cannot change its location.

See Installing the Connector for more information about Persistent Store.

Resolved Issues

The following are issues resolved in release 9.1.1.4:

Bug Number	Issue	Resolution
9110130	The connector did not allow the setting of time delay to less than one minute. If the connector was installed on two Domain Controllers, and the password change operations were initiated on both within one minute, then the order in which the password reset operations were processed was incorrect.	This issue has now been resolved. The password change operations are now carried out in the correct sequence.

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

ORACLE®

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

- 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" 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" 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.

ORACLE®

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

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" 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.
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" for more information.

Additions to the List of Known Issues

In Known Issues and Workarounds, the following items 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.

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 9.1.0

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.

Documentation-Specific Updates

The following sections discuss documentation-specific updates:

- Documentation-Specific Updates in Release 9.1.1.5
- Documentation-Specific Updates in Release 9.1.1.4
- Documentation-Specific Updates in Release 9.1.0.1

Documentation-Specific Updates in Release 9.1.1.5

The following is a documentation-specific update in revision "25" of this guide:

A Note present in section Configuring the IT Resource for the Target System and Specifying a Value for the Allow Password Provisioning Parameter has been updated.

The following is a documentation-specific update in revision "24" of this guide:

The "Target system" row of Table 1-2 has been updated to include support for Microsoft Active Directory 2008 R2.

The following is a documentation-specific update in revision "23" of this guide:

Microsoft Active Directory Password Synchronization Connector Creates a Dummy User During Installation has been added.

The following are documentation-specific updates in revision "22" of this guide:

ORACLE®

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

- The "Target system" row of Table 1-2 has been updated to include support for Microsoft Active Directory 2019. In addition, information about the minimum supported connector patch version has been added.

- The "Other software" row of Table 1-2 has been updated.

- Information about installing the connector manually has been added as a note in Installation.

- Minor updates to the document structure has been made for better readability.

The following are documentation-specific updates in revision "21" of this guide:

- The "Oracle Identity Governance or Oracle Identity Manager" row of Table 1-2 has been updated to include support for Oracle Identity Governance 12*c* (12.2.1.4.0).

- Configuring the Connector for Oracle Identity Governance 12*c* (12.2.1.4.0) or 14*c* (14.1.2.1.0) has been added.

- Support for New Version of the Connector has been added to Software Updates in Release 9.1.1.5.

- A "Note" regarding dummy user has been added to Step 14 of Installing the Connector.

The following are documentation-specific updates in revision "20" of this guide:

- A "Note" in Configuring SSL has been updated to include information on the password sync issue if Microsoft Active Directory is running on Windows 2008 R2.

- Excluding Users for Password Synchronization has been added.

- Uninstalling Release 9.1.1.5.x of the Connector has been added.

The following are documentation-specific updates in revision "19" of this guide:

- Steps 3 and 4 of Removing an Existing Installation of Release 9.1.1.x have been modified.

- Step 7 of Configuring Custom Identity Keystore in Oracle WebLogic Server has been modified.

The following are documentation-specific updates in revision "18" of this guide:

- The "Oracle Identity Manager" row of Table 1-2 has been renamed to "Oracle Identity Governance or Oracle Identity Manager" and also updated to include support for Oracle Identity Governance 12.2.1.3.0.

- Setting up the SPML-DSML.ear for Password Synchronization has been added.

- Steps 3 and 4 of Removing an Existing Installation of Release 9.1.1.x have been modified.

The following is a documentation-specific update in revision "17" of this guide:

The "Target systems" row of Table 1-2 has been updated to include support for Microsoft Active Directory 2016.

The following are documentation-specific updates in revision "16" of this guide:

- The "Target systems" row of Table 1-2 has been updated.

- Appendix A, "Special Characters Supported for Passwords" has been removed as all special characters that you can use in the Password field of Microsoft Active Directory are supported in Oracle Identity Manager.

- The "Known Issues" chapter has been renamed to Known Issues and Workarounds and has been restructured.

- Issue with ASCII Characters in User Names has been added to describe a known issue related to ASCII characters.

The following are documentation-specific updates in revision "15" of this guide:

- An issue related to InstallShield has been added to Table 4-1.

- Determining the Release Number of the Connector has been added.

- The reference information in Appendix A, "Special Characters Supported for Passwords" has been modified.

- The "Other software" row of Table 1-2 has been updated.

- The "Oracle Identity Manager" row of Table 1-2 has been updated.

- A "Note" regarding special characters that are not supported has been added to Appendix A, "Special Characters Supported for Passwords."

The following are documentation-specific updates in revision "14" of this guide:

- The "Target systems and target system host platforms" row has been renamed to "Target systems" in Table 1-2.

- The "Target systems" and "Other software" rows of Table 1-2 have been updated.

The following are documentation-specific updates in earlier revisions of this guide:

- In Installing the Connector, step number 12 has been updated for time interval after which password synchronization happens with OIM (in Seconds).

- A "Note" has been added to Configuring the IT Resource for the Target System and Specifying a Value for the Allow Password Provisioning Parameter.

- Information has been added to step 15 in Installing the Connector.

- Information has been added to step 7 in Configuring Custom Identity Keystore in Oracle WebLogic Server.

- Information has been added to the "Description" column in the "OIM User Attribute" row, in Table 2-2.

- In Signing the Certificate, information about importing the self-signed certificate as a trusted entry in the Java standard store has been added.

- Troubleshooting the Connector has been added.

- Instructions specific to Oracle Identity Manger release 11.1.2.*x* have been added throughout the guide, wherever applicable.

- The "Verifying Deployment Requirements" section has been removed. However, the contents of that section have been moved to Certified Components.

- The "Target systems and target system host platforms" row of Table 1-2 has been modified.

Documentation-Specific Updates in Release 9.1.1.4

The following are documentation-specific updates in release 9.1.1.4:

- Section 2.1.1, "Verifying Deployment Requirements" has been updated.

- An attribute has been added in Table 2-1.

- Appendix B, "PrepAD.ldif" has been added to provide information about the PrepAD.ldif file.

Documentation-Specific Updates in Release 9.1.0.1

The following are documentation-specific updates in release 9.1.0.1:

- In the [Deploying the Connector](#) chapter, the "Determining the Release Number of the Connector" section has been removed.

- In the [Known Issues and Workarounds](#) 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.

1

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](#)
- [Functionality of the Microsoft Active Directory User Management and Password Synchronization Connectors](#)
- [Certified Components](#)
- [Guidelines on Using the Connector](#)
- [Connector Architecture](#)
- [Roadmap for Deploying and Using the Connector](#)

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.

Functionality of the Microsoft Active Directory User Management and Password Synchronization Connectors

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	**Only user management connector installed:** User data from Active Directory is matched with OIM Users
	Only password synchronization connector installed: NA
	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.
Target resource reconciliation from Active Directory	**Only user management connector installed:** User data from Active Directory is matched with the Active Directory resource assigned to OIM Users
	Only password synchronization connector installed: NA
	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.

Table 1-1 (Cont.) Functionality of the User Management and Password Synchronization Connectors

Event	Action Performed by the Connector
OIM User's password changed	**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.
	The Allow Password Provisioning parameter is an IT resource parameter for the user management connector. If you set this parameter to `yes`, 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 `no`, then Oracle Identity Manager does not propagate the password change to all of the resources allocated (provisioned) to the OIM User.
	Note: This applies only if pre-populate adapters have been configured to propagate passwords from OIM Users to the resources.
	Note: This does not apply to release 11.1.1.*x* of the connector.
	Only password synchronization connector installed: NA
	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.
Password changed on Active Directory	**Only user management connector installed:** Passwords changed on Active directory are not propagated to Oracle Identity Manager
	Only password synchronization connector installed: Passwords changed on Active directory are propagated to Oracle Identity Manager
	Both user management and password synchronization connectors installed: Passwords changed on Active directory are propagated to Oracle Identity Manager

Certified Components

Table 1-2 lists the certified components for this connector.

Table 1-2   Certified Components

Item	Requirement
Oracle Identity Governance or Oracle Identity Manager	You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager: • Oracle Identity Governance 14c (14.1.2.1.0) • Oracle Identity Governance 12*c* (12.2.1.4.0) • Oracle Identity Governance 12*c* (12.2.1.3.0) • Oracle Identity Manager 11g Release 2 PS3 (11.1.2.3.0) • Oracle Identity Manager 11*g* release 2 PS2 (11.1.2.2.0) and any later BP in this release track • Oracle Identity Manager 11*g* release 2 PS1 (11.1.2.1.0) and any later BP in this release track • Oracle Identity Manager 11*g* release 2 BP02 (11.1.2.0.2) and any later BP in this release track **Note:** In this guide, **Oracle Identity Manager release 11.1.2.*x*** has been used to denote all releases in the Release 2 track listed here, and future releases in the 11.1.2.*x* series that the connector supports. • Oracle Identity Manager 11*g* release 1 PS2 (11.1.1.7.0) and any later BP in this release track • Oracle Identity Manager 11*g* release 1 PS1 (11.1.1.5.0) and any later BP in this release track • Oracle Identity Manager 11*g* release 1 (11.1.1.3.0) and any later BP in this release track **Note:** In this guide, **Oracle Identity Manager release 11.1.1** has been used to denote Oracle Identity Manager 11*g* Release 1 (11.1.1). • Oracle Identity Manager release 9.1.0.0 and any later BP in this release track **Note:** In this guide, **Oracle Identity Manager release 9.1.0.*x*** has been used to denote Oracle Identity Manager release 9.1.0.0 and future releases in the 9.1.0.*x* series that the connector supports.
Target systems	The target system can be any one of the following: • Microsoft Active Directory 2003 (x86 or x64) • Microsoft Active Directory 2008 (x86 or x64) • Microsoft Active Directory 2008 R2 (x86 or x64) • Microsoft Active Directory 2012 (x64) • Microsoft Active Directory 2012 R2 (x64) • Microsoft Active Directory 2016 (x64) • Microsoft Active Directory 2019 (x64) • Microsoft Active Directory 2022 (x64) • Microsoft Active Directory 2025 (x64) **Note:** The minimum supported Microsoft Active Directory Password Synchronization connector one-off patch version is 9.1.1.5.17 (that is, patch 30856343). Ensure that you apply the one-off patch release 9.1.1.5.17 (that is, patch 30856343) by downloading it from My Oracle Support.
Other software	The following is the software that the computer hosting the Microsoft Active Directory domain controller on which you want to install the connector must be able to access: • For Oracle Identity Manager release 9.1.0.*x:* SPML Web Service • For Oracle Identity Manager release 11.1.1, 11.1.2.*x,* 12*c*, or 14*c*: SPML-DSML Service
Other consideration	The target system host computer must be able to ping the application server host using both IP address and host name.

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.

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
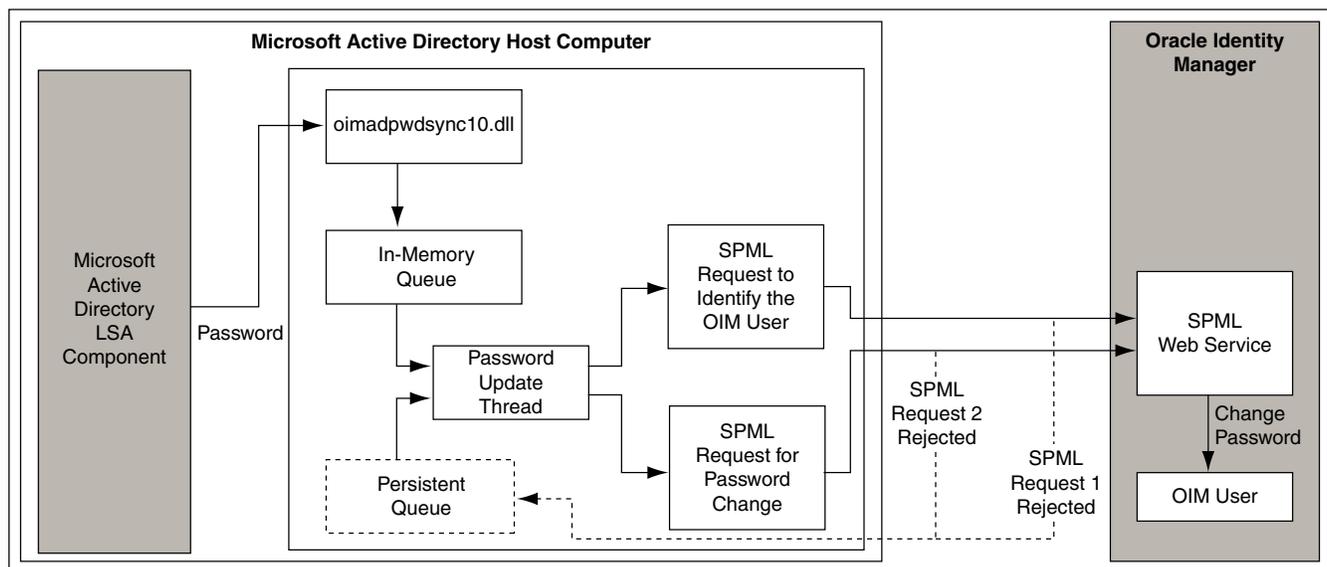
This section describes the connector architecture in the following topics:

- Password Synchronization Process
- Processes Associated With Events for SPML Requests
- Password Synchronization Connector in a Multi-Domain Controller Environment

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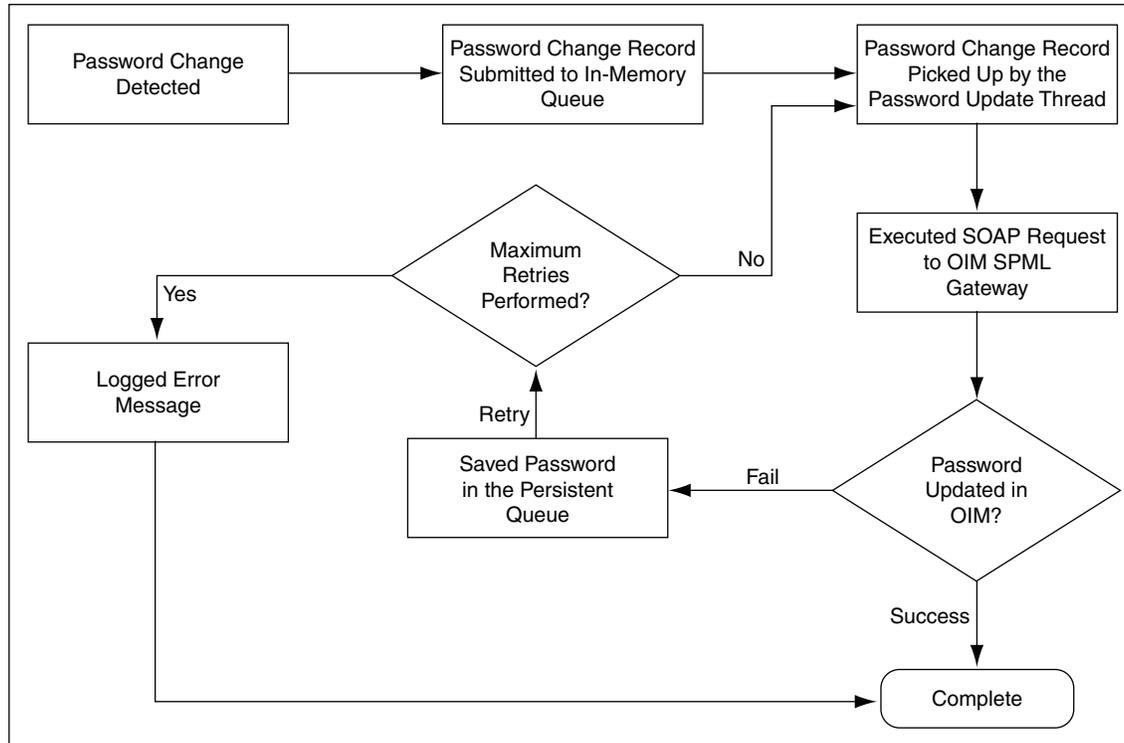
The following is the sequence of events that take place during password synchronization:

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

Processes Associated With Events for SPML Requests

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

- First SPML Request Rejected
- First SPML Request Accepted
- Oracle Identity Manager Is Not Available

> **ⓘ 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

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_STAMP*OIMMain.log file:

```
The user does not exist in OIM
```

See "Enabling and Disabling Logging" for information about the connector log files.

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](#)" 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=oimpwdsync*DOMAIN_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_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" 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" 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.

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_STAMP*OIMMain.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

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.

Roadmap for Deploying and Using the Connector

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

• Deploying the Connector describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.

• Removing the Connector describes the procedure to uninstall the connector.

• Troubleshooting the Connector lists solutions to errors that you may encounter while using the connector.

• Known Issues and Workarounds lists known issues associated with this release of the connector.

• PrepAD.ldif provides information about the PrepAD.ldif file.

2

Deploying the Connector

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

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

Preinstallation

Preinstallation for the connector involves performing the procedures described in the following sections:

- [Deploying the SPML-DSML Service](#)
- [Setting up the SPML-DSML.ear for Password Synchronization](#)
- [Testing the SPML Web Service and SPML-DSML Service](#)
- [Determining the Release Number of the Connector](#)
- [Configuring the Connector for Oracle Identity Governance 12*c* (12.2.1.4.0) or 14*c* (14.1.2.1.0)](#)

Deploying the SPML-DSML Service

> ⓘ **Note**
>
> Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.1, 11.1.2.*x,* or 12*c*.
>
> If you are using Oracle Identity Governance 12*c*, perform the steps in [Setting up the SPML-DSML.ear for Password Synchronization](#) after deploying the SPML-DSML.ear.
>
> If you are using Oracle Identity Manager release 9.1.0.*x*, then skip this section and deploy the SPML Web Service. See Oracle Identity Manager Tools Reference for detailed information.

Before you deploy the connector, deploy the SPML-DSML Service on the Oracle WebLogic Application Server on which Oracle Identity Manager is running:

1. Log in to the Oracle WebLogic Server Administration Console.
2. In the Change Center region, click **Lock & Edit** to enable modification to the settings on the page.
3. In the Domain Structure region, click **Deployments.**
4. On the right pane, click **Install.**

5. On the Locate deployment to install and prepare for deployment page, in the **Path** field, enter `OIM_HOME\server\apps`. For example, `D:\my_install\middleware\Oracle_IDM1\server\apps`.

6. In the region following the Current Location field, select **spml-dsml.ear** and then click **Next.**

7. On the Choose targeting style page, click **Next** to accept the default selection and proceed with installation.

8. On the Select deployment targets page, in the Available targets for spml-dsml region, select **oim_server1** if Oracle Identity Manager is installed in a nonclustered environment. Otherwise, select **oim_cluster.**

9. Click **Next.**

10. On the Optional Settings page, in the Source accessibility region, select **I will make the deployment accessible from the following location,** and then click **Next.**

11. On the Review your choices and click Finish page, verify the data that you have provided, and then click **Finish.**

12. On the Settings for spml-dsml page, review the configuration information of the deployed SPML-DSML Service, and then click **Save.**

13. In the Change Center region, click **Activate Changes** for the changes to take effect.

14. On the left pane, in the Domain Structure region, click **Deployments.**

15. On the right pane, in the Deployments table, select **spml-dsml,** and then from the Start list, select **Servicing all requests.**

    The SPML-DSML Service is started.

Setting up the SPML-DSML.ear for Password Synchronization

> ⓘ **Note**
>
> This procedure is applicable only for Oracle Identity Governance 12*c*.

After deploying SPML-DSML ear, perform the following steps in the WebLogis Server (WLS) console to enable the Web Service test tool which is disabled by default:

1. In the WLS console, click the domain name you want to modify.

2. On the General tab, open the Advanced section and select **Enable Web Service Test Page**.

3. Click **Save**.

4. Restart all the servers.

Testing the SPML Web Service and SPML-DSML Service

> **ⓘ Note**
>
> You can use the information in this section to test the SPML Web Service on Oracle Identity Manager release 9.1.0.*x*, or the SPML-DSML Service on Oracle Identity Manager release 11.1.1 or 11.1.2.*x*.

To test whether the SPML Web service is deployed successfully on Oracle Identity Manager, navigate to the following URL:

- **For IBM WebSphere Application Server:**

  http://*IP ADDRESS:PORT NUMBER/*spmlws/HttpSoap11

  https://*IP ADDRESS:SSL PORT NUMBER/*spmlws/HttpSoap11

- **For JBoss Application Server:**

  http://*IP ADDRESS:PORT NUMBER/*spmlws/services/HttpSoap11

  https://*IP ADDRESS:SSL PORT NUMBER/*spmlws/services/HttpSoap11

- **For Oracle Application Server:**

  http://*IP ADDRESS:PORT NUMBER/*spmlws/HttpSoap11

  https://*IP ADDRESS:SSL PORT NUMBER/*spmlws/HttpSoap11

- **For Oracle WebLogic Server:**

  http://*IP ADDRESS:NON-SSL PORT NUMBER/*spmlws/OIMProvisioning

  https://*IP ADDRESS:SSL PORT NUMBER/*spmlws/OIMProvisioning

Determining the Release Number of the Connector

> **ⓘ Note**
>
> Perform the procedure described in this section only if you are using Oracle Identity Manager Microsoft Active Directory Password Synchronization Connector release 9.1.1.5.13 (patch 21492223) or later. The following procedure is not applicable to prior releases of the connector.

You might have a deployment of an earlier release of the connector. While deploying the latest release, you might want to know the release number of the earlier release. To determine the release number of the connector that has already been deployed, perform the following procedure:

1. Open the Windows System Registry (regedit.exe).

2. Navigate to the registry key at the following location:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\oimpwdsync\Install

3. In the registry key, the release number of the connector is displayed in the string data as the value of the InstallID property.

Sample value: `9.1.1.5.13`

Configuring the Connector for Oracle Identity Governance 12*c* (12.2.1.4.0) or 14*c* (14.1.2.1.0)

> ⓘ **Note**
>
> Perform the procedure described in this section only if you are using Oracle Identity Governance 12*c* (12.2.1.4.0) or Oracle Identity Governance 14*c* (14.1.2.1.0).

To configure the connector:

1. Configure a new administrative user in the connector. For example, **admin1**.

   > ⓘ **Note**
   >
   > - Be sure not to create **XELSYSADM** as the new user.
   > - Ensure that the new user exists in Oracle Identity Governance with appropriate permissions, including `Admin Role`.

2. Log in to the Design Console and perform the following steps:

   a. Search for and open the **Lookup.AD.Users** lookup definition.

   b. Add the following new values:

   For **Code Key**, enter the value of the new administrative user configured in connector.

   For **Decode**, enter the application instance name for Active Directory.

3. Save the lookup definition.

Installation

> ⓘ **Note**
>
> Skip the procedures described in this section and install the connector manually if any of the following conditions are true:
>
> - You are unable to install or reconfigure release 9.1.1.5.0 of the connector using GUI-based installation or reconfiguration.
> - You are using Microsoft Active Directory 2019, 2022 or 2025 as your target system.
>
> To install the latest version of the connector manually, you must first install the 9.1.1.5.16 version of the connector by applying patch 28353217. This patch includes a README.text file with instructions for manual installation, manual reconfiguration, and manual uninstallation of the connector. Then, apply patch 30856343 for the 9.1.1.5.17 version of the connector. You can download patches 28353217 and 30856343 from My Oracle Support.

This section discusses the following topics:

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

Installing the Connector

Installing the connector is described in the following topics:

- [Installation Procedure](#)
- [Microsoft Active Directory Configuration Parameters](#)
- [Oracle Identity Manager Configuration Parameters](#)
- [Ensuring that the Connector is Ready for Propagating Passwords](#)

Installation Procedure

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 to want install the connector.

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

   Figure 2-1   Installation Directory Page (Installation)
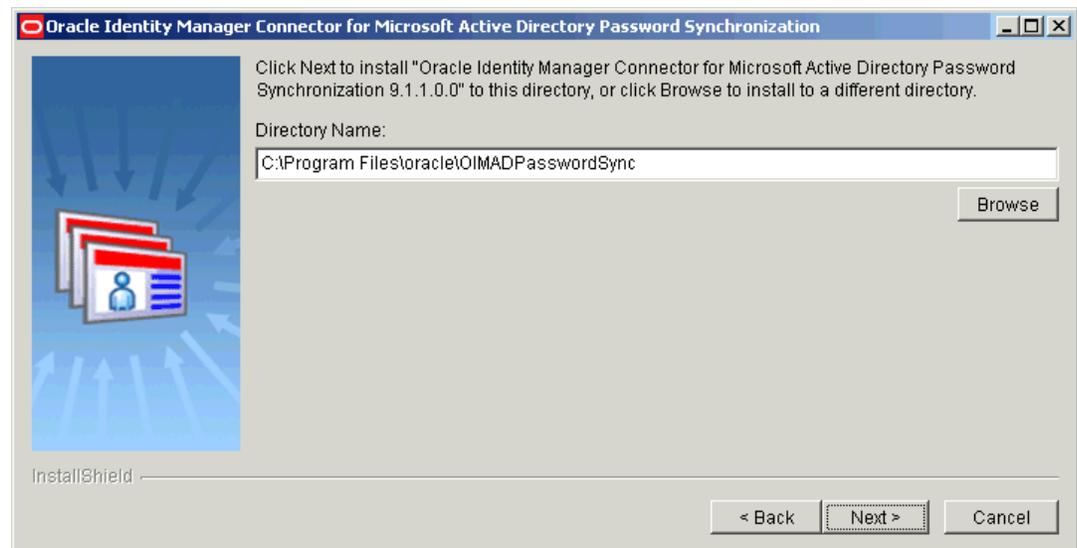
5. Click **Next.**

   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)

See Microsoft Active Directory Configuration Parameters for information about the Active Directory configuration parameters.

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" 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)

See Oracle Identity Manager Configuration Parameters for information about the Oracle Identity manager configuration parameters.

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 Seconds)**: Enter an integer value in this field. This value represents the number of seconds 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)
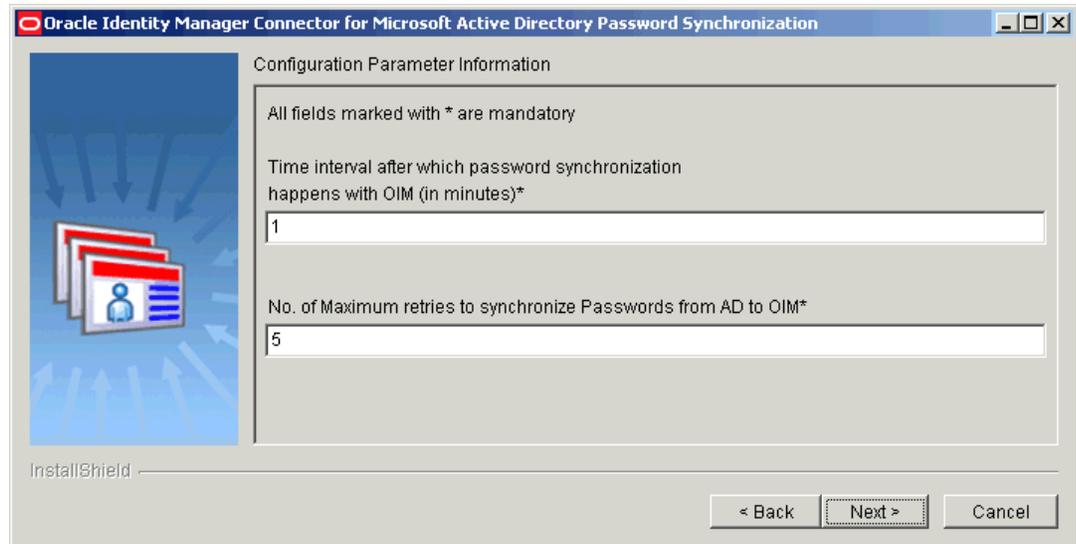
13. Click **Next.**

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 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.

- 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.

Figure 2-6   Summary Page (Installation)
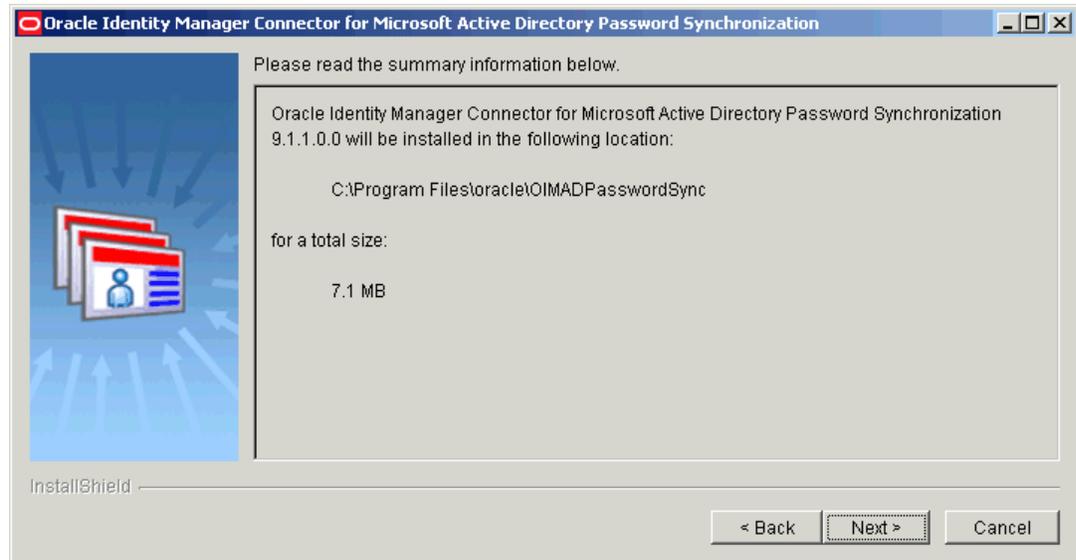
> ⓘ **Note**
>
> A dummy Active Directory user named **oidtmpuser** gets created and deleted immediately in the Active Directory server during installation to verify if the actual Active Directory Password Synchronization administrative user has required administration privileges or not.

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

Figure 2-7   Restart Page (Installation)
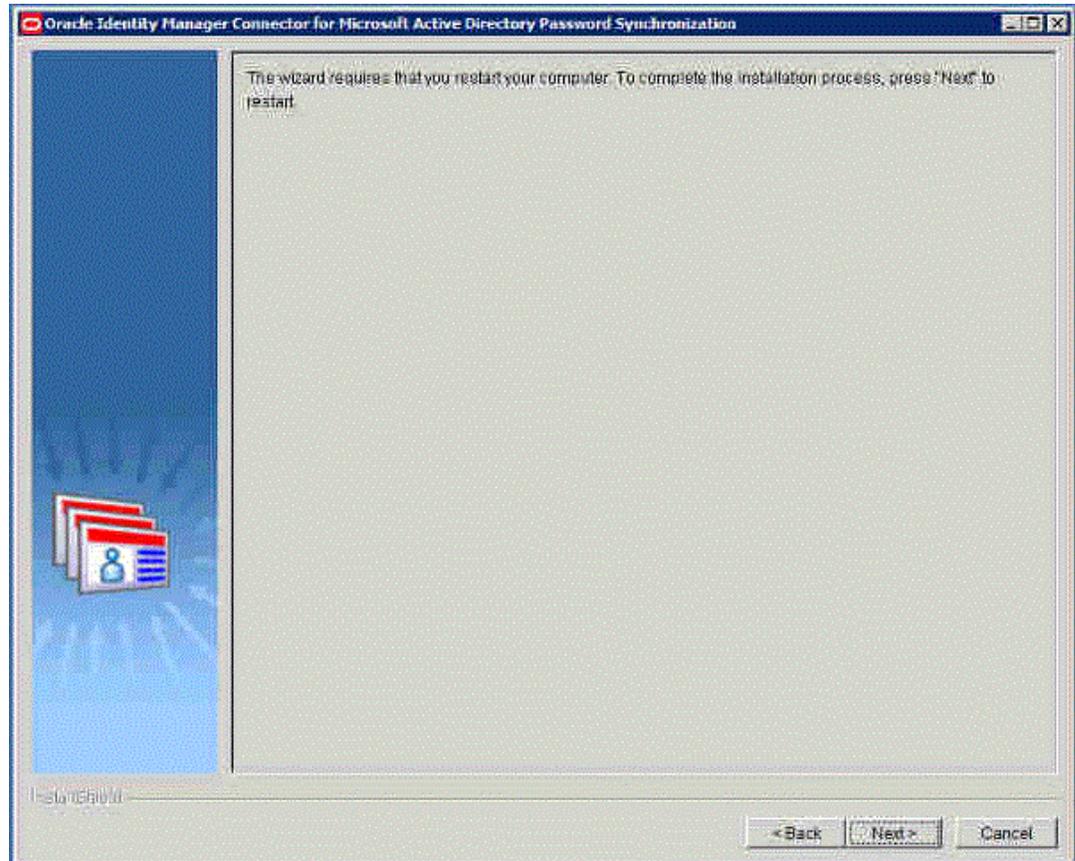
Clicking Next will force a restart. The restart is required to initialize the oimadpwdsync10.dll file. If the oimadpwdsync10.dll file is not initialized, then the connector is not ready for propagating passwords changes from target system to Oracle Identity Manager.

Microsoft Active Directory Configuration Parameters

Table 2-1 describes each configuration parameter of Microsoft Active Directory.

Table 2-1   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: `example.com`
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 organizationUnit, will be created within this container. Therefore, the base DN that you specify must be capable of holding `organizationalUnit` objects.
	Sample value: `DC=example,DC=com`
Port	Enter the port number at which LDAP for Microsoft Active Directory host computer is enabled.
	Default value: `389`

Table 2-1   (Cont.) Microsoft Active Directory Configuration Parameters

Parameter	Description
Host	Enter the IP address or the host name of the Microsoft Active Directory host computer. Sample value: `172.20.55.120`
Persistent Store	Enter the Distinguished Name of the Organizational Unit where the Persistent Store Container has to be created. Sample value: `ou=Org`

Oracle Identity Manager Configuration Parameters

Table 2-2 describes each configuration parameter of Oracle Identity Manager.

Table 2-2   Oracle Identity Manager Configuration Parameters

Parameter	Description
Host	Enter the IP address (not the host name) of the Microsoft Active Directory host computer. **Note:** The host name must be accessible from the Microsoft Active Directory host computer. Sample value: `oimhost`
Port	Enter the number of the port at which the Oracle Identity Manager SPML Web service is listening. Sample value: `8080`
Administrator Login	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.
Administrator Password	Enter the password of the account that will be used by the connector to login to Oracle Identity Manager during a password synchronization operation.
OIM User Attribute	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. Note that the corresponding column in the USR table on the Oracle Identity Manager Database must be unique. During password synchronization, the sAMAccountName value of the user whose password is changed is compared against values in this column. Sample value (for predefined OIMUser fields): `Users.User ID` For user-defined OIMUser fields, you can use the USR_UDF_*FIELD_NAME* format. Sample Value: `USR_UDF_USERNAME` See the "Metadata Column Codes" appendix in *Oracle Identity Manager API Usage Guide* for information about the mapping between the physical column names and metadata column codes.
OIM Application Server Type	Select the name of the application server that hosts Oracle Identity Manager. Sample value: `JBoss`
Use SSL	Select Yes, if you are going to configure SSL communication between Microsoft Active Directory and Oracle Identity Manager. Otherwise, select `No`. Default value: `Yes` **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" for information about enabling SSL.

Table 2-2   (Cont.) Oracle Identity Manager Configuration Parameters

Parameter	Description
Client Certificate Subject Name	Enter a value for this parameter only if `Use SSL` parameter has been set to `Yes` and client authentication is required by the application server. Enter a string that identifies the client certificate that must be used for SSL. Sample value: `TQL17` Here, TQL17 is the Issued To value in the certificate.

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_STAMP*OIMMain.log file by performing the procedure described in "Enabling and Disabling Logging".

2. Check if the *TIME_STAMP*OIMMain.log file is generated in the path specified in the Log File Path field while performing Step 8 of "Installing the Connector".

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

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 2-8 shows the Active Directory Configuration Parameters page on which sample values have been specified.

Figure 2-8   Active Directory Configuration Parameters (Reconfiguration)
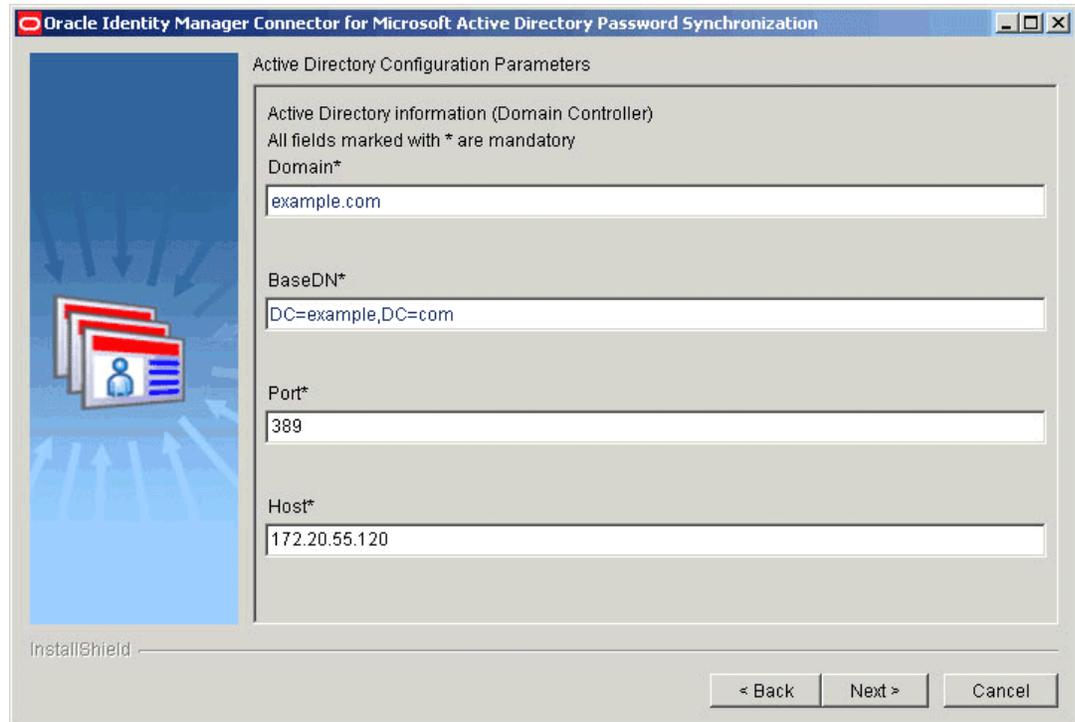
4. Click **Next.**

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 2-9 displays the Oracle Identity Manager Configuration Parameters page on which sample values have been specified.

Figure 2-9   Oracle Identity Manager Configuration Parameters Page (Reconfiguration)

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 2-10 is a screenshot of the Configuration Parameters page on which sample values have been specified.

Figure 2-10   Configuration Parameters Page (Reconfiguration)

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 2-11 is a screenshot of the second Active Directory Configuration Parameters page on which sample values have been specified.

Figure 2-11   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.

Postinstallation

You must perform the following steps after you install the connector:

- 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
- Excluding Users for Password Synchronization

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 section contains the following topics:

- Log Files
- Enabling or Disabling Logging

Log Files

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: `2009318O1311828_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_STAMP*OIMMain.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_STAMP*OIMMain.log file name, *TIME_STAMP* represents the time at which the log file was created in the `YearMonthDay` format.

    Sample value: `2009318OIMMain.log`

    The *TIME_STAMP*OIMMain.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.

Enabling or Disabling 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.

To enable or disable logging:

> ⓘ **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_STAMP*OIMMain.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.

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 (for example, 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.

> ⓘ **Note**
>
> This procedure is not applicable if you are using release 11.1.1.*x* or 12.2.1.3.*x* of the Microsoft Active Directory 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.

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.
>
> - This procedure is not applicable if you are using release 11.1.1.*x* or 12.2.1.3.*x* of the Microsoft Active Directory User Management connector.

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

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:

   - For Oracle Identity Manager release 9.1.0.*x:*

     a. Log in to the Oracle Identity System Administration.

     b. Expand **Resource Management,** and then click **Manage IT Resource.**

   - For Oracle Identity Manager release 11.1.1:

     a. Log in to the Oracle Identity System Administration.

     b. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.

     c. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource.**

   - For Oracle Identity Manager release 11.1.2.*x:*

     a. Log in to Oracle Identity System Administration.

     b. In the left pane, under Configuration, click **IT Resource**.

2. In the IT Resource Name field on the Manage IT Resource page, enter ADITResource and then click **Search.**

3. Click the edit icon for the IT resource.

4. From the list at the top of the page, select **Details and Parameters.**

5. 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.

6. 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`.

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.

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.
>
> • If Microsoft Active Directory is running on Windows Server 2008 R2, then you must install all available Windows updates and apply the Easy fix provided on the Microsoft Support page for enabling TLS 1.2 at https://support.microsoft.com/en-us/help/3140245/update-to-enable-tls-1-1-and-tls-1-2-as-a-default-secure-protocols-in.
>
>   If you do not do so, then Transport Layer Security (TLS) 1.2 connection is not enabled for SSL with Oracle Identity Governance 12c (12.2.1.3.0) Server and password sync fails due to SSL handshake issues.

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](#)

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](#)

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 *WEBSPHERE_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\websp.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.

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") 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.

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

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.

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
```

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 IDENITTY_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
```

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 IDENITTY_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
```

Importing the Certificate

To import the application server certificate:

1.   Copy the certificate (exported in "Exporting the Certificate") 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.

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.

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

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.

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.

Exporting the Certificate

To export the application server certificate from the *WALLET_LOCATION* directory that you specified in Step 1 of Enabling SSL for HTTP Communication to Oracle HTTP Server, 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 Enabling SSL for HTTP Communication to Oracle HTTP Server) 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

Importing the Certificate

To import the application server certificate:

1. Copy the certificate (exported in Step 3 of Enabling SSL for HTTP Communication to Oracle HTTP Server) 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.

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 Oracle 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.

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
```

Signing the Certificate

The procedure to sign a certificate and import the self-signed certificate as a trusted entry in the Java standard store is as follows:

1. Use the following command to sign a certificate:

```
keytool -selfcert -alias PRIVATE_KEY_ALIAS -sigalg MD5withRSA -validity2000 -keypass
PRIVATE_KEY_PASSWORD -keystore IDENTITY_STORE_FILE -storepass
IDENITTY_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. Use the following command to import the certificate (signed in Step 1) as trusted entry in
   the Java standard store:

```
keytool -importcert -trustcacerts -alias PRIVATE_KEY_ALIAS -file CERT_FILE_NAME  -
keystore JAVA_STANDARD_TRUST -storepass JAVA_STANDARD_STORE_FILE_PASSWORD
```

The following is a sample command:

```
keytool -importcert -trustcacerts -alias support -file
C:\bea\user_projects\domains\oim\supportcert.pem -keystore
c:\jdk-6u25\jre\lib\security\cacerts -storepass changeit
```

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 IDENITTY_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
```

Configuring Custom Identity Keystore in Oracle 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.

> ⓘ **Note**
>
> If Oracle WebLogic Server is deployed on Oracle Identity Manager release 11.1.1 or 11.1.2.*x,* then the default port is 14001.

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 region, click **Lock & Edit** to enable modification to the settings on the page.

   b. From the **Keystores** box, perform one of the following steps:

      • If Oracle WebLogic Server is deployed on Oracle Identity Manager release 9.1.0.*x,* then select **Custom Identity and Custom Trust**, and then click **Continue.**

      • If Oracle WebLogic Server is deployed on Oracle Identity Manager release 11.1.1 or 11.1.2.*x,* then select Custom Identity and Custom Trust or **Custom Identity and Java Standard 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 region, 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. Click the **Advanced Properties** tab, and select **Client Certs not Requested** from the dropdown list, and save the changes.

8. Restart the server for the changes to take effect.

> ⓘ **Note**
>
> For a clustered installation, repeat all the steps on each node of the cluster. Then, restart each node.

Importing the Certificate

To import the application server certificate:

1. Copy the certificate (exported in "Exporting the Certificate") 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.

Excluding Users for Password Synchronization

> ⓘ **Note**
>
> You can perform this procedure only if you are using the latest 9.1.1.5.*x* patch for the connector.

By default, the connector captures all passwords changed on the target system and propagates them to Oracle Identity Manager. If you do not want the connector to propagate the password changes to Oracle Identity Manager for certain users, then you must configure the connector to use the ADUsrExclusionFilter config parameter. In other words, by using the AD UsrExclusionFilter config parameter, you can configure the connector to filter AD users whose password changes must not be propagated to Oracle Identity Manager.

To configure the ADUsrExclusionFilter config parameter to exclude AD Users for password synchronization with Oracle Identity Manager:

1. Open the system registry by running the `regedit.exe` command.

2. Navigate to the following registry key:

   `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\oimpwdsync\OIMConfig`

3. In the right pane, double-click the **ADUsrExclusionFilter** value.

4. In the Value data field of the Edit String dialog box, enter a filter string value for all AD users that the connector must exclude for password synchronization.

   Consider the following examples:

   - If you want to exclude all AD users whose account name contains "xyz", then enter `(samAccountName=*xyz*)`.

   - If you want to exclude a specific user whose account name is johndoe, then enter `(samAccountName=johndoe)`.

   - If you want to exclude more than one user, then enter `(|(samAccountName=johndoe)(samAccountName=richardroe)(samAccountName=janedoe))`.

   If the Value data field is empty, then the exclusion filter is disabled.

   > ⓘ **Note**
   >
   > You can apply filters only for User objects. Filtering records for password synchronization based on attributes of other objects such as Groups, Organizational Units, and so on is not supported.

3

Removing the Connector

This chapter describes the procedure to remove the connector installation for release 9.1.0.1 and 9.1.1.x.

- [Removing an Existing Installation of Release 9.1.0.1](#)
- [Removing an Existing Installation of Release 9.1.1.x](#)
- [Uninstalling Release 9.1.1.5.x of the Connector](#)

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.

Removing an Existing Installation of Release 9.1.1.x

To remove an existing installation of the release 9.1.1.x 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.

> **ⓘ Note**
>
> see [PrepAD.ldif](#) for more information about the prepAD.ldif file.

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, click **Uninstall a program** listed under Programs.

4. In the Programs and Features window, select **Oracle Identity Manager Connector for Microsoft Active Directory Password Synchronization** from the list of currently installed programs, right click it, and then click **Uninstall**.

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**.

[Summary Page for Removing the Connector](#) shows the Summary page for removing the connectors.
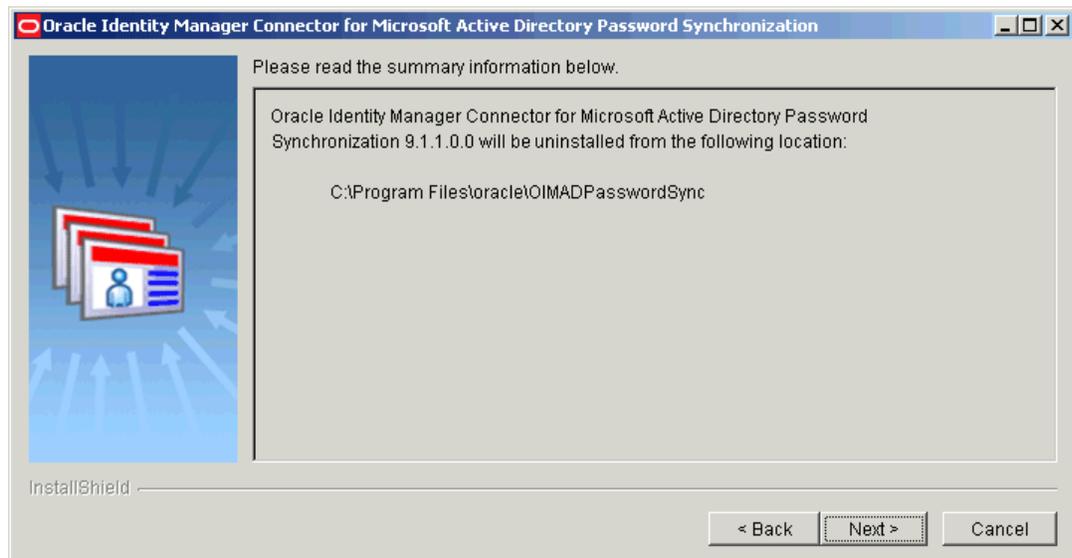
7. On the next page, click **Next**.

8. On the subsequent page, click **Next**. This will restart your computer.

9. 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.

Uninstalling Release 9.1.1.5.x of the Connector

If you want to to cancel an ongoing 9.1.1.5.0 installation or if you want to manually remove an existing installation of the 9.1.1.5.x connector, then perform the following steps before restarting the domain controller:

1. Delete the connector-related registry keys as follows:

   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. Remove oimadpwdsync10 from the list of values, and click **OK**.

   > ⓘ **Note**
   >
   > Do not remove other existing values in the "Notification Packages" key data.

2. Remove oimadpwdsync10 from the list of values in "Notification Packages" key under "HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa" .

3. Move the oimadpwdsync10.dll and orclmessages.dll from the C:\WINDOWS\system32 directory to a different location (C:\SomeOtherLocation).

4. Reboot Windows Server by running the following command:

   `%WINDIR%\System32\shutdown.exe /r /t 0`

5. Remove the following registry key including its sub entries under it:

   `[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\oimpwdsync]`

6. Delete the oimadpwdsync10.dll, orclmessages.dll files, and logs directory.

4

Troubleshooting the Connector

This chapter discusses the solutions to the common problems that you might encounter.

Table 4-1 lists the solutions to issues associated with the connector.

Table 4-1   Troubleshooting the Connector

Problem	Solution
The following issue is encountered while configuring SSL on Oracle WebLogic Application Server: Oracle Identity Manager becomes unavailable.	The certificate creation procedure that is performed using the keytool command, must contain –dname="CN=OIMHOST" which must be exactly the same as the OIMHost parameter in the password configuration. The password configuration can be viewed by using the Registry Editor in the following location: `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\oimpwdsync\OIMConfig`
The InstallShield Preparing Java step fails and prevents the connector from being installed.	Install the Windows Enhanced Mitigation Experience Toolkit (EMET) on the host and run the connector installer once again.

5
Known Issues and Workarounds

The following sections discuss issues and workarounds associated with the connector:

The oimpwdsync.log File is Retained with Reinstallation or Reconfiguration of Password Synchronization Connector

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.

There is no workaround available for this issue.

Issue with ASCII Characters in User Names

If a user name contains an extended ASCII character (ASCII value 128 onwards), then the connector does not update the password for the user and an error is encountered.

There is no workaround available for this issue.

Microsoft Active Directory Password Synchronization Connector Creates a Dummy User During Installation

During installation, the Microsoft Active Directory Password Synchronization Connector creates **oidtmpuser** - a dummy user, and deletes it immediately. This user is created to verify if the primary Active Directory administrative user has the required administrator privileges or not.

There is no workaround available for this issue.

A

PrepAD.ldif

This file is generated in the installation directory when the connector is installed. It creates the Persistent Store in the Active Directory where the user data (User ID and Password) is stored, if the Password Reset fails in Active Directory.

It uses LDAP Data Interchange Format (LDIF) commands to create the organizational unit in Active Directory.

For example:

```
dn: CN=John Doe, OU=Training, DC=domain, DC=com
changetype: add
cn: John Doe
objectClass: user
samAccountName: John
givenName: John
sn: Doe
```

Index