Oracle® Identity Manager

Password Synchronization Module for Microsoft Active Directory
Installation and Configuration Guide

Release 9.0.1

B31129-01

June 2006

ORACLE®

Oracle Identity Manager Password Synchronization Module for Microsoft Active Directory Installation and Configuration Guide, Release 9.0.1

B31129-01

Contents

Preface

Oracle Identity Manager Password Synchronization Module for Microsoft Active Directory Installation and Configuration Guide provides information about installing and configuring the Oracle Identity Manager Password Synchronization Module for Microsoft Active Directory. This guide also provides instructions for updating an existing instance of the module to the current D version.

> **Note:** This is a transitional release following Oracle's acquisition of Thor Technologies. Some parts of the product and documentation still refer to the original Thor company name and Xellerate product name and will be rebranded in future releases.

Audience

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

Documentation Accessibility

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

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

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

Related Documents

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

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation and Upgrade Guide for JBoss*
- *Oracle Identity Manager Installation and Upgrade Guide for WebLogic*
- *Oracle Identity Manager Installation and Upgrade Guide for WebSphere*
- *Oracle Identity Manager Administrative and User Console Guide*
- *Oracle Identity Manager Administrative and User Console Customization Guide*
- *Oracle Identity Manager Design Console Guide*
- *Oracle Identity Manager Tools Reference Guide*
- *Oracle Identity Manager Audit Report Developer Guide*
- *Oracle Identity Manager Best Practices Guide*
- *Oracle Identity Manager Connector Framework Guide*
- *Oracle Identity Manager Connector Guide for Microsoft Active Directory*
- Connector guides for various other third-party applications

Documentation Updates

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

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

Conventions

The following text conventions are used in this document:

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.

1

Overview of the Password Synchronization Module

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

This chapter contains the following sections:

- Components for Connecting Oracle Identity Manager to Microsoft Active Directory

- Files and Directories That Comprise the Password Synchronization Module

Components for Connecting Oracle Identity Manager to Microsoft Active Directory

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

- Connector for Microsoft Active Directory

- Password synchronization module for Microsoft Active Directory

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

The following table compares the functionality offered by both tools.

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

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

The following figure illustrates the functionality of the connector for Microsoft Active Directory.
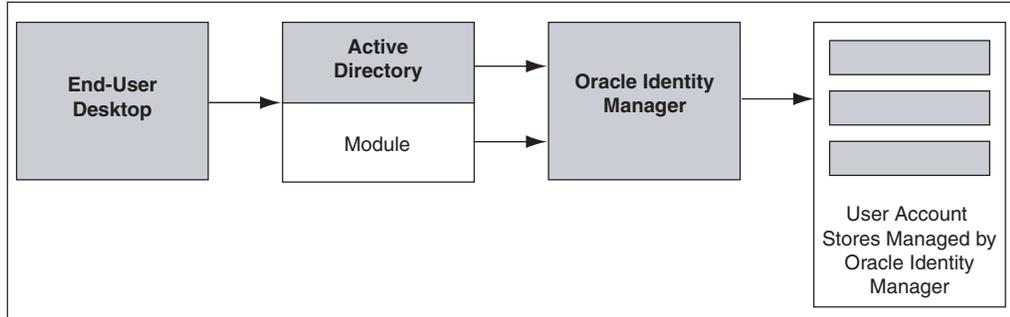
The password synchronization module for Active Directory updates password changes made only in Active Directory.

The following figure illustrates the functionality of the password synchronization module for Microsoft Active Directory.
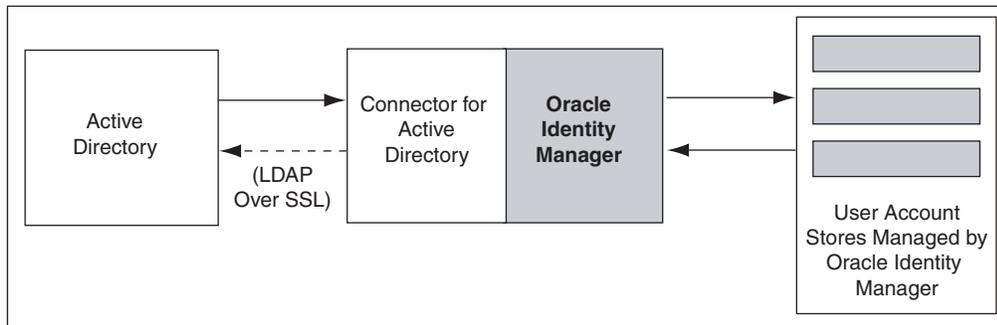
Files and Directories That Comprise the Password Synchronization Module

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

```
Directory Servers\Microsoft Active Directory\Microsoft Active Directory Password
Sync Rev 4.4.0.zip
```

These files and directories are listed in the following table.

Directory in the Installation Media	Contents
jpclient\lib	■ XellerateClient.jar ■ xlAPI.jar ■ xlAuthentication.jar ■ xlCache.jar ■ xlCrypto.jar ■ xlDataObjectBeans.jar ■ xlLogger.jar ■ xlUtils.jar ■ xlVO.jar
xlhome\ext	■ aixppk.jar ■ as400ppk.jar ■ engine.jar ■ genericunixppk.jar ■ hpuxppk.jar ■ linuxppk.jar ■ macosxppk.jar ■ solarisppk.jar ■ win32ppk.jar ■ windowsppk.jar
xlhome\install	■ xlCryptoMy.jar ■ xlCustom.jar ■ xlInstaller.jar
docs	■ docs\B31129_01.pdf ■ docs\html

2

Deploying the Password Synchronization Module

This guide covers two scenarios:

- Upgrading an existing instance of the password synchronization module to the current version, which is Revision D

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

- Installing and configuring Revision D of the password synchronization module

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

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

- Step 1: Preparing to Install the Password Synchronization Module
- Step 2: Enabling Password Policies for Active Directory
- Step 3: Installing the Password Synchronization Module
- Step 4: Performing Postinstallation Steps for the Password Synchronization Module
- Step 5: Configuring the Password Synchronization Module

Step 1: Preparing to Install the Password Synchronization Module

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

- An instance of Oracle Identity Manager release 8.5.3 or later is installed, running, and visible to the computer hosting the Active Directory domain controller on which you want to install the password synchronization module.

  > **See Also:** Depending on the application server that you use, refer to one of the following guides:
  >
  > *Oracle Identity Manager Installation and Upgrade Guide for JBoss*
  >
  > *Oracle Identity Manager Installation and Upgrade Guide for WebLogic*
  >
  > *Oracle Identity Manager Installation and Upgrade Guide for WebSphere*

- If the Oracle Identity Manager server to which Active Directory will connect is hosted by an IBM WebSphere application server, then you must install on the computer where you are installing the password synchronization module an

instance of the IBM WebSphere Application Client that is compatible with the installed version of the IBM WebSphere application server.

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

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

Item	Requirement
Microsoft Active Directory	Active Directory Server
Host operating system	Any one of the following:
	■ Microsoft Windows 2000, Server Edition with SP4
	■ Microsoft Windows Server 2003

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

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

```
Directory Servers\Microsoft Active Directory\Microsoft Active Directory Password
Sync Rev 4.4.0.zip
```

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

> **See Also:** Refer to the "Files and Directories That Comprise the Password Synchronization Module" section on page 1-2 for more information about these files.

Step 2: Enabling Password Policies for Active Directory

To activate password policies for Active Directory:

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

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

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

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

3. Select **Security Settings,** select **Account Policies,** and then click **Password Policy.** The Security Policy Setting dialog box is displayed.

4. In the Security Policy Setting dialog box, select **Define this policy setting,** select **Enabled,** and then click **OK.**

Step 3: Installing the Password Synchronization Module

To install the password synchronization module:

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

   a. Open Microsoft Windows Explorer.

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

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

2. Read the text on the Welcome page, and then click **Next.**

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

   `C:\OracleProvisioningAD`

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

4. Click **Next.**

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

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

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

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

6. On the WebSphere Directory page, specify the path to the directory where the IBM WebSphere Application Client is installed, on the computer where you are installing the module. Then, click **Next.**

7. On the JRE page, specify the JRE option that you want to use with the module. The following choices are available:

   ■ JRE bundled with Oracle Identity Manager

■ An existing JRE 1.4.2 installation on the computer where you are installing the password synchronization module. The following table lists the appropriate JRE version for the supported application servers.

Application Server	Required JRE	Comments
JBoss Application Server	Sun JRE 1.4.2_09 or later	However, all versions of Sun JRE 1.5 are *not* supported.
BEA WebLogic	Sun JRE 1.4.2_09 or later	However, all versions of Sun JRE 1.5 are *not* supported.
IBM WebSphere	IBM JRE 1.4.2_*x*	Available as part of the IBM WebSphere Application Client installation

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

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

The default account for login is `xelsysadm`.

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

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

■ The host name of the application server hosting Oracle Identity Manager

■ The naming port associated with the application server. The following table lists the default naming ports for the supported application servers.

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

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

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

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

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

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

11. The Complete page displays the following message to indicate successful installation:

```
The Oracle Identity Manager Installer has successfully
installed Oracle Identity Manager AD Password
Synchronization.
```

Click **Finish** to close the installer.

12. Restart the computer.

Files Copied During the Password Synchronization Module Installation

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

File	Description
Windows_System32_Directory\Adsync.dll	This file is registered as a listener for password changes to the Active Directory Domain controller. Whenever an Active Directory password is changed, it calls the Change Password script named `ChangePassword.cmd.`
ADSYNC_HOME\config\xlconfig.xml	This file contains all the user-configurable settings for the password synchronization module. Users can edit this file after installing the module. For details, see the "Step 5: Configuring the Password Synchronization Module" section on page 2-6.
ADSYNC_HOME\lib\xliADSync.jar	This JAR file contains the class files required by the Change Password script.
ADSYNC_HOME\ChangePassword.cmd	This script, which is called by `adsync.dll` in response to a password change, uses the correct classpath and command-line parameters to call the `ChangePassword` class, which is in the `xliADSync.jar` file.
ADSYNC_HOME\wsChangePassowrd.cmd	This is the version of the Change Password script that is used by IBM WebSphere.
ADSYNC_HOME\lib\xliADSync.ear	This file contains the class files required by the version of the Change Password script used by IBM WebSphere.

Step 4: Performing Postinstallation Steps for the Password Synchronization Module

Perform the following postinstallation steps:

1. On the computer on which Oracle Identity Manager is installed:

    a. Navigate to the root installation directory for Oracle Identity Manager.

    b. Copy the following files from the ext directory to the *ADSYNC_HOME*\ext directory on the computer where you installed the password synchronization module:

    `javagroups-all.jar` (or `jgroups-all.jar`)

    `oscache-2.0.2-22Jan04.jar` (or `oscache.jar`)

    c. Copy the `javagroups-all.jar` or `jgroups-all.jar` file (whichever of these files exists in the \ext directory) to the *ADSYNC_HOME*\ext directory on the computer where you installed the password synchronization module.

    d. Copy the `oscache-2.0.2-22Jan04.jar` or `oscache.jar` file (whichever of these files exists in the \ext directory under the root installation directory of Oracle Identity Manager) to the *ADSYNC_HOME*\ext directory on the computer where you installed the password synchronization module.

2. Determine the file appropriate for the particular application server hosting your Oracle Identity Manager server, and copy this file from the computer hosting

Oracle Identity Manager to the appropriate directory on the computer where you installed the password synchronization module.

The following table lists the application server-specific file that should be copied as well as the destination to which the file should be copied.

Application Server	File to Be Copied
JBoss Application Server	`jbossall-client.jar`
BEA WebLogic	`weblogic.jar`

3. Copy the JAR files from the *XLCLIENT_HOME*\lib directory on the computer hosting the Oracle Identity Manager Design Console to the *ADSYNC_HOME*\lib directory on the computer where you install the password synchronization module.

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

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

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

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

   In the `xlconfig.xml` file, change the `<java.naming.provider.url>` tag to the value stored in the tag in the `xlconfig.xml` file associated with the instance of the Design Console that you have previously installed as part of the Oracle Identity Manager deployment.

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

   ADSYNC_HOME\config\

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

Step 5: Configuring the Password Synchronization Module

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

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

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

The following example provides a listing of the original (default) contents of the `<ADSync>` tag:

```
<ADSync>
 <!--
 The Login section provides information about how the utility is authenticated.
 If UseSignature is true, the username is used for authentication, using the
 signature-based login. The key in the "PrivateKey" alias will be used.
 If UseSignature is false, the username and password are used for
 authentication.
 -->
 <Login>
  <UseSignature>false</UseSignature>
  <Username>xelsysadm</Username>
  <Password encrypted="true">tPzEM127PIQxO64w2g7wgw==</Password>
 </Login>
 <!--
 The Active Directory name should match an Oracle Identity Manager user name.
 If the MatchingMethod is UserID, the Active Directory user name is assumed to be
 the Oracle Identity Manager user name.
 For UDF, FieldName must contain the name of the User Defined field that
 contains the active directory user ID.
 For ResourceField, Process Forms of those Users who have ResourceObject
```

```
    specified will be searched to find the suitable user. This can be used if
    active directory is provisioned as an account, but not a trusted source.
    -->
    <UserMatch>
     <!-- UserID, UDF and ResourceField -->
     <MatchingMethod>UserID</MatchingMethod>
     <FieldName>UD_ADUSER_LOGIN</FieldName>
     <ResourceObject>AD User</ResourceObject>
    </UserMatch>
    <!--
    If required, a UDF field can be updated with the result of the operation and
    Timestamp so that additional workflow can be started.
    -->
    <Result>
     <UpdateUDF>false</UpdateUDF>
     <FieldName>USR_UDF_ADPWDRES</FieldName>
     <SuccessValue>SUCCESS</SuccessValue>
     <FailureValue>FAIL</FailureValue>
     <AppendTimeStamp>true</AppendTimeStamp>
    </Result>
</ADSync>
```

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

3

Upgrading the Password Synchronization Module

You can upgrade an existing password synchronization module to the current revision, which is revision D.

To upgrade to Revision D of the password synchronization module for Active Directory, complete the following procedures:

1. Refer to "Chapter 4" for instructions on removing an earlier instance of the password synchronization module.

2. Verify that your environment is ready for the Revision D module by completing the procedure in the "Step 1: Preparing to Install the Password Synchronization Module" section on page 2-1.

3. Complete the procedure in the "Step 2: Enabling Password Policies for Active Directory" section on page 2-2.

4. Complete the procedure in the "Step 3: Installing the Password Synchronization Module" section on page 2-3 to install the Revision D module on the computer hosting the Active Directory domain controller for which you want to implement password synchronization.

5. Complete the procedure in the "Step 4: Performing Postinstallation Steps for the Password Synchronization Module" section on page 2-5 to copy the required files from the computer hosting Oracle Identity Manager to the computer on which you install the password synchronization module.

4

Removing the Password Synchronization Module

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

1. On the computer hosting the Active Directory domain controller where the password synchronization module resides, start the Domain Security Policy application as follows:

    a. Click **Start.**

    b. Select **Programs,** and then select **Administrative Tools.**

    c. Click **Domain Security Policy.**

2. If you are working with Active Directory 2003, select **Window Settings**, on the left pane of the Domain Security Policy application window.

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

4. In the Security Policy Setting dialog box, select **Disabled**, and then click **OK.**

5. Delete the module-related registry keys by completing 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 item 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.

6.   Restart the computer.

7.   Delete the `ADSync.dll` file from the `WINDOWS\system32` directory.

8.   Delete the `ADSYNC_HOME` directory.

Index