Oracle® Fusion Middleware

Enterprise Single Sign-On Suite Installation Guide

11g Release 2 (11.1.2.2)

E37691-05

June 2014

ORACLE

Oracle Fusion Middleware Enterprise Single Sign-On Suite Installation Guide, 11g Release 2 (11.1.2.2)

E37691-05

Contents

5 Installing Provisioning Gateway

6 Installing Universal Authentication Manager

Preface

This guide explains how to prepare your environment for installation of each suite application, install each of the suite applications, and complete the necessary post-installation tasks.

Audience

This guide is intended for experienced administrators responsible for the planning, implementation and deployment of applications. Administrators are expected to have solid knowledge of directory environments, permission structures, domain administration, and databases.

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 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 more information, see the following documents in the Oracle Enterprise Single Sign-On Suite Release 11.1.2.2 documentation set:

- *Oracle Enterprise Single Sign-On Suite Release Notes*
- *Oracle Enterprise Single Sign-On Suite Administrator's Guide*
- *Oracle Enterprise Single Sign-On Suite Secure Deployment Guide*
- *Oracle Enterprise Single Sign-On Suite User's Guide*
- *Deploying Logon Manager with a Directory-Based Repository*
- *Configuring and Diagnosing Logon Manager Application Templates*

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

Before You Install Oracle Enterprise Single Sign-On Suite

Before you install Oracle Enterprise Single Sign-On Suite, read the information contained in this section carefully and follow it closely. This section contains the following topics:

1.1 Overview of the Oracle Enterprise Single Sign-On Suite Installation Process

Oracle Enterprise Single Sign-On Suite handles all tasks related to granting users access to applications, including automatic sign-on, application password change, Windows password reset, kiosk session management, application credential provisioning, as well as strong authentication inside and outside of the session.

Oracle Enterprise Single Sign-On Suite consists of the following components:

- **Logon Manager** - provides single sign-on functionality.
- **Provisioning Gateway** - provides remote credential provisioning capability.
- **Password Reset** - provides the self-service password reset ability. Consists of the following components:
  - **Password Reset Client** - installed as a selectable component during the Logon Manager installation.
  - **Password Reset Server** components.
- **Kiosk Manager** - provides session and application management for kiosk environments.
- **Universal Authentication Manager** - provides strong authentication inside and outside the Windows session.
- **Anywhere** - provides the ability to deploy custom-configured installation packages to end-user workstations not connected to the enterprise network.

The following is a high-level overview of the suite installation process:

Note: If this installation is an upgrade, please refer to the "Upgrading an Existing Installation..." section for the selected component(s).

---

1. Determine which components of the Oracle Enterprise Single Sign-On Suite and their features you will be installing, based on the business requirements of your organization.
2. Ensure that supporting software listed in Required Supporting Software has been installed on the target machine(s). Refer to the *Oracle Enterprise Single Sign-On Suite Release Notes* for a per-application list of requirements.
3. Obtain and decompress the appropriate installer archive. See Contents of the Oracle Enterprise Single Sign-On Suite Master Archive for the description of its contents.
4. Complete the installation steps in this guide for each component you've chosen to install.
5. If any problems arise during the installation or post-installation tasks, see Troubleshooting Oracle Enterprise Single Sign-On Suite Installations.

1.2 Required Supporting Software

In order to install and function properly, the Oracle Enterprise Single Sign-On Suite applications require the following third-party supporting software to be installed on the target machines if it has not already been installed:

- The Windows Installer InstallScript redistributable. This package is required by all Suite application installers; you must install this package unless your machine already has it installed. It can be obtained from http://consumerdocs.installshield.com/selfservice/viewContent.do?externalId=Q108322.
- The Microsoft .NET 4.0 "Full Profile" framework. This package is required by Logon Manager and the Administrative Console; you must install it if your machine does not already have the .NET Framework version 4.0 installed. It can be obtained from http://www.microsoft.com/en-us/download/details.aspx?id=17718
- The Microsoft .NET 3.5 SP1 framework. This software is required by Provisioning Gateway Server. It can be obtained from http://www.microsoft.com/en-us/download/details.aspx?id=22
- The latest 32-bit Java Runtime Environment. Required by the Java-based help system.

1.3 Contents of the Oracle Enterprise Single Sign-On Suite Master Archive

The following section describes the purpose of the files contained in the Oracle Enterprise Single Sign-On Suite master archive. The archive contains the following folders:

- Logon Manager
- Password Reset
- Provisioning Gateway
- Universal Authentication Manager
- Anywhere
- Reporting

The archive root also contains a PDF file, "ESSRN.PDF," which contains the product release notes.

1.4 Contents of the Logon Manager Folder

The contents of this folder are as follows:

- **ESSO Administrative Console.msi** - the Oracle Enterprise Single Sign-On Administrative Console installer.
- **ESSO-LM.msi** - the 32-bit Logon Manager installer.
- **ESSO-LMx64.msi** - the 64-bit Logon Manager installer.
- **BIP Reports** - report files for generating usage reports for Oracle Enterprise Single Sign-On Suite applications with Oracle Business Intelligence Publisher.
- **Language Transforms** - MSI installer language transform files that allow you to launch the Logon Manager installer in a specific supported language.
- **Utility** - folder that contains supplementary software and unsupported Logon Manager troubleshooting tools. These are:
  - **SSOHiddenWindowResponse.exe**- the Hidden Window Response utility. Use this utility to allow Logon Manager to detect hidden application windows by window title and class. For more information, see the guide, Using the Hidden Window Response Utility, available in the online documentation center.
  - **ssoSCDetect.exe** - SmartCard detection tool. When troubleshooting logon issues with the SmartCard authenticator, run this tool to determine whether Logon Manager can see an inserted SmartCard.
  - **TraceController.exe** - the Trace Controller utility. Use this utility to enable and manage trace logging in Logon Manager and other Oracle Enterprise Single Sign-On Accelerator Suite applications.
- **Logon Manager Event Viewer.msi** - the Logon Manager Event Viewer installer. Installs and registers the messaging libraries required to view Logon Manager events in the Windows Event Viewer.

For more information, see the *Oracle Enterprise Single Sign-On Suite Administrator's Guide*.

1.4.1 Contents of the Password Reset Folder

The contents of this folder are as follows:

- **ESSO-PR_Server.msi**- 32/64-bit installer for the Password Reset server-side software.

1.4.2 Contents of the Provisioning Gateway Folder

The contents of this folder are as follows:

- **ESSO-PG_ClientCLI.msi** - 32-bit installer for the Provisioning Gateway command-line interface client-side software. Note that installation on 64-bit environments is not supported.
- **ESSO-PG_Server.msi**- 32/64-bit installer for the Provisioning Gateway server-side software.

1.4.3 Contents of the Universal Authentication Manager Folder

The contents of this folder are as follows:

- **ESSO-UAM.msi** - the 32-bit installer for Universal Authentication Manager.
- **ESSO-UAM-64.msi** - the 64-bit installer for Universal Authentication Manager.
- **Language Transforms** - MSI installer language transform files that allow you to launch the Universal Authentication Manager installer in a specific supported language.
- **SmartCard** - contains .reg files that enable supported smart cards.
- **ProximityCard** - contains .reg files that enable supported proximity cards.
- **Utility** - contains the command-line and graphical configuration tools, DeployTool.exe and ConfigEditor.exe, their supporting files, as well as documentation describing their use.

1.4.4 Contents of the Anywhere Folder

The contents of this folder are as follows:

- **Console** - contains the Anywhere Console installer MSI file.
- **Utility** - contains the VBS script file that adds the required MIME types to Microsoft IIS.

1.4.5 Contents of the Reporting Folder

The contents of this folder are as follows:

- **MSSQL** -Table setup scripts, stored procedure SQL scripts, and .NET stored procedures for the Microsoft SQL Server database.
- **ORACLE** -Table setup scripts, stored procedure SQL scripts, and Java stored procedures for the Oracle database.

2

Installing the Oracle Enterprise Single Sign-On Administrative Console

When installing on Windows XP, you must install the latest root certificate update from Microsoft, otherwise the installation will fail. For instructions, see the following Microsoft Knowledge Base article: http://support.microsoft.com/kb/931125

2.1 Installing the Console

To install and configure the Oracle Enterprise Single Sign-On Administrative Console:

1. Close all programs.
2. Execute the **ESSO Administrative Console.msi** installer file.
3. Wait while the installer loads.
4. On the Welcome Panel, click **Next>**.
5. Select a setup type. The **Complete** option installs all program features. The **Custom** option allows you to choose which program features to install and where they will be installed. If you will be performing a custom installation, go to step 6. If not, go to step 7.
6. If you are performing a custom setup, choose from the following installation options:
   - To install the Console, click **ESSO Administrative Console** and select **This feature and all of its subfeatures will be installed to the local hard drive**.
   - To install sample application templates, click **Templates** and select This feature and all of its subfeatures will be installed to the local hard drive.
   - To change the installation folder, click **Change** and navigate to the desired destination folder, then click **OK.**
   - For help with the installation options, click **Help**.

   When you have finished making your selections, click **Next**.
7. The InstallShield Wizard is ready to begin the installation. Click **Install**.
8. Wait for the installation to complete. When the "Completed" screen appears, click **Finish**.

3

Installing Logon Manager

This section describes the steps necessary for installing Logon Manager. It covers the following topics:

3.1 Prerequisites for Installing Logon Manager

Before you install Logon Manager, ensure the prerequisites listed in this section have been satisfied.

> **Note:** Please refer to the latest release notes to find out about last-minute requirements or changes that might affect your installation.

3.1.1 Prerequisites for Installing Logon Manager

If you are installing Logon Manager on a 64-bit (x64) system, you must use the 64-bit installer files marked with the _x64 suffix. While the installers have been compiled for the 64-bit platform, Logon Manager itself is a 32-bit application that runs via the Windows-on-Windows 64-bit (WoW64) emulation engine and is installed into the "Program Files (x86)" parent directory. The 32-bit version of Logon Manager is fully compatible with the supported 64-bit operating systems listed below.

Oracle supports the installation of Logon Manager on the following 64-bit platforms:

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows XP
- Windows 7

If you plan to synchronize with a database, or have the Reporting Service store application events in a database, you must install the appropriate database client in order to allow Logon Manager to connect to the database instance. Additionally, if you are installing Logon Manager on a 64-bit system and plan to connect to an Oracle database, you must install the 32-bit version of the Oracle database client on the target end-user machine; otherwise, the Reporting Service will not be able to connect to the Oracle database.

Note: When installing on Windows XP, you must install the latest root certificate update from Microsoft, otherwise the installation will fail.

For details and instructions, see the following Microsoft Knowledge Base article: http://support.microsoft.com/kb/931125

3.1.2 Prerequisites for Unattended ("Silent") Installations

In order to successfully install Logon Manager in unattended ("silent") mode, the Windows Management Instrumentation (WMI) service must be running before the installer is executed.

To check whether the WMI service is running, and start it if necessary, do the following on each target machine:

1. Open the System Management Console.
2. Open the **Services** snap-in.
3. Navigate to the **Windows Management Instrumentation** service and check its status and startup mode.

Depending on the status, do one of the following:

- If the status is **Started**, the WMI service is running; proceed to the next section.
- If the status is blank, check the service's startup type and start it as follows:
  1. Double-click the service.
  2. In the properties box that appears, set the startup type to **Manual** or **Automatic**, as dictated by your environment and click **Apply**.
  3. Click **Start**. The status changes to **Started**.
  4. Click **OK** to close the service properties dialog box.

3.2 Upgrading an Existing Logon Manager Installation

This section provides information on upgrading an existing Logon Manager installation to the latest version.

Upgrading to Logon Manager 11.1.2 is supported for the following versions of Logon Manager:

- 11.1.1.2.x
- 11.1.1.5.x

Oracle fully supports installing version 11.1.2 of Logon Manager on top of existing installations of Logon Manager as listed above. The installer will uninstall the previous version automatically, and then proceed with installation of the new version. Refer to the sections in this guide for more information on installing both the Logon Manager Administrative Console and the Logon Manager Agent.

> **Note:** If the original installer was customized using the Logon Manager Administrative Console, you must customize the new installer in the same manner before performing the upgrade, otherwise your current Logon Manager settings will be overwritten by the defaults in the unmodified installer.
>
> Oracle recommends that you do not change the primary logon method during an upgrade, as such a change introduces unneeded complexity to the process. Changes to the primary logon method should be undertaken as a separate project.

The following are the basic recommended steps to upgrade to Logon Manager 11.1.2.

1. Perform a backup of your existing credentials.
2. Run your installation as outlined in the sections, Installing the Oracle Enterprise Single Sign-On Administrative Console and Installing the Logon Manager Client-Side Software.
3. If deploying on Microsoft Active Directory, set the Use secure location for storing user settings option under **Global Agent Settings > [TargetSettingsSet] > ADEXT** to **Yes** and publish this setting to the repository as an administrative override.

   > **Note:** Only deploy this override once all instances of Logon Manager have been upgraded to version 11.1.2.0.0 or above; otherwise, once Logon Manager 11.1.2.0.0 or above synchronizes with the repository, all previous versions will no longer be able to synchronize with the repository for that user. For more information on this setting, see the *Oracle Enterprise Single Sign-On Suite Secure Deployment Guide*.

4. Update all of your repository objects (policies, templates, and so on) to the latest data schema used by the latest version of Logon Manager as follows:
   a. Connect to your repository with the latest version of the Oracle Enterprise Single Sign-On Administrative Console.
   b. Retrieve all of your templates, policies, and any other data from the repository and into the Console.
   c. (Optional) Make any configuration changes in your templates and policies as desired.
   d. Publish all of the retrieved objects back to your repository.

   > **Note:** This procedure is mandatory and must be performed in a test environment before deploying Logon Manager to end-users. This is because the latest version of Logon Manager introduces a new data schema to its configuration objects, such as templates and policies, which is incompatible with objects created with previous versions of Logon Manager. Attempting to synchronize Logon Manager with a repository that has not been updated will result in data corruption. Oracle highly recommends that you create a separate OU in your repository to test your new configuration objects before deploying them enterprise-wide.

5. Restore your backed up credentials to the new installation.

   Note: The **Passphrase Suppression** setting is, as of the 11.1.5.1 release, configurable under **Global Agent Settings > [TargetSettingsSet] > Authentication > Windows v2 > Recovery Method**. The default is to display the passphrase. If you want to suppress the passphrase, you must change this setting.

   Note that if you have a custom passphrase suppression (a DLL that implements the Secondary Authentication API), this DLL must return a unique GUID from its GetID function. Also, you must set the:

   HKLM\Software\Passlogix\MsAuth\ResetMethods:ResetMethod GUID

   registry value to that GUID.

   See the *Oracle Enterprise Single Sign-On Suite Administrator's Guide* more details.

6. After the installer has finished and your credentials are restored, the upgrade is complete. Refer to the *Oracle Enterprise Single Sign-On Suite Release Notes* to learn about the new product features.

3.3 Installing the Logon Manager Client-Side Software

Note: If you have a previous version of Kiosk Manager installed and are updating it during this installation, you must first uninstall the previous Kiosk Manager using the Control Panel Add/Remove Programs or the Uninstall option of the earlier software installer.

For additional considerations with regard to Kiosk Manager, see the *Oracle Enterprise Single Sign-On Suite* Administrator's Guide.

To install and configure Logon Manager:

1. Close all programs.
2. Execute one of the following files to begin the installation:
   - **ESSO-LM.msi** for 32-bit installations.
   - **ESSO-LMx64.msi** for 64-bit installations.

   Note: If you are installing in a language other than English and would like to launch the installer in the desired language, execute the following command:

   msiexec /I <packagename>.msi TRANSFORMS=<language>.mst

   where `<packagename>` is the name of the Logon Manager installer MSI package, and <language>.mst is the name of the corresponding language transform file (included in the installer archive).

3. On the Welcome Panel, click **Next>.**

4. Select a setup type. **Typical** provides a path to select commonly used program features easily. **Advanced** provides a detailed tree view of all the program features available for installation. If you select a typical setup, go to step 6; for an advanced setup, go to step 7.

   Click **Next**.

5. The "Typical Setup" screen appears. Select your authentication methods and indicate whether you want to use multiple authenticators.

   Authentication methods. In order to authenticate a user and grant access to stored credentials, Logon Manager offers a number of authentication methods implemented as authenticator plug-ins, with the most common method being a user name and password. In Active Directory environments, Logon Manager supports this authentication method through its Windows Logon (WinAuth) v2 plug-in.

   If you are using a strong authentication method, refer to the *Oracle Enterprise Single Sign-On Suite Administrator's Guide* which describes specific settings that must be enabled within an authenticator to work with Logon Manager. It also describes all the Logon Manager Administrative Console settings and any steps that must be taken to integrate with Kiosk Manager.

   Multiple Authenticators. The Authentication Manager feature adds the capability to enable multiple logon methods to authenticate the user. These logon methods can be the standard Logon Manager supported logon methods such as LDAP and Windows Logon v2, or the strong authenticators such as smart cards, proximity devices, and RSA SecurID tokens.

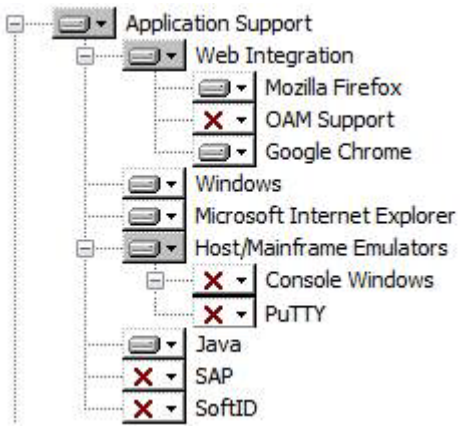
   Click **Next**.

6. Select your repositories and indicate which audit logging capabilities should be installed. If you install the Oracle Enterprise Single Sign-On Reporting Server, refer to the *Oracle Enterprise Single Sign-On Suite Administrator's Guide* for configuration information. Click **Next>** and continue to the next step.

7. If you are performing an advanced setup, choose from the following installation options:

Application Support

This option installs all necessary files and settings that serve as the core of the application, and allows you to select the application types for Logon Manager to interact with.



Web Integration	Helper objects that allow integration with Web browsers and external Web services.

Application Support	
Mozilla Firefox	Helper object that adds Logon Manager support for Mozilla-based browsers.
OAM Support	Helper object that adds Logon Manager support for Oracle Access Manager-protected browser applications.
Google Chrome	Helper object that adds Logon Manager support for the Google Chrome browser.
Windows	Support for Windows desktop applications. Windows support files are installed by default. These files cannot be deselected.
Microsoft Internet Explorer	Helper object that adds Logon Manager support for Internet Explorer. Installed by default.
Host/Mainframe Emulators	Helper object that adds Logon Manager support for HLLAPI-based emulators.
Console Windows	Support for Console windows (command prompt) within the Logon Manager mainframe plug-in.
PuTTY	Support for PuTTY windows within the Logon Manager mainframe plug-in.
Java	Helper object that adds native Logon Manager support for Java applications.
SAP	Helper object that adds SAP application support to Logon Manager.
SoftID	Helper object that adds Logon Manager support for SoftID applications. See the *Oracle Enterprise Single Sign-On Suite Administrator's Guide* for more information on using this feature. To use this helper object, the Authentication Manager authenticator must be installed and selected as your Primary Logon Method.

Authenticators

The authenticators are plug-ins that provide different methods for logging on to Logon Manager. By default, Windows Logon v2 is installed.

If you are installing Proximity Card, Read-Only Smart Card, RSA SecurID, Secure Data Storage, or Smart Cards, see the *Oracle Enterprise Single Sign-On Suite Administrator's Guide*.

Authenticators	
Windows Logon (deprecated)	Deprecated plug-in that enables logging on to Logon Manager by logon to Windows. Note: Do not install this component unless explicitly instructed to do so by Oracle support. It is being provided for legacy purposes only.
Windows Logon v2	Plug-in that enables logging on to Logon Manager by logon to Windows with secure passphrase support. This authenticator is installed by default.
GINA	Module that works with the Windows Logon v2 method. The GINA option is available only for Windows XP. You must select between GINA and Network Provider. It is not possible to install both methods.
LDAP	Plug-in that enables logging on to Logon Manager by logon to an LDAP directory.
LDAP v2	Plug-in that enables logging on to Logon Manager by logon to an LDAP directory. This plug-in also includes secure passphrase support.
Network Provider	Eliminates double authentication by utilizing the Network Provider mechanism to log on to Logon Manager. Supports all current Microsoft Windows operating systems. This feature has been moved to its own node, and is no longer a sub-feature of Windows Logon v2, as of version 11.1.1.5.1.
Proximity Card	Authenticator plug-in that supports authentication with HID Proximity Cards.
Smart Card	Plug-in that enables logging on to Logon Manager using MS-CAPI-capable smart cards.
Smart Card (Read-Only)	Plug-in that enables logging on to Logon Manager using a Read-Only Smart Card.
RSA SecurID	Plug-in that enables logging on to Logon Manager using one-time passwords generated by RSA SecurID tokens.
Local Authentication Toolkit	Components needed to perform RSA SecurID authentication.
Authentication Manager	This feature adds the capability to allow multiple logon methods to authenticate the user. If you want to use the Enrollment, Grade, and Order functionality, you must install this feature.

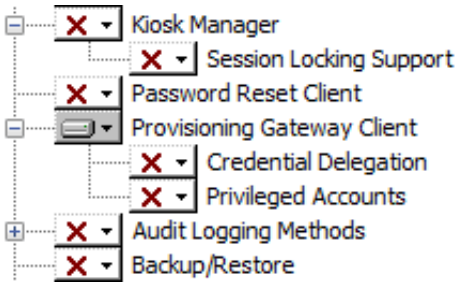
Synchronizers

This plug-in provides for the management of synchronization extensions to the application.

The available synchronization plug-ins are:

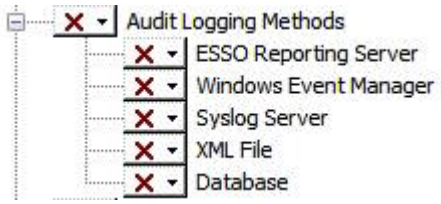
Microsoft Active Directory	Synchronization plug-in that supports storage and retrieval of credentials and settings from an Active Directory server.
Microsoft AD LDS (ADAM)	Synchronization plug-in that supports storage and retrieval of credentials and settings from an AD LDS (ADAM) server.

Synchronizers	
LDAP	Plug-in that supports storage and retrieval of credentials and settings from an LDAP-compliant directory, such as Oracle Identity Manager.
Database	Synchronization plug-in that supports storage and retrieval of credentials and settings from a database.
Roaming Profile (deprecated)	Synchronization plug-in that supports roaming profiles. Do not install this component unless explicitly instructed to do so by Oracle support. It is being provided for legacy purposes only.
File System	Synchronization plug-in that supports storage and retrieval of credentials and settings from a file share.

Kiosk Manager	
Kiosk Manager Plug-in that is available to support kiosk scenarios.	 To use Kiosk Manager, you must install the LDAP Authenticator and a synchronizer. You must also ensure that Windows Authenticator v2 is not installed. Refer to the *Oracle Enterprise Single Sign-On Suite Administrator's Guide* for more information.
Session Locking Support	Installs the Kiosk Manager session locking component to support kiosk scenarios. This component is not installed by default. If you install this component, the Kiosk Manager Agent (SMAgent) starts automatically. If you do not install the Kiosk Manager GINA, the Kiosk Manager Agent (SMAgent) does not start automatically, but events can be triggered through the command line from other applications. Using this scenario, you can install Kiosk Manager on a workstation and have it run only when executed. See the *Oracle Enterprise Single Sign-On Suite* Administrator's Guide for more information on using the command-line options.

Password Reset	
Password Reset Client	Installs the client-side component of Password Reset which provides knowledge-based authentication and password reset functionality. You must install the Password Reset server-side component before you install the client-side component. Password reset is not installed as part of the Typical installation option. For more information on installing Password Reset, see Installing Password Reset.

Provisioning Options	
Provisioning Gateway Client	Installs the Provisioning Gateway client-side software that provides remote credential provisioning functionality as well as credential delegation. You must install the Provisioning Gateway server component (as described in Installing Provisioning Gateway) before you install the client-side software.
Credential Delegation	Installs the Provisioning Gateway credential delegation component, allowing a user to temporarily delegate one or more credentials to another user. Requires Provisioning Gateway to be installed and functional on the target machine.
Privileged Accounts	Installs the Provisioning Gateway privileged accounts component, allowing a user to temporarily check out one or more credentials from an Oracle Privileged Account Manager server, temporarily enable single sign-on functionality for applications associated with that credential, and check the credential back in when it is no longer needed. Requires Provisioning Gateway to be installed and functional on the target machine.

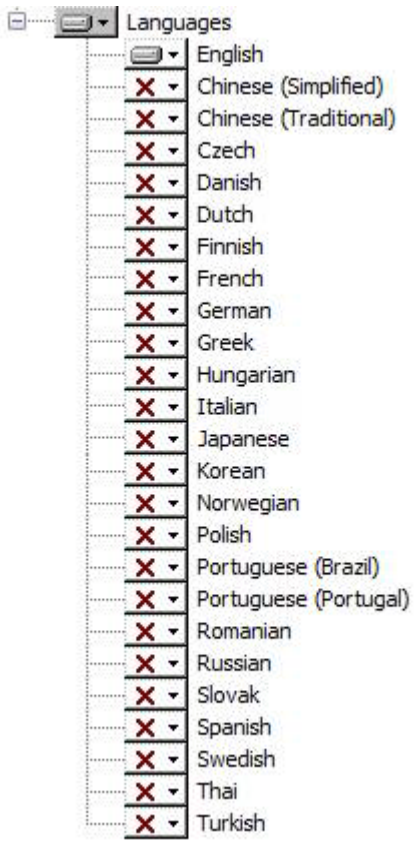
Audit Logging Methods	
This plug-in provides for the management of event logging extensions to the application. The available plug-ins are:	
ESSO Reporting Server	Event Management plug-in that supports logging of events to the reporting service.
Windows Event Manager	Event Management plug-in that supports logging of events to the Windows Event Manager.
Syslog Server	Event Management plug-in that supports logging of events to a Syslog server.
XML File	Event Management plug-in that supports logging of events to a local XML file.
Database	Event Management plug-in that supports logging of events to a Database.

Backup/Restore

This plug-in provides a simple file-based backup and restore mechanism via a wizard interface.

Languages

The localized language support packages that allow the Agent to be displayed in the displayed languages.



Note: To change the destination folder, click **Change**, navigate to the desired path, and click **OK**.

8. The InstallShield Wizard is ready to begin the installation. Click **Install**.
9. Wait for the installation to complete. When the "Completed" screen appears, click **Finish**.
10. The Logon Manager installation does not require restarting, except in the following scenarios:
    - If you installed the Windows Authentication v2 authenticator with the GINA or Network Provider components (Windows XP only), you will be prompted to restart your workstation after you click **Finish**. Continue with step 11 after restart.
    - If you installed Kiosk Manager , you must configure Logon Manager to synchronize with one of the synchronizers that you selected during

installation. Refer to the *Oracle Enterprise Single Sign-On Suite Administrator's Guide* for instructions. Additionally, on Windows XP, do not install any other GINAs if you install the Kiosk Manager GINA. Restart your workstation after setting up synchronization, then continue with step 11.

11. After your workstation or server restarts, log on to Windows. The Logon Manager Welcome Screen/First Time Use (FTU) Wizard launches. Follow the instructions on the screen to complete the FTU Wizard. After the FTU is complete, an icon appears in the tool tray.

Note: Refer to the *Oracle Enterprise Single Sign-On Suite User's Guide* and online help for information on completing the FTU Wizard and using Logon Manager.

3.4 MSI Package Components

This section describes the contents of the Logon Manager MSI installer. The feature names listed in this section are as they appear in the "Advanced Setup" section of the Logon Manager installer.

The following are mandatory core components - omitting them during command-line installation or when creating a customized MSI package will result in a non-functional installation:

- Application Support (Core)
- Provisioning Gateway Client (Provisioning
- At least one authenticator
- At least one language pack

Oracle also recommends including the Internet Explorer support component in all Logon Manager deployments.

Additionally, note the following::

- Feature names are case-sensitive.
- The following features are mutually exclusive (i.e., only one can be installed at a time): `SSOGINA`, `SSOGINA.x64`, `SMGina`, `SMAgent`, `Locking`, `SSONP`, `SSONP.x64`
- The MSI package contains critical components that are not listed in this section and should not be tampered with in any way, as they are essential to the proper functioning of Logon Manager and other Enterprise Single Sign-On Suite features. Only install/include, or uninstall/remove components listed in this section.
- The `ADDLOCAL` command only installs components that are explicitly specified, plus their parent components and child components required by the parent. If you do not explicitly specify a component to be installed, it will not be installed. Omission of any of the mandatory core components listed above will result in a non-functional installation.

  For example, specifying `Chrome` will also install its parent component `Core`, as well as `Core_Support6` which is required by the Core component, but it will not install any language packs.

Example installation command:

```
msiexec /i <my.msi> ADDLOCAL="Core,Provisioning,MSauth,English_Pack,
InternetExplorer"
```

Additional information on using the msiexec command-line tool can be found at the following URLs:

- http://support.microsoft.com/kb/230781 and
- http://technet.microsoft.com/en-us/library/cc759262(v=ws.10).aspx

Application Support

Title (as seen in installer)	Feature Name	Feature Parent	Additional Information
Application Support	Core	N/A	Mandatory for a functional installation.
Web Integration	WebIntegration	Core	
Mozilla Firefox	Mozilla	WebIntegration	
OAM Support	OAMSupport	WebIntegration	
Google Chrome	Chrome	WebIntegration	
Windows	Core_Support6	Core	
Microsoft Internet Explorer	InternetExplorer	Core	Recommended.
Host/Mainframe Emulators	MainframeEmulators	Core	
Console Windows	DOSHelper	MainframeEmulators	
PuTTY	PuttySupport	MainframeEmulators	
Java	JavaHelper.x86	Core	32-bit OS only.
J	JavaHelper.x64	Core	64-bit OS only.
SAP	SAP	Core	
SoftID	SoftIdHO	Core	

Authenticators

Title (as seen in installer)	Feature Name	Feature Parent	Additional Information
Authenticators	Authenticators	N/A	At least one authenticator is mandatory for a functional installation.
Windows Logon	SLA	Authenticators	
Windows Logon v2	MSauth	Authenticators	
GINA	SSOGina	MSauth	Windows XP 32-bit only.
	SSOGina.x64	MSauth	Windows XP 64-bit only.
LDAP	LDAP	Authenticators	
LDAP v2	LDAPauth	Authenticators	
Network Provider	SSONP	Authenticators	32-bit OS only
Network Provider	SSONP.x64	Authenticators	64-bit OS only
Proximity Card	ProxCardAuth	Authenticators	

Authenticators

Title (as seen in installer)	Feature Name	Feature Parent	Additional Information
Smart Card	SCAuth	Authenticators	
Smart Card (Read-Only)	ROSCAuth	Authenticators	
RSA SecurID	SecurID	Authenticators	
Local Authentication Toolkit (LAT)	LocalAuthToolkit	SecurID	
Authentication Manager	MultiAuth	Authenticators	

Synchronizers

Title (as seen in installer)	Feature Name	Feature Parent	Additional Information
Synchronizers	Synchronizers	N/A	
Microsoft Active Directory	AD_Sync	Synchronizers	
Microsoft AD LDS (ADAM)	ADAM_sync	Synchronizers	
LDAP	LDAP_Sync	Synchronizers	
Database	DB_Sync	Synchronizers	
Roaming Profile (deprecated)	Roam_Sync	Synchronizers	
File System	File_Sync	Synchronizers	

Kiosk Manager

Title (as seen in installer)	Feature Name	Feature Parent	Additional Information
Kiosk Manager	SMAgent_Files	N/A	
Session Locking Support	SMGina	SMAgent_Files	Window XP only.
	SMAgent_Locking	SMAgent_Files	Window 7 and above

Password Reset Client

Title (as seen in installer)	Feature Name	Feature Parent	Additional Information
Password Reset Client	PR_Components	N/A	

Provisioning Gateway Client			
Title (as seen in installer)	**Feature Name**	**Feature Parent**	**Additional Information**
Provisioning Gateway Client	Provisioning	N/A	
Credential Delegation	DelegateMgr	Provisioning	
Privileged Accounts	OpamMgr	Provisioning	

Audit Logging Methods			
Title (as seen in installer)	**Feature Name**	**Feature Parent**	**Additional Information**
Audit Logging Methods	EventMgr	N/A	
ESSO Reporting Server	ReportingExt_ Release	EventMgr	
Windows Event Manager	WindowsEventExt	EventMgr	
Syslog Server	SyslogEventExt	EventMgr	
XML File	LocalFileExt	EventMgr	
Database	DatabaseEventExt	EventMgr	

Backup/Restore			
Title (as seen in installer)	**Feature Name**	**Feature Parent**	**Additional Information**
Backup/Restore	BackupMgr	N/A	

Languages			
Title (as seen in installer)	**Feature Name**	**Feature Parent**	**Additional Information**
Languages	Languages	_TopLevel Feature	
English	English_Pack	Languages	Mandatory Automatically selected if any other language is selected with ADDLOCAL
Chinese (Simplified)	Chinese_Simplified_ Pack	Languages	
Traditional Chinese	Chinese_Traditional_ Pack	Languages	
Czech	Czech_Pack	Languages	
Danish	Danish_Pack	Languages	
Dutch	Dutch_Pack	Languages	
Finnish	Finnish_Pack	Languages	

Languages			
Title (as seen in installer)	**Feature Name**	**Feature Parent**	**Additional Information**
French	French_Pack	Languages	
German	German_Pack	Languages	
Greek	Greek_Pack	La nguages	
Hungarian	Hungarian_Pack	Languages	
Italian	Italian_Pack	Languages	
Japanese	Japanese_Pack	Languages	
Norwegian	Norwegian_Pack	Languages	
Korean	Korean_Pack	Languages	
Polish	Polish_Pack	Languages	
Portuguese (Brazil)	Portuguese_ Brazilian_Pack	Languages	
Portuguese (Portugal)	Portuguese_ Portugal_Pack	Languages	
Romanian	Romanian_Pack	Languages	
Russian	Russian_Pack	Languages	
Slovak	Slovak_Pack	Languages	
Spanish	Spanish_Pack	Languages	
Swedish	Swedish_Pack	Languages	
Thai	Thai_Pack	Languages	
Turkish	Turkish_Pack	Languages	

3.5 Completing the Installation of Logon Manager

This section describes the steps necessary to complete the installation of Logon Manager.

3.5.1 Completing the Installation of the Mozilla Firefox Support Component

In order to complete the installation of the Mozilla Firefox Support component of Logon Manager, you must do the following after installing Logon Manager:

- If Mozilla Firefox was running during the installation, close all of its instances and re-launch it,
- Ensure that the component is enabled in the "Extensions" list in the "Add-Ons" panel in Mozilla Firefox,
- Restart Logon Manager.

In the online documentation center, you will find the complete set of product-specific guides for the Oracle Enterprise Single Sign-On Suite. The following table lists the high-level tasks you will need to perform to complete your installation and deployment, and the documents associated with each task.

For This Task…	Refer to…
Configuring a repository	*Deploying Logon Manager with a Directory-Based Repository*
Configuring the Agent	*Oracle Enterprise Single Sign-On Suite Administrator's Guide*
Configuring authenticators	*Oracle Enterprise Single Sign-On Suite Administrator's Guide*
Configuring application templates	*Configuring and Diagnosing Logon Manager Application Templates*

4

Installing Password Reset

This section describes the steps necessary for installing Password Reset. It covers the following topics:

4.1 Prerequisites for Installing Password Reset

Before you install Password Reset, ensure the prerequisites listed in this section have been satisfied.

> **Note:** Please refer to the latest release notes to find out about last-minute requirements or changes that might affect your installation.

4.1.1 Prerequisites for Installing the Password Reset Client

> **Note:** When installing on Windows XP, you must install the latest root certificate update from Microsoft, otherwise the installation will fail.
>
> For details and instructions, see the following Microsoft Knowledge Base article:
>
> `http://support.microsoft.com/kb/931125`

- Because the Password Reset Client relies on the Password Reset Server to function, you must install the Password Reset Server first before you will be able to install and successfully configure the Password Reset Client component.

- If you are installing Password Reset Client and Logon Manager on the same Windows XP workstation, you cannot use the Logon Manager Network Provider logon method.
- Installing the Password Reset Client on Windows XP disables the Fast User Switching feature, which allows multiple users to be logged on to a computer at the same time and to switch among logons by pressing Win+L. This feature is unavailable because Password Reset utilizes a custom GINA (Graphical Identification and Authentication) component that replaces the Microsoft default GINA dynamic link library (Msgina.dll). To change logons on a Windows XP computer, a user must log off to allow the next user to log on. To do this, open Task Manager (CTRL+ALT+DELETE), and click Log off.
- If you want to use Password Reset on a workstation where Kiosk Manager is installed, refer to the *Oracle Enterprise Single Sign-On Suite Administrator's Guide* for configuration information.
- The optional registry settings, AutomaticEnroll and ForceEnrollment, control whether a workstation user is asked or required to enroll in the password reset service on next logon. These values can be set by modifying the installer package; they are not added by the install wizard on the client. See the *Enterprise Single Sign-On Suite Administrator's Guide* for the locations and values of those settings.
- When you install the Password Reset Server, take note of the URLs for the Password Reset Web resources listed in the table below; you will enter those URLs during the installation of the Password Reset Client. Those resources, served by the Password Reset Server, provide the client with the enrollment and reset capability.

Enroll URL	Enter the URL of the Enrollment service default page: http://host/vgoselfservicereset/enrollmentclient/EnrollUser.aspx
Reset URL	Enter the URL of the reset service default page: http://host /vgoselfservicereset/resetclient/default.aspx
Check Enroll URL	Enter the URL of the Enrollment check service (checks if user is enrolled): http://host/vgoselfservicereset/resetclient/checkenrollment.aspx
Check Force Enroll URL	Enter the URL of the force enrollment check service (checks if user is forced to enroll): http://host /vgoselfservicereset/resetclient/checkforceenrollment.aspx
Check Status URL	Enter the URL of the status check service (checks for Password Reset service availability): http://host /vgoselfservicereset/resetclient/checkstatus.aspx

4.1.2 Prerequisites for Installing the Password Reset Server

- Review the hardware and software requirements in the *Oracle Enterprise Single Sign-On Suite Release Notes* thoroughly and verify that your environment meets all requirements.
- You must use matching versions of the Oracle Enterprise Single Sign-On Administrative Console and the Password Reset server component; otherwise, unpredictable behavior may result.
- You must not install the Password Reset server-side components on a domain controller. Use a member server instead.
- Ensure that DNS is configured and working properly, including correct enumeration of forward and reverse lookup zones.

- Verify that your servers and workstations have the latest service packs and Windows updates installed on them.
- Install the IIS Web Server first as described in Configuring IIS for Password Reset on Windows Server 2008/2008 R2 or Configuring IIS for Password Reset on Windows Server 2012.
- By default, members of the "Domain Administrators" group in Active Directory are automatically added to the local "Administrators" group on the member server. If you are not a member of the "Domain Administrators" group, add yourself to the local "Administrators" group on the member server. For simplicity, the instructions in this guide assume that an "Administrator" account, which is a member of the "Schema Administrators" group is used to install and set up Password Reset Server.
- For the creation of service accounts, consider using long, complex passwords and set the accounts to lock out after a specific number of bad password attempts. These actions will prevent a hacker from successfully launching a dictionary attack on service accounts.

Note: Microsoft recommends that IIS servers be installed on member servers. For a full discussion of this matter, visit the Microsoft Web site.

4.1.3 Prerequisites for Unattended ("Silent") Installations

In order to successfully install Password Reset in unattended ("silent") mode, the Windows Management Instrumentation (WMI) service must be running before the installer is executed.

To check whether the WMI service is running, and start it if necessary, do the following on each target machine:

1. Open the System Management Console.
2. Open the **Services** snap-in.
3. Navigate to the **Windows Management Instrumentation** service and check its status and startup mode.

Depending on the status, do one of the following:

- If the status is **Started**, the WMI service is running; proceed to the next section.
- If the status is blank, check the service's startup type and start it as follows:
  1. Double-click the service.
  2. In the properties box that appears, set the startup type to **Manual** or **Automatic**, as dictated by your environment and click **Apply**.
  3. Click **Start**. The status changes to **Started**.
  4. Click **OK** to close the service properties dialog box.

4.2 Upgrading an Existing Password Reset Installation

This section provides information on upgrading an existing Password Reset installation to the latest version.

Upgrading to Password Reset 11.1.2.2.0 is supported from the following versions of Password Reset:

- 11.1.1.2.x
- 11.1.1.5.x

When upgrading a Password Reset Server installation, do the following:

1. Backup the server settings with an export of the `HKEY_LOCAL_MACHINE\Software\Passlogix\SSPR` registry key.
2. Follow the instructions in Installing the Password Reset Server Component. After completing the installation, you must restart Microsoft IIS and verify that the required service accounts are active within the system and that Password Reset is still configured to use them.
3. (Optional) If you are upgrading an instance of Password Reset that uses an Oracle database as its repository, you must add new indexes required by Password Reset 11.1.2 by running the following queries:
   - `CREATE INDEX SSPR.UQ_USERID ON SSPR.USERQUESTIONS (USERSID);`
   - `CREATE INDEX SSPR.EI_USERID ON SSPR.ENROLLMENTINFORMATION (USERSID);`
   - `CREATE INDEX SSPR.RI_USERID ON SSPR.RESETINFORMATION (USERSID);`

4.3 Configuring IIS for Password Reset on Windows Server 2008/2008 R2

Prior to installing the Password Reset server, you must install Microsoft Internet Information Services as follows:

1. In the Windows Server Manager, select **Roles>Add Roles**.
2. In the Add Roles Wizard, select the **Web Server (IIS)** role.
3. In the popup window that appears, confirm that you want to add the required features.
4. Click **Next**.
5. In the "Role Services" window, select the following roles, if they are not already selected:
   - **Application Development:** ASP .NET and its required features
   - **Common HTTP Features:** Static Content, Default Content, Directory Browsing, HTTP Errors
   - **Health and Diagnostics:** HTTP Logging, Request Monitor
   - **Security:** Windows Authentication, Digest Authentication, IP and Domain Restrictions, Request Filtering
   - **Performance:** Static Content Compression
   - **Management Tools:** IIS Management Console, IIS Management Scripts and Tools, Management Service, IIS 6 Management Compatibility (with all sub-components)
6. Click **Next**.
7. In the confirmation window, verify your installation selections. Click **Back** if you want to change any of your selections. Click **Install** when you are ready to begin installation.

   After the installation completes, continue to Installing the Password Reset Server Component.

4.4 Configuring IIS for Password Reset on Windows Server 2012

Prior to installing the Password Reset server, you must install Microsoft Internet Information Services as follows:

1. In the Windows Server Manager, click **Manage** in the upper-right corner, and select **Add Roles or Features**. from the menu that appears.
2. In the Add Roles and Features Wizard, click **Next**.
3. In the "Select installation type" screen, select **Role-based or feature-based installation** and click **Next**.
4. In the "Select destination server" screen, select the **Select a server from the server pool** option, then select the target server from the list and click **Next**.
5. In the "Select server roles" screen, select **Web Server (IIS)**; in the pop-up requesting to add features required by IIS, click **Add Features**; click **Next**.
6. In the "Web server role (IIS)" screen, click **Next**.
7. In the "Features" screen, click **Next**.
8. In the "Role services" screen, select the following and accept any prompts for installing features related to your selections:
   - **Common HTTP Features:** Default Document, Directory Browsing, HTTP Errors, Static Content, HTTP Redirection
   - **Health and Diagnostics:** HTTP Logging, Logging Tools, Request Monitor, Tracing
   - **Performance:** Static Content Compression
   - **Security:** Request Filtering, Digest Authentication, IP and Domain Restrictions, Windows Authentication
   - **Application Development:** .NET 3.5 Extensibility, .NET 4.5 Extensibility, ASP.NET 3.5, ASP.NET 4.5, ISAPI Extensions, ISAPI Filters
   - **Management Tools:** IIS Management Console, IIS 6 Management Compatibility (with all sub-components), IIS 6 Management Scripts and Tools
9. Click **Next**.
10. In the "Summary" screen, confirm your selections, click **Install**, and wait for the installation to complete.

    After the installation completes, continue to Installing the Password Reset Server Component.

4.5 Installing the Password Reset Server Component

> **Note:** Make sure you have completed the steps in Configuring IIS for Password Reset on Windows Server 2008/2008 R2 or Configuring IIS for Password Reset on Windows Server 2012 before beginning this installation.

1. Close all programs.
2. Launch the `ESSO-PR_Server.msi` installer file.
3. In the "Welcome" panel, click **Next**.

4. Select **Complete** or **Custom** setup type and click **Next**.

   Custom setup allows you to specify an alternate installation directory.

5. Click **Install**.

6. When the installation is complete, click **Finish**.

4.6 Completing the Installation of the Password Reset Server-Side Component

Perform the steps in this section to configure your host environment for Password Reset Server and configure your Password Reset Server installation for operation. You must do the following in order to start using Password Reset Server:

- Configuring the Password Reset Authentication and Password Reset Services
- Configuring Password Reset Server to Store Data in Active Directory
- Limiting the Inherited Permissions for the SSPRRESET Account to the Required Minimum
- Configuring the Password Reset Web Service's IIS Site as a Trusted Site in Active Directory
- Restricting Access to the Password Reset Web Console
- Configuring Password Reset for SSL Connectivity

4.6.1 Configuring the Password Reset Authentication and Password Reset Services

Complete the steps in this section to configure the necessary Password Reset services.

4.6.1.1 Creating the Required Service Accounts

Create the following two accounts on your domain controller. These accounts should be ordinary users in the "Domain Users" group (default):

- **SSPRWEB**. This account will be responsible for Password Reset IIS functions and will make changes, additions, and so forth, to the organizational unit (OU) that you will create later. When creating the OU, you must grant the SSPRWEB account permissions to read, write, modify, and delete all objects within the OU.

  If the IIS instance hosting the Password Reset Web service and the Active Directory or AD LDS (ADAM) repository are running on separate machines, this account must be in the same domain as (or in a trusted domain of) the Active Directory or AD LDS (ADAM) repository and must have read and write permissions to the Password Reset Web service's IIS site directories and subdirectories.

- **SSPRRESET**. This account will run the actual reset service on the Password Reset member server with IIS. It will be responsible for resetting user passwords on the domain level.

Note: Make these accounts members of the local "Administrators" group on the IIS host to avoid problems.

These accounts will be the service accounts that Password Reset uses to manage the container where user questions and enrollment information will be housed and to handle the actual password reset process. Because these are service accounts, you should use highly complex passwords and prudent practices in terms of user lockout after a certain number of bad attempts. Although this might result in some help desk calls from users who cannot reset their passwords, it will also alert you that someone has been trying to attack these service accounts. For information as to best practices for service accounts and security log monitoring, visit Microsoft's knowledge base.

4.6.1.2 Assigning the Required Service Account to the Password Reset System Service

Complete the steps below to assign the service account to the Password Reset system service:

1. Run: **Control Panel > Administrative Tools > Services**.
2. From the list in the right-hand pane, right-click **Self Service Password Reset,** and select **Properties**.
3. In the Self Service Password Reset Properties dialog box, select the **Log On** tab.
4. Select **This account** and enter the account name: **Domain\SSPRRESET**. Then enter and confirm (re-enter) the password for the account.

   A dialog box displays to advise you that changes will apply after the service is restarted.
5. Restart the service as indicated. The SSPRRESET account setup is complete.

Note: The SSPRRESET account runs the password reset service on the IIS server where the server-side components reside.

The SSPRWEB account runs the virtual Web site on the IIS server where the server-side components reside.

4.6.1.3 Adding SSPRWEB Account Credentials to the Password Reset Server Configuration

In order for Password Reset Server to function properly, it must be provided with the SSPRWEB account credentials. Complete the following steps to do so:

1. Add the credentials to the `Web.config` file:
   a. Locate the following file on the Password Reset machine and open it in a text editor:

      `<PR_Install_Directory>\WebServices\Web.config`

   b. Locate the following line:

      `<identity impersonate="true">`

   c. Modify the line to look as follows and replace the example values of the `userName` and `password` parameters with the SSPRWEB account credentials.

(Retain the quotation marks enclosing the values. The parameter names are case-sensitive.)

```
<identity impersonate="true" userName="domain\ssprweb"
password="ssprweb_password" />
```

d. Save and close the file.

2. Encrypt the credentials:

a. On the Password Reset server machine, launch the command prompt with administrator privileges.

b. Change into the following directory:

```
%windir%\Microsoft.NET\Framework\v4.0.30319
```

c. Run the following command:

```
aspnet_regiis.exe -pe "system.web/identity" -app
"/vgoselfservicereset/webservices"
```

d. Run the following command:

```
aspnet_regiis.exe -pa "NetFrameworkConfigurationKey" "IIS
APPPOOL\SSPR AppPool"
```

The SSPRWEB account credentials will be encrypted and the Password Reset Web service will be able to decrypt and use them to run under the SSPRWEB account.

To manually decrypt the credentials, run the following command:

```
aspnet_regiis.exe -pd "system.web/identity" -app
"/vgoselfservicereset/webservices"
```

4.6.1.4 Configuring Access for the Password Reset Web Service's IIS Web Site Contents

You must configure access to the Password Reset Web service's IIS Web site contents (under the `vgoSelfServiceReset` virtual directory) as follows:

Parameter	Value
Virtual Directory	EnrollmentClient
Enable Anonymous Access	NO
Integrated Windows Authentication	NO
Digest Authentication	YES
Authentication and Access Control	SSPRWEB
Virtual Directory	ManagementClient
Enable Anonymous Access	NO
Integrated Windows Authentication	YES
Digest Authentication	NO
Authentication and Access Control	SSPRWEB
Virtual Directory	ResetClient
Enable Anonymous Access	YES
Integrated Windows Authentication	YES

Parameter	Value
Digest Authentication	NO
Authentication and Access Control	SSPRWEB
Virtual Directory	WebServices
Enable Anonymous Access	NO
Integrated Windows Authentication	YES
Digest Authentication	NO
Authentication and Access Control	SSPRWEB

Note: The only virtual directory that permits anonymous access is the `ResetClient` directory.

4.6.1.5 Configuring the Password Reset Web Service's Access to the Password Reset Registry Settings

In order for Password Reset to function properly, the SSPRWEB service account needs full permissions to the following registry key on the member server containing the Password Reset server side components:

- On 32-bit systems: `HKLM\SOFTWARE\Passlogix\SSPR`
- On 64-bit systems: `HKLM\SOFTWARE\Wow6432Node\Passlogix\SSPR`

Note: After applying permissions to this key, drill down several levels to verify that permissions have been propagated throughout.

To avoid possible permissions problems during the configuration of the Password Reset server-side components, Oracle recommends that you make both the SSPRWEB and SSPRRESET accounts members of the local administrator's group on the IIS Member Server where you are installing the Password Reset server-side components.

After you have finished the installation and configuration of the Password Reset server-side components, you can remove these accounts from the local administrator's group on the member server.

4.6.2 Configuring Password Reset Server to Store Data in Active Directory

Password Reset stores user questions, answers, configuration, and enrollment information within an organizational unit in Active Directory. Select any name for the OU that will identify the unit easily.

Note: Before you proceed, create this organizational unit at the root of your domain. If the OU does not exist when you try to enable storage, you might receive an error message indicating that no such object exists on the server.

The Connect As account performs the schema extension. As such, this account must be a member of the Schema Administrator's group and have permissions to create objects within the Password Reset OU.

To enable the storage of Password Reset data in Active Directory:

1. Launch the ESSO Suite Administrative Console.
2. Select the **Password Reset** tab, enter the administrative interface URL of the target Password Reset server instance and click **Apply**.
3. In the left-hand tree, select the **System** node, then select the **Storage** tab in the main pane.
4. From the **Storage Type** drop-down menu, select **AD**.
5. In the **Servers** field, click **Add** and do the following in the dialog that appears:
   a. Enter the fully qualified host name or IP address of the target domain controller.
   b. Enter the desired port number (see table below) of the target domain controller. By default, the SSL port is 636 and the non-SSL port is 389.
   c. Click **OK** to save your changes.

      The new entry appears in the **Servers** list.
6. In the **Server timeout** field, specify the number of seconds Password Reset should wait before deeming a connection attempt unsuccessful.
7. In the **Storage Location (DN)** field, enter the full path to the Password Reset OU. The SSPRWEB account must have permissions to read, write, modify, and delete all objects stored within this OU.
8. If your repository is using SSL for secure connections (recommended), select the **Use SSL** check box.
9. In the **Initialize Storage** field, do the following:
   a. Select the **Initialize Storage for ESSO-PR** check box. This will cause Password Reset to extend the Active Directory schema and create the required objects.
   b. In the **Connect As (User)** field, enter the name of the domain's schema administrator account. This account should also have permissions required to create objects within the Password Reset OU.
   c. In the **Password** field, enter the password for the account.
10. Click **Submit** to save your changes.

Note: To verify that the Password Reset OU is configured correctly, open a fresh instance of **Active Directory Users and Computers** on your targeted domain controller, using the **Advanced** view. You should see an OU named **ESSOPR** (or the name that you chose) and two subordinate OUs named **SystemQuestions** and **Users**. The existence of these two subordinate OUs indicates success.

You can now remove both the SSPRWEB and SSPRRESET accounts from the local administrator's group on the IIS member server where you installed the Password Reset server-side components.

4.6.3 Limiting the Inherited Permissions for the SSPRRESET Account to the Required Minimum

The SSPRRESET account must be granted no privileges beyond those required to reset user passwords and unlock accounts with this account.

Note that the SSPRRESET account is simply a member of your domain users group. As a fail-safe built into Active Directory, this account cannot be used to change the password of a user that has greater rights (such as, an administrator account).

You can assign this right at the organizational unit level or group level. Assigning this right at the user level should not be a general practice and is not recommended.

4.6.3.1 Planning Your Privilege Hierarchy

The assignment of password reset permissions mandates careful consideration and planning to ensure that the desired accounts, and only the desired accounts, are granted this permission. Some practices and caveats that might help you fine-tune your strategy as you set up these accounts include:

- Consider granting the password reset account granular permissions based on organizational units or specific groups. After applying permissions to either, test to make sure that you have the desired results.
- Do not run the Delegation of Control Wizard at the root of your domain: if you do, you will give the password reset account rights that extend beyond users to objects such as computers and printers.
- Because the password reset account is a member of the domain users group, its password reset permissions are applied to all the members of the domain users group, who are at the same level.

So, if you store all of your users in the default users container in AD and run the Delegation of Control Wizard at that level, it will not permit a domain user account to reset administrator account passwords. Active Directory does not permit users to have administrative rights over administrators.

In this scenario, the password reset service account will not be granted permission to reset the password of your administrators. Your administrators will be able to enroll in Password Reset and go through the entire password reset dialog. However, when they attempt to reset their passwords, they will receive an error message because the password reset service account is not designed to have permissions to reset the password for users in a higher security group.

Carefully consider whether you want members of your domain administrators group to be able to have their passwords reset by an ordinary user account. While you can grant this level of control to the password reset account, you might decide it is wiser not to do so.

4.6.3.2 Delegating Control at the OU Level

Consider an OU structure in Active Directory where users are divided in the following manner:

- `OU = Users1`
- `OU = Users2`
- `OU = Users` (the default user container created in Active Directory)

Assigning users to organizational units makes it possible to manage the SSPRRESET service account permissions of many users in a simple and uniform manner.

1. Go to **Start>Administrative Tools> Active Directory Users and Computers**.
2. Enable the **Advanced Feature**s option in the **View** menu if it's not already enabled.
3. Navigate to **Active Directory Users and Computers > YourDomain > YourOU**.
4. Right-click the OU that you want to control and select **Properties**.
5. In the **Properties** window, select the **Security** tab and click **Advanced**.
6. In the window that appears, click **Add**.
7. in the **Enter the object name to select** field, enter the name of your SSPRRESET account. (Use the **Check names** button to validate your entry.)
8. Click **OK**.
9. In the **Object** tab of the **Permission Entry** window, select **User objects** from the **Apply onto:** dropdown menu.
10. In the **Permissions** window, check the **Reset Password** box in the **Allow** column.
11. In the **Permission Entry** window, select the **Properties** tab.
12. From the **Apply onto:** dropdown menu, select **User objects**.
13. in the **Permissions** window, check the **Allow** box for the **Write lockoutTime** and **Write pwdLastSet** permissions.
14. Click **OK**.
15. Click **OK** two more times to close the windows. Your changes take effect immediately.

To verify that permissions were correctly assigned:

1. Right-click the OU to which you just assigned the new permissions.
2. Select **Properties**.
3. Select the **Security** tab.

   The SSPRRESET account should be listed as having **Special Permissions**. The **Advanced** tab will indicate that this account has password reset permissions on the OU.

4.6.4 Configuring the Password Reset Web Service's IIS Site as a Trusted Site in Active Directory

There are two virtual directories within Password Reset that do not permit anonymous access, but that are configured to use integrated Windows authentication (that is, if you are logged onto the domain with your Windows password, you should be able to get to that page).

Due to security policies for IIS running on Windows Server 2008, the first time a user attempts to enroll, he might encounter a popup screen requesting user name and password, as is customary with any Web site with such settings. You can avoid this behavior (which can lead to undesired help desk calls) by putting the fully qualified domain name of your Password Reset IIS server in your list of trusted sites for any user in your domain.

To designate your Password Reset server as a trusted intranet site:

- For an individual computer, add the Password Reset IIS server's default Web site to your list of trusted intranet sites.

- Within Active Directory, add this site to your list of trusted intranet sites through a group policy.

To accomplish this, you need:

- Domain administrator rights
- The ability to create or modify group policies at the OU or domain level.

In the following example, the Password Reset server site is designated as a trusted intranet site for the entire domain. As such, it is a trusted site to all domain users.

> **Note:** You might choose to create this policy for each OU that contains potential Password Reset users for more granular access control. Regardless of your approach, the end result is the inclusion of the Password Reset IIS server default Web site as a trusted site.

To add the Password Reset IIS server to the list of trusted sites in your organization, you must first create a policy for Windows clients that do not have the Internet Explorer Enhanced Security Configuration installed (by default, Windows XP does not have this feature installed):

1. Remove the **Internet Explorer Enhanced Security Configuration** settings (**Control Panel > Add/Remove Programs > Add/Remove Windows Components**).
2. De-select (remove) the **Internet Explorer Enhanced Security Configuration**.

> **Note:** You can install this enhanced security feature on your domain controller after having created this policy. Read the dialog box that pops up when you attempt to import the current zone within Group Policy Object Editor.
>
> To create this policy, open Active Directory Users and Computers, right-click on the organizational units that contain users who will be enrolling in Password Reset (in this example, at the root level of the domain) and click the Group Policy tab.

3. Click **New** to create a policy. Name the policy `SSPR TRUSTED INTRANET SERVER`.
4. Click **Edit**.
5. In the left-hand tree, navigate to **User Configuration > Windows Settings > Internet Explorer Maintenance > Security > Security Zones and Content Ratings**.
6. Click **Modify Settings**.
7. Read the displayed message and proceed.
8. In the **Internet Properties** dialog box, click the **Local intranet zone** icon, then click the **Sites** button.
9. In the **Local Intranet** dialog box, click **Advanced**.
10. Enter the fully qualified domain name of your Password Reset IIS default website where indicated.
11. Click **Close**.
12. Click **OK** and **Apply** as needed to close out of the Group Policy Object Editor.

Depending on the replication speed within your network, it could take some time to replicate this policy throughout your Active Directory structure.

To confirm that this policy was applied at your desired level in AD:

1. Log on as a user who would be affected by this policy (having given AD group policy replication sufficient time).
2. In Internet Explorer, open **Tools > Internet Options > Security > Local Intranet > Sites > Advanced**.

   Internet Explorer should list the site you added in its **Trusted Sites** window.

4.6.5 Restricting Access to the Password Reset Web Console

In order to avoid unauthorized users from accessing the Web-based Password Reset management console, perform the following steps:

1. Open Windows Explorer and navigate to:
   - On 32-bit systems: `C:\Program Files\Passlogix\v-GO SSPR`
   - On 64-bit systems: `C:\Program Files (x86)\Passlogix\v-GO SSPR`
2. Right-click the **Management Client** and select **Properties** from the shortcut menu.
3. In the **Properties** dialog box, click the **Security** tab.
4. Click **Advanced**.
5. Click **Change Permissions**.
6. Deselect the **Include inheritable permissions from this object's parent** check box.
7. In the warning dialog box that appears, click **Add**.
8. Click **OK**.
9. In the **Security** tab, remove the **Users** group (part of the default inheritance) as well as any other unauthorized users.
10. Click **Add**.
11. Click **Advanced search** and select the **IIS_IUSRS** group.
12. Click **OK**.

Note: All permissions except **Full** should be checked under the **Allow** column. Additionally, the domain group containing the users who will be granted access to the console must also be added to the security ACL.

4.6.6 Configuring Password Reset for SSL Connectivity

Before configuring Password Reset for SSL connectivity on Windows Server 2008/2008 R2 or Windows Server 2012, you must obtain an X.509 Certificate from a trusted certificate authority (CA). This trusted CA must be installed in the list of trusted Root CAs. The certificate must be valid for the current date and its subject must exactly match the network name (either its host name or fully qualified URL containing a host name and domain suffix) that Password Reset client instances will use when connecting to the Password Reset server instance. The instructions in this section assume that a valid certificate has been obtained and is ready to be installed.

Note: The following articles from the Microsoft Web site can be referred to for information on installing certificates and setting up SSL:

· "How to: Obtain an X.509 Certificate" http://msdn2.microsoft.com/en-us/library/ms819929.aspx

· "How to: Set Up SSL on a Web Server" http://msdn2.microsoft.com/en-us/library/aa302411.aspx

If you use Microsoft Certificate Services to obtain the X.509 certificate, choose a Server Authentication Certificate. Also, enable the Mark keys as exportable and Use local machine store options under the Key Options section.

The steps required to enforce SSL-only connections to Password Reset server are as follows:

1. Installing the X.509 Certificate in Microsoft IIS
2. Modifying the Password Reset Server Configuration Files
3. Granting Password Reset Server Access to the WebServices Directory
4. Restricting Password Reset Connectivity to SSL Only
5. Testing the New Connectivity Configuration

4.6.6.1 Installing the X.509 Certificate in Microsoft IIS

1. Launch Microsoft IIS Manager.
2. In the **Connections** pane on the left, select the target server instance.
3. In the **Home** pane in the center, double-click the **Server Certificates** icon.
4. In the **Actions** pane on the right, click **Complete Certificate Request...**.
5. In the Complete Certificate Request dialog that appears, do the following:
   a. In the **File** name containing the certificate authority's response field, browse to or provide the full path and file name of the target X.509 certificate.
   b. In the **Friendly name** field, enter a descriptive name for the certificate.
   c. Click **OK**.

   The certificate appears in the target machine's **Server Certificates** list.
6. Bind the installed certificate to the https protocol for the selected site. In the **Connections** pane on the left, expand the target machine node and drill down to and select the **Default Web Site** node.
7. In the **Edit Site** section in the **Actions** pane on the right, click **Bindings**.
8. In the "Site Bindings" dialog that appears, click **Add**.
9. In the "Add Site Binding" dialog that appears, do the following:
   a. From the **Type** drop-down list, select **https**.
   b. From the **Certificate** drop-down list, select the certificate you installed earlier in this procedure.

c. Leave the remaining settings at their defaults.

d. Click **OK** to save your changes and dismiss the Add Site Binding dialog.

10. Click **Close** to dismiss the Site Bindings dialog.

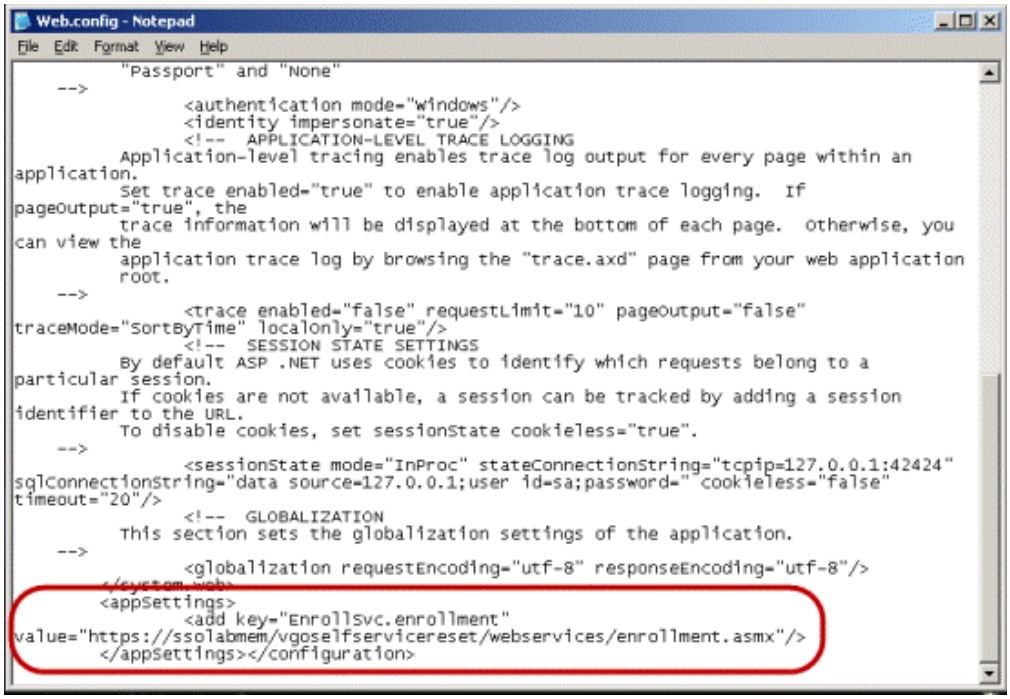
4.6.6.2 Modifying the Password Reset Server Configuration Files

You must update the following configuration files to use the HTTP-over-SSL (HTTPS) protocol when calling the Password Reset Web pages:

- `%PROGRAMFILES%\Passlogix\v-GO SSPR\EnrollmentClient\web.config`
- `%PROGRAMFILES%\Passlogix\v-GO SSPR\ManagementClient\web.config`
- `%PROGRAMFILES%\Passlogix\v-GO SSPR\ResetClient\web.config`

Modify the `\EnrollmentClient\web.config` file as follows:

1. Locate the `<appSettings>` section.
2. Modify the `EnrollSvc.enrollment` key value as follows:
   a. Change `http` to `https`.
   b. Replace `localhost` with the **Issued To** value from your X.509 certificate. (You recorded this value in the previous part of this procedure.)
   c. (Optional) If you are using a custom port to connect to this service, append the port number at the end of the host name, separated by a semicolon. For example: `https://sssolabmem.ssolab.com:1880`.
3. Save and close the file.

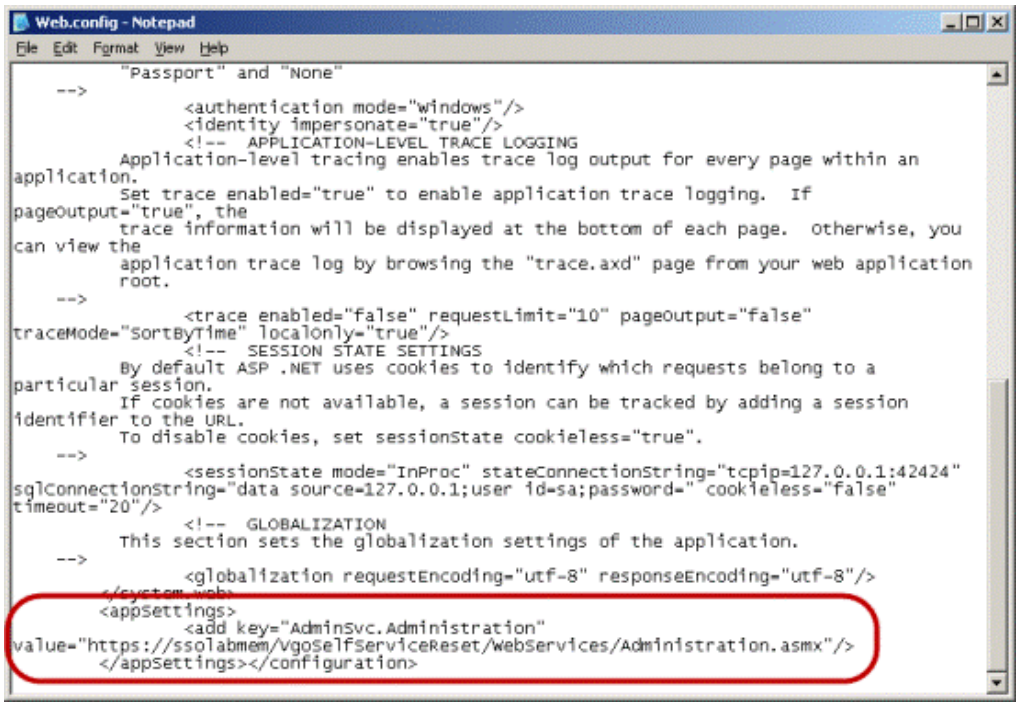


Modify the `\ManagementClient\web.config` file as follows:

1. Locate the `<appSettings>` section.
2. Modify the `AdminSvc.administration` key value as follows:

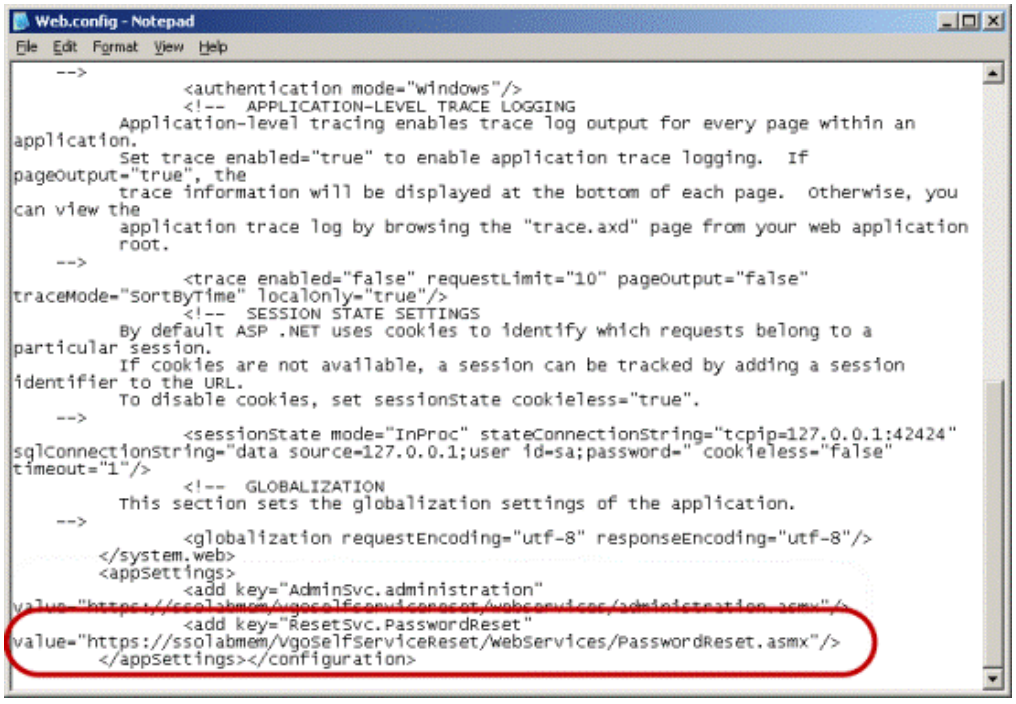
1. Change `http` to `https`.
2. Replace `localhost` with the **Issued To** value from your X.509 certificate. (You recorded this value in the previous part of this procedure.)
3. (Optional) If you are using a custom port to connect to this service, append the port number at the end of the host name, separated by a semicolon.
   For example: `https://sssolabmem.ssolab.com:1880`.

3. Save and close the file.



Modify the `\ResetClient\web.config` file as follows:

1. Locate the `<appSettings>` section.
2. Modify the `ResetSvc.PasswordReset` key value as follows:
   a. Change `http` to `https`.
   b. Replace `localhost` with the **Issued To** value from your X.509 certificate. (You recorded this value in the previous part of this procedure.)
   c. (Optional) If you are using a custom port to connect to this service, append the port number at the end of the host name, separated by a semicolon.
      For example: `https://sssolabmem.ssolab.com:1880`.
3. Save and close the file.



4.6.6.3 Granting Password Reset Server Access to the WebServices Directory

1. Launch Microsoft IIS Manager if it is not already open.
2. In the **Connections** pane on the left, expand the target machine node and drill down to and select the **Sites > Default Web Site > WebServices** node.
3. In the Default Web Site Home pane in the center, double-click the **IP Address and Domain Restrictions** icon.
4. In the Actions pane on the right, click **Add Allow Entry...** .
5. In the "Add Allow Restriction Rule" dialog that appears, do the following:
   a. Select the **Specific IP Address** radio button.
   b. Enter the IPv4 or IPv6 address of the target machine.
   c. Click **OK** to save your changes and dismiss the dialog.

4.6.6.4 Restricting Password Reset Connectivity to SSL Only

1. Launch Microsoft IIS Manager if it's not already open.
2. In the Connections pane on the left, select the target machine node.
3. Under the target machine node, drill down to and select the **Sites > Default Web Site** node.
4. In the Default Web Site Home pane in the center, double-click the **SSL Settings** icon.
5. In the SSL Settings screen in the center pane, select the **Require SSL** check box and leave the **Client certificates** option at its default value.
6. In the Actions pane on the right, click **Apply** to save your changes.

4.6.6.5 Testing the New Connectivity Configuration

Using a Web browser directly on the Password Reset server machine (do not perform this test from a remote machine), access each of the Password Reset interface services using the new SSL-enabled URLs (i.e., using the https protocol header in place of http). The URLs are as follows:

- EnrollmentClient: `https://<new_host_name>:<new_port>/vGOSelfServiceReset/WebServices/Enrollment.asmx`
- ManagementClient: `https://<new_host_name>:<new_port>/vGOSelfServiceReset/ WebServices/Administration.asmx`
- ResetClient: `https://<new_host_name>:<new_port>/vGOSelfServiceReset/WebServices/PasswordReset.asmx`

If any of the URLs fails to load, or a certificate error is displayed, check your configuration, such as virtual directory permissions and certificate options, and correct it if necessary, then try again.

4.7 Installing Password Reset Client-Side Software

Note: The Password Reset Client Installer provides the following functions:

- Supplies the components needed to run Password Reset through the Windows interface
- Sets the registry values that point the Password Reset client to the enrollment and reset service
- Offers or obliges workstation users to enroll in the password reset service if so configured

---

To install and configure the Password Reset client-side software, make sure you have created a functioning installation of Password Reset server as described in Installing the Password Reset Server Component.

Note: To perform an unattended ("silent") installation of the Password Reset client, see Installing the Password Reset Client-Side Software from the Command Line.

Then, follow the instructions in Installing the Logon Manager Client-Side Software and do the following when prompted by the installer:

1. When prompted to select between a **Typical** and **Advanced** installation, select **Advanced**.
2. In the Advanced Setup screen, click **Password Reset Client** and select **This feature, and all subfeatures, will be installed on local hard drive.** Make any other installation choices as desired, then click Next.
3. In the Setup Configuration Information screen, enter the Password Reset Server URLs.
4. When you have finished, click **Next**.

5. Continue the installation process as prompted by the installer and described inInstalling the Logon Manager Client-Side Software.

4.8 Installing Password Reset Language Packs

In order to install additional language packs after initial installation:

1. In the Windows control panel, launch **Add/Remove Programs.**
2. Highlight **Logon Manager** and click the Change button.
3. Navigate through the install wizard and click the **Modify** button.
4. Select the additional language packs that you want to install.
5. Reboot as instructed and re-launch **Add/Remove Programs** to complete the additional language installation.

4.8.1 Reverting to the Original Language Pack After Installing Another

To revert to the original language pack after you've installed another one:

1. Launch **Add/Remove Programs** and modify the Logon Manager installation to set the appropriate language pack.
2. Reboot as instructed after the installation finishes.
3. Repair the installation.

Note: You must repair the installation after modifying it. Failure to do so will cause improper functionality of the GINA button.

4.8.2 Installing Language Packs at the Command Line

In order to install the various language packs, you must install Password Reset using command line switches as illustrated below; otherwise the GINA stub will not appear on localized operating systems. You install the desired language pack by adding the language name to the string that follows the `ADDLOCAL` switch.

Following is the minimum command line for the `ADDLOCAL` switch:

```
msiexec /i "Location of .msi" ADDLOCAL=Gina,VersionTracker,English,
CheckEnrollment.x86_only,Release_Only
```

And following is an example of a command line to install silently (`/q`) with the German language pack added:

```
msiexec /i "Location of .msi" /q ADDLOCAL=Gina,vgo_sspr_
client,English,German, CheckEnrollment.x86_only,Release_Only
```

Switch	Action
`/i`	Install.
`/q`	Quiet installation.
`ADDLOCAL`	Follow with options to install (listed below)

4.8.2.1 ADDLOCAL Options

- `GINA`:

  - Required for all operating systems prior to Windows 7 (Windows Vista is not supported)
  - Do not include for Windows 7
- Required Items:
  - `VersionTracker`
  - `CheckEnrollment.x86_only` (32-bit operating systems only)
  - `CheckEnrollment.x64_only` (64-bit operating systems only)
  - `Release_Only` (32-bit operating systems only)
  - `Release_Only.x64` (64-bit operating systems only)
  - `Vista_Only` (Windows 7 32-bit only)
  - `Vista_Only.x64` (Windows 7 64-bit only)
- Installable Language Packs (English is always installed): Brazilian Portuguese, Czech, Danish, Dutch, English, Finnish, French, German, Greek, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Romanian, Russian, Simplified Chinese, Slovak, Spanish, Swedish, Thai, Traditional Chinese, Turkish.

4.8.3 Installing the Password Reset Client-Side Software from the Command Line

Note: If you are upgrading the Client from an earlier version on the Microsoft Windows 7 32-bit operating system, you must uninstall the older version before performing the following procedure.

The Password Reset client can be installed via an msiexec command, using the following syntax:

```
msiexec /q /i c:\ESSO-LM_installer.msi
ADDLOCAL="component1,component2,component3" programURLs
[REBOOT=ReallySuppress]
```

For a list of a available component names and their functions, see the table below.

For a list of command-line switches for msiexec, refer to the Microsoft MSDN site at http://msdn.microsoft.com.

`REBOOT=ReallySuppress` - tells the Installer not to reboot under any circumstances.

Example:

Using the following command line, you can perform a silent installation without a reboot of the workstation. This command assumes that the user's Windows directory is Windows and the Logon Manager installer file is named `ESSO-LM_installer.msi`:

```
msiexec /q /i "ESSO-LM 07.004_121.x64.msi"
ADDLOCAL="InternetExplorer.x64,JavaHelper.x64,Mozilla,Chrome.x64,Mainframe
Emulators,PR_Components.x64,Provisioning,Authenticators,MSauth,AD_
Sync,English_Pack" REG_
CHECKENROLLURL="http://host/vgoselfservicereset/resetclient/
checkenrollment.aspx" REG_
CHECKFORCEENROLLURL="http://host/vgoselfservicereset/
resetclient/checkforceenrollment.aspx" REG_ENROLLURL="
http://host/vgoselfservicereset/enrollmentclient/enrolluser.aspx" REG_
RESETURL="http://host/vgoselfservicereset/resetclient/default.aspx" REG_
```

```
CHECKSTATUSURL="http://host/vgoselfservicereset/resetclient/checkstatus.as
px" REBOOT=ReallySuppress
```

> **Note:** You must type out the full path to the installer .msi, as in the example above. A single space must separate each REG_*="*.aspx"-not a line return.

ProgramURLs (required)

```
REG_CHECKENROLLURL="
http://host/vgoselfservicereset/resetclient/checkenrollment.aspx"

REG_CHECKFORCEENROLLURL="
http://host/vgoselfservicereset/resetclient/checkforceenrollment.aspx"

REG_ENROLLURL="http://host/vgoselfservicereset/enrollmentclient/enrolluser.aspx"

REG_RESETURL=" http://host /vgoselfservicereset/resetclient/default.aspx"

REG_CHECKSTATUSURL="http://host
/vgoselfservicereset/resetclient/checkstatus.aspx"
```

Where `host` is the server name (or IP address) of the server that is running the Password Reset service.

4.8.4 Installing Password Reset without Logon Manager

To install Password Reset only on an end-user workstation without installing Logon Manager, use the following command:

```
msiexec /i ""<lm_installer>.msi" TRANSFORMS="pr_client_only.mst"
```

Be sure to specify the full path and name to the installer file and the full path to the transform file.

4.8.5 Completing the Installation of the Password Reset Client

Perform the steps in this section to complete the installation of Password Reset Client component.

4.8.5.1 Enabling the Password Reset Quiz on Windows Server 2008/2012

The Password Reset client runs under the "Local System" account, which by default prevents it from displaying the password reset quiz on Windows Server 2008/2012 systems due to heightened security, namely a stricter "Trusted Sites" zone configuration. To work around this issue, you must add the fully qualified Password Reset server hostname to the affected client system's "Trusted Sites" zone.

For example, to add `server.subdomain.domain.com` to the "Trusted Sites" zone, create the following registry key:

```
[HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet
Settings\ZoneMap\Domains\domain.com\server.subdomain]
```

Under that key, create a DWORD value named `*` and set it to `2`.

The value name of `*` denotes that both the `http` and `https` protocols are allowed; the value setting of `2` denotes that the entry is a member of the "Trusted Sites" zone.

4.8.5.2 (Optional) Running the Reset Client Under a Specified User Account

> **Note:** This feature is not available on Windows 7; it applies to Windows XP only.
>
> You can download the aspnet_setreg.exe tool from the Microsoft Web site at:
>
> http://support.microsoft.com/kb/329290

The Password Reset client provides the ability to run the Reset client under a specified user account instead of the Local System account. This eliminates the possibility that the Reset client will have rights to access resources it should not.

To enable this feature, follow these steps:

1. Open a command prompt and run the following command:

   ```
   aspnet_setreg -k:software\passlogix\sspr\windowsinterface
   -u:domain\username -p:password
   ```

   Replace domain\username and password with real values.

2. Ensure that the key `HKLM\Software\Passlogix\SSPR\WindowsInterface\ASPNET_SETREG` exists. There should be two values in the key: `password` and `userName`.

3. Rename the `ASPNET_SETREG` key to **RestrictedUser**.

   The Reset Client should launch under the configured user. The Enrollment Client will run under the logged on user.

To test this feature:

1. Open the Registry and browse to `HKLM\Software\Passlogix\SSPR\WindowsInterface`.

2. Copy the value of `EnrollURL` and set `ResetURL` to that value.

3. Change the authentication method for the **EnrollmentClient** Web application on the Password Reset server from **Digest** to **Windows Authentication**.

   > **Note:** Modifying the IIS authentication method for the **EnrollmentClient** Web application is only required for the purpose of this test; you must revert it back to **Digest** after you have successfully completed the test.

4. Manually add your Password Reset server URL to the "Trusted Sites" zone of the machine.

5. Launch the Password Reset client. The Enrollment screen appears, listing the specified user.

4.8.5.3 Disabling the "Redirection" Popup

You can disable the popup that indicates that Password Reset is redirecting the user to an external reset page.

To disable this popup, the Password Reset client will create the following setting before launching windowsinterface.exe, and then restore it after redirection: `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings Value: WarnonZoneCrossing`.

4.8.5.4 Specifying a Custom Window Title

You can configure Password Reset so that the Password Reset GINA button displays as a banner at the top of any window you choose.

To specify the windows that display this banner, add them to the list in: `HKLM\Software\Passlogix\SSPR\WindowsInterface\xx\GinaWindows`

where *xx* is the two-letter language code of the currently installed Password Reset language pack.

Within this key, add a `REG_SZ` value for each window title that you want to have display the banner. The value name will be `WindowTitleX`, where `X` is a sequence number starting from 1, and the value data is the window title. For example:

```
WindowTitle1=Log On to Windows

WindowTitle2=Unlock Computer
```

> **Note:** The window title must match exactly, including any leading or trailing white space.

4.8.5.5 Using Password Reset Client With a Custom Reset Web Application

You can configure the Password Reset client in the absence of a Password Reset server installation.

Follow the instructions to install Password Reset on the client machine.

1. Set the `ResetURL` value to point to the custom reset Web application.
2. Set the StatusURL to a resource that will return the success response. This forces Password Reset to bypass the status check and display the `ResetURL` contents. See below for details.

   The StatusURL setting should point to a resource (such as an HTML file) that contains the following content:

   ```
   <HTML>

   <HEAD>

   <TITLE>CHECKSTATUS</TITLE>

   </HEAD>

   <BODY>

   GOOD SSPR STATUS

   </BODY>

   </HTML>
   ```

5

Installing Provisioning Gateway

This section describes the steps necessary for installing Provisioning Gateway. It covers the following topics:

5.1 Prerequisites for Installing Provisioning Gateway

Before you install Provisioning Gateway, ensure the following prerequisites have been satisfied:

> **Note:** When installing on Windows XP, you must install the latest root certificate update from Microsoft, otherwise the installation will fail.
>
> For details and instructions, see the following Microsoft Knowledge Base article:
>
> `http://support.microsoft.com/kb/931125`
>
> Please refer to the latest release notes to find out about last-minute requirements or changes that might affect your installation.

- In order to install the Provisioning Gateway server-side component, you must run the installer as a user with administrative privileges; otherwise, the installer will fail.
- Provisioning Gateway Server at the very minimum requires the following software to function:
  - Microsoft Windows Server 2008/2008 R2, or Windows Server 2012.
  - Microsoft Internet Information Server version 7.0 or later. Provisioning Gateway uses the IIS Web server to provide a browser-based interface for user enrollment, general setup, and administrative tasks.

  - Microsoft Active Directory®, Microsoft AD LDS (ADAM), Oracle Directory Server Enterprise Edition, Oracle Unified Directory, Oracle Virtual Directory, IBM LDAP Directory, Oracle Internet Directory, Novell eDirectory Server.

    Note: If Active Directory or AD LDS (ADAM) is used, the anonymous account used in IIS must have administrative privileges and the server must be joined to the domain.

  - Microsoft SQL Server 2000, Microsoft SQL Server 2000 Desktop Engine (MSDE 2000), Microsoft SQL Server 2005 Express Edition, or Microsoft SQL Server 2005 (only required if you are using event logging) , or
  - Oracle database

- You must configure a data repository as described in the guide *Deploying Logon Manager with a Directory-Based Repository*. This repository will store Provisioning Gateway data. If you have already deployed Logon Manager, you can use the existing Logon Manager repository with Provisioning Gateway.
- During the installation of Provisioning Gateway, you must provide the following information to set up a connection to your Provisioning Gateway repository:

host	Name of the server hosting the directory server instance.
port	Port number of directory server instance.
name1[name2, name3]	Distinguished name of the directory server domain root.

- An X.509 Certificate for SSL must be obtained from a certificate authority (CA). A trusted root CA certificate should also be downloaded from your certificate authority into the list of trusted root CA certificates on the local computer. For more information, see Configuring Provisioning Gateway for SSL Connectivity.

  If you do not have a certificate authority in place and want to use Microsoft Certificate Services to obtain certificates, refer to the *Oracle Enterprise Single Sign-On Suite Administrator's Guide*, which explains how to obtain the necessary certificates using Microsoft Certificate Services. The guide also explains how to set up Provisioning Gateway to use a certificate.

5.1.1 Prerequisites for Unattended ("Silent") Installations

In order to successfully install Logon Manager, Provisioning Gateway Client, and Password Reset Client in unattended ("silent") mode, the Windows Management Instrumentation (WMI) service must be running before the installer is executed.

To check whether the WMI service is running, and start it if necessary, do the following on each target machine:

1. Open the System Management Console.
2. Open the **Services** snap-in.
3. Navigate to the **Windows Management Instrumentation** service and check its status and startup mode.

Depending on the status, do one of the following:

- If the status is **Started**, the WMI service is running; proceed to the next section.

- If the status is blank, check the service's startup type and start it as follows:
  1. Double-click the service.
  2. In the properties box that appears, set the startup type to **Manual** or **Automatic**, as dictated by your environment and click **Apply**.
  3. Click **Start**. The status changes to **Started**.
  4. Click **OK** to close the service properties dialog box.

5.2 Configuring IIS for Provisioning Gateway on Windows Server 2008/2008 R2

Prior to installing the Provisioning Gateway server, you must install Microsoft Internet Information Services as follows:

1. In the Windows Server Manager, select **Roles>Add Roles**.
2. In the Add Roles Wizard, select the **Web Server (IIS)** role.
3. In the popup window that appears, confirm that you want to add the required features.
4. Click **Next**.
5. In the "Role Services" window, select the following roles, if they are not already selected:
   - **Application Development:** ASP .NET and its required features
   - **Common HTTP Features:** Static Content, Default Content, Directory Browsing, HTTP Errors
   - **Health and Diagnostics:** HTTP Logging, Request Monitor
   - **Security:** Windows Authentication, Digest Authentication, IP and Domain Restrictions, Request Filtering
   - **Performance:** Static Content Compression
   - **Management Tools:** IIS Management Console, IIS Management Scripts and Tools, Management Service, IIS 6 Management Compatibility (with all sub-components)
6. Click **Next**.
7. In the confirmation window, verify your installation selections. Click **Back** if you want to change any of your selections. Click **Install** when you are ready to begin installation.

   After the installation completes, continue to Installing the Provisioning Gateway Server-Side Component.

5.3 Configuring IIS for Provisioning Gateway on Windows Server 2012

Prior to installing the Provisioning Gateway server, you must install Microsoft Internet Information Services as follows:

1. In the Windows Server Manager, click **Manage** in the upper-right corner, and select **Add Roles or Features**. from the menu that appears.
2. In the Add Roles and Features Wizard, click **Next**.

3. In the "Select installation type" screen, select **Role-based or feature-based installation** and click **Next**.
4. In the "Select destination server" screen, select the **Select a server from the server pool** option, then select the target server from the list and click **Next**.
5. In the "Select server roles" screen, select **Web Server (IIS)**; in the pop-up requesting to add features required by IIS, click **Add Features**; click **Next**.
6. In the "Web server role (IIS)" screen, click **Next**.
7. In the "Features" screen, click **Next**.
8. In the "Role services" screen, select the following and accept any prompts for installing features related to your selections:
   - **Common HTTP Features:** Default Document, Directory Browsing, HTTP Errors, Static Content, HTTP Redirection
   - **Health and Diagnostics:** HTTP Logging, Logging Tools, Request Monitor, Tracing
   - **Performance:** Static Content Compression
   - **Security:** Request Filtering, Digest Authentication, IP and Domain Restrictions, Windows Authentication
   - **Application Development:** .NET 3.5 Extensibility, .NET 4.5 Extensibility, ASP.NET 3.5, ASP.NET 4.5, ISAPI Extensions, ISAPI Filters
   - **Management Tools:** IIS Management Console, IIS 6 Management Compatibility (with all sub-components), IIS 6 Management Scripts and Tools
9. Click **Next**.
10. In the "Summary" screen, confirm your selections, click **Install**, and wait for the installation to complete.

    After the installation completes, continue to Installing the Provisioning Gateway Server-Side Component.

5.4 Upgrading an Existing Provisioning Gateway Installation

If you are upgrading from an earlier version of Provisioning Gateway, perform the following procedures:

- Provisioning Gateway Server. Follow the instructions in Installing the Provisioning Gateway Server-Side Component to install Provisioning Gateway Server. After running the installer, reset Microsoft IIS and verify that the anonymous service accounts are still assigned.
- Provisioning Gateway Agent. The Agent has been integrated into Logon Manager and is installed with it automatically. To upgrade, uninstall all previous versions of Provisioning Gateway Agent, shut down the Logon Manager, then follow the instructions in Upgrading an Existing Logon Manager Installation. Restart Logon Manager when done.

5.5 Installing the Provisioning Gateway Server-Side Component

To install and configure the Provisioning Gateway Server:

1. Close all programs.
2. Launch the ESSO-PG_Server.msi installer file.

3. On the Welcome Panel, click Next.
4. On the Setup Type screen, select Complete or Custom. Complete installs all program files. Custom allows you to choose which program files are installed and where they are installed. Custom installations are only recommended for advanced users. Click Next.
5. Provisioning Gateway is ready to be installed. Click Install. Wait for the installation to complete. When it is done, click Finish.

5.6 (Optional) Installing the Client-Side Provisioning Gateway Command-Line Interface (CLI)

Note: This installation procedure is optional. The Provisioning Gateway Client CLI SDK is supplied as an integration component for Provisioning Solutions.

This software requires that a Java runtime environment version 1.6 or later is installed on the target machine.

The Provisioning Gateway Server provides a Web service that allows integration with other third-party provisioning systems. The Provisioning Gateway CLI is used to communicate with this Web service. You can use it as a traditional scripting tool or, if you prefer, you can use the SDK library to develop more complex integration solutions and connectors for the Provisioning Gateway Server.

Complete the following procedure to install and configure the Provisioning Gateway CLI. For more information on the CLI syntax and usage, refer to the Provisioning Gateway CLI Guide.

1. Close all programs.
2. Launch the ESSO-PG_ClientCLI.msi installer file.
3. On the Welcome Panel, click Next.
4. The Setup Type panel appears. Select Complete or Custom. Complete installs all program files; Custom allows you to choose what program files are installed and the location. Custom installations are only recommended for advanced users. To install the Java CLI, you must choose the custom panel.
5. Select the proper setup options and click Next.
6. Provisioning Gateway is ready to be installed. Click Install.
7. When the installation is complete, click Finish.

5.7 Completing the Installation of Provisioning Gateway

This section describes the tasks necessary to create a fully functional Provisioning Gateway deployment. It covers the following topics:

- Granting the Required Permissions to the PMSERVICE Account
- Setting the Automatic Resynchronization Interval
- Granting Provisioning Rights to Domain Users
- Configuring Syslog

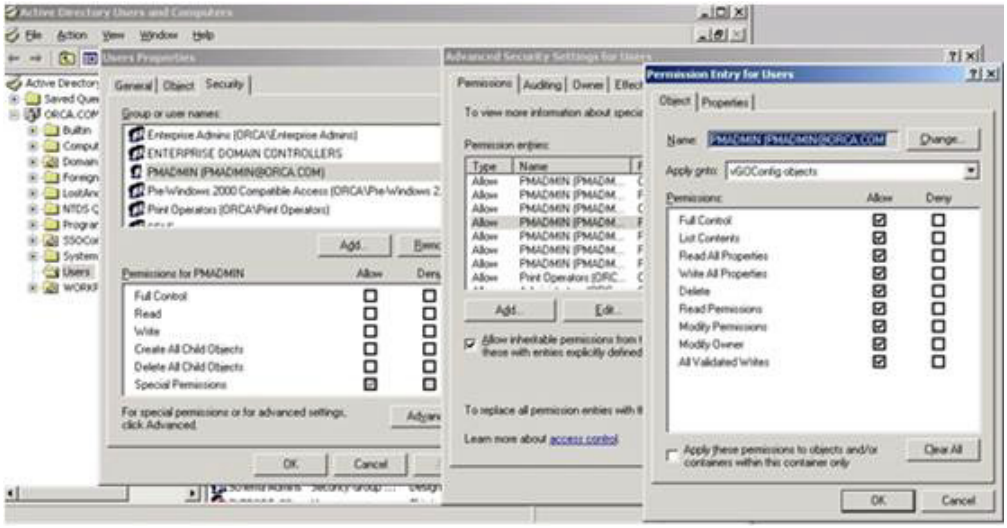
- Creating or Identifying a User Account for Anonymous Logon
- Granting the IIS Anonymous Account Access to AD LDS (ADAM)
- Configuring Provisioning Gateway for SSL Connectivity
- Configuring Provisioning Gateway Server for Connectivity with Oracle Privileged Account Manager

5.7.1 Granting the Required Permissions to the PMSERVICE Account

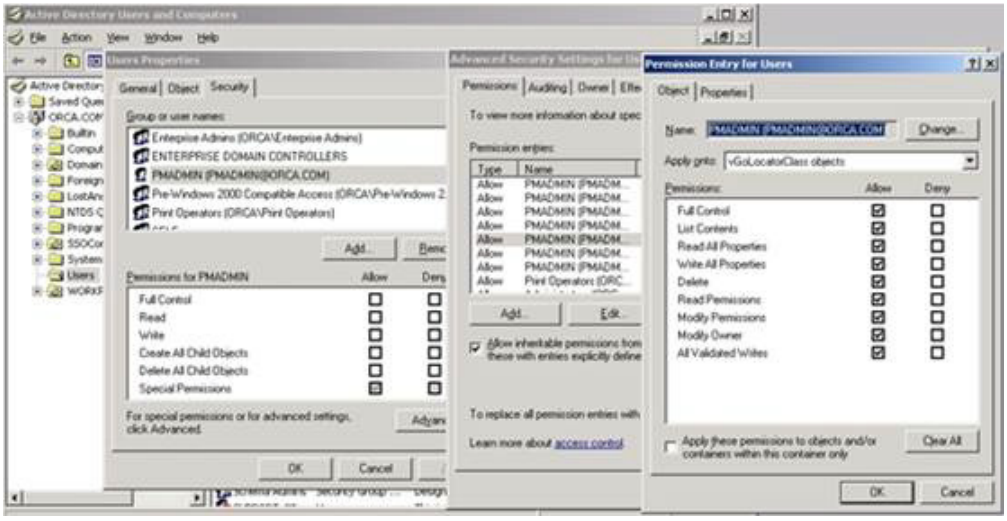
You must grant the permissions required by Provisioning Gateway to each repository container holding user data to the PMSERVICE account as follows:

1. In the repository, navigate to the Logon Manager configuration data container (usually named `SSOConfig`) and open its permission dialog, then do the following:
   a. Select **This object and all child objects** from the **Apply onto:** drop-down list.
   b. Grant the `PMSERVICE` account read-only access to the `SSOConfig` container.
2. Navigate to the **Users** container and open its permissions dialog and do the following:
   a. Select **User Objects** from the **Apply Onto:** drop-down list.
   b. Grant the `PMSERVICE` account the following `ALLOW` privileges:

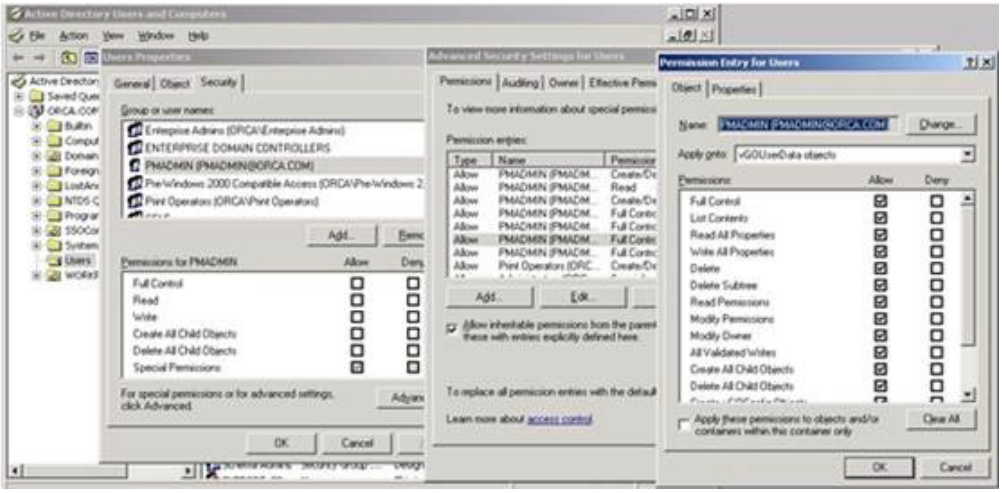
      Create vGOConfig Objects, Delete vGOConfig Objects, Create vGOUserData Objects, Delete vGOUserData Objects, List Contents, Read All Properties, Read Permissions.
3. Grant the `PMSERVICE` account the **Full Control** privilege over `vGOConfig` objects:



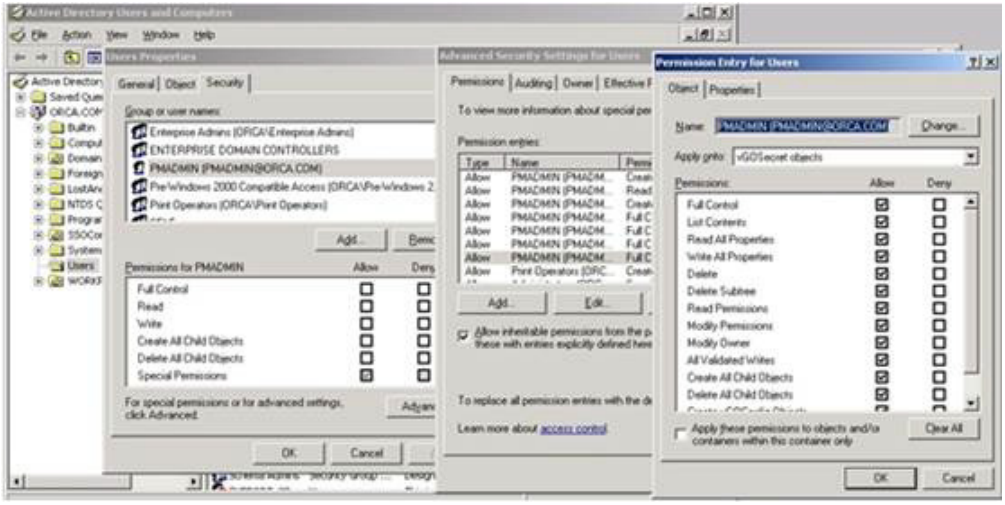
4. Grant the `PMSERVICE` account the **Full Control** privilege over `vGOLocatorClass` objects:



5. Grant the `PMSERVICE` account the **Full Control** privilege over `vGOUserData` objects:



6. Grant the `PMSERVICE` account the **Full Control** privilege over `vGOSecret` objects:

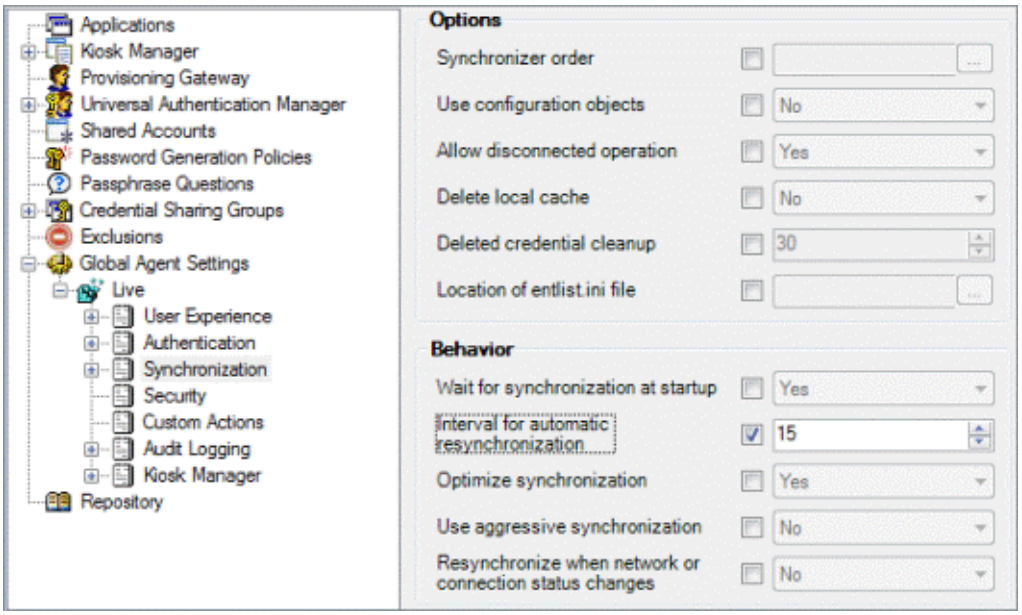


5.7.2 Setting the Automatic Resynchronization Interval

In order for Provisioning Gateway to function properly, the Provisioning Gateway Agent must synchronize to retrieve the provisioning instructions from the directory.

When you deploy Provisioning Gateway, you must decide on the synchronization interval. If this is not set to a non-zero value, synchronization only occurs upon user activity. Oracle recommends that this key be set to a value, for example, 15 minutes. This setting would guarantee that the provisioning instructions are pulled down from the directory within 15 minutes (or whatever interval is set) of when they are put there by the Provisioning Gateway Server.

1. Launch the Oracle Enterprise Single Sign-On Administrative Console.
2. Expand **Logon Manager > Global Agent Settings > [Target Settings Set] > Synchronization**.
3. Select the check box next to the **Interval for automatic resynchronization** option and enter the desired value into the field.



4. Publish your changes to the repository.

Note: This procedure applies only to running Logon Manager agents. If a user does not have Logon Manager running, the provisioning instructions are not processed until the user starts Logon Manager.

Processing the provisioning instructions requires that the user be authenticated to Provisioning Gateway. If the user is not authenticated to Provisioning Gateway (for example, the timeout expired) then an authentication UI is presented and the synchronization process is blocked until the user authenticates.

5.7.3 Granting Provisioning Rights to Domain Users

If you want an ordinary domain user to have the ability provision Logon Manager credentials via Provisioning Gateway, do the following:

- Create a user group and add the desired domain user accounts to it.
- Grant the permissions described in Granting the Required Permissions to the PMSERVICE Account to the group.
- Add the PMSERVICE account to the group.

5.7.4 Configuring Syslog

After Provisioning Gateway installation is complete, you must configure Syslog:

1. Click the **Settings** option, then click **Event Log**.
2. From the **Database Type** drop-down list, select **Syslog Daemon**.
3. Click **Save Changes**.
4. Complete the following changes in the registry:
   a. Open regedit and navigate to the following location:

      `HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix\Extensions\EventManager\Syslog`

   b. Enter the IP address of your Syslog server in the `RemoteAddress` key.

Note: If you are using a non-standard Syslog port, enter the correct port number of your Syslog server in the RemotePort key.

5.7.5 Creating or Identifying a User Account for Anonymous Logon

You must create or identify a dedicated Anonymous User account through which Provisioning Gateway users and administrators access Provisioning Gateway Web Services. This Anonymous User account should be a member of the Administrators group.

Note: Because the default Anonymous User account in IIS, IUSR_MACHINE_NAME, is not a member of the Administrator group, you must create or choose a domain user account that is an Administrator; this will allow the account to perform the following tasks:

- Change which Web service account to use from the management console
- Read from and write to the directory service (if Active Directory or AD LDS (ADAM))
- Write to the local-machine registry (HKLM).
- To create a new user account or assign Administrator rights to an existing account, use the Active Directory Users and Computers console (for an Active Directory domain) or the Computer Management console (for non-Active Directory domains)

The user account you create or choose is specified as the Anonymous User dialog of the Services tool during this step.

1. Launch the Microsoft IIS Manager.
2. In the left-hand tree, drill down to **<Server> > Sites > Default Web Site** and select the **v-GO PM Service** node.

3. In the IIS section of the center pane, double-click **Authentication**.
4. In the Authentication pane, right-click **Anonymous Authentication** and select **Edit**.
5. In the dialog box that appears, select **Specific User** and click **Set**.
6. In the dialog box that appears, enter the name of the anonymous access user account in the `<DOMAIN>\<user>` form, and the appropriate password, then click OK.
7. Click **OK** in the "Edit Anonymous Access" dialog to dismiss it.
8. When you have finished, restart Microsoft IIS to apply your changes.

Note: By default, the Provisioning Gateway Management Console is not restricted. Any user with a credential in the backend storage can log in. If you want to restrict access to a particular group, please see the "Additional Security Settings" in the Provisioning Gateway section of the *Enterprise Single Sign-On Suite Administrator's Guide*.

5.7.6 Granting the IIS Anonymous Account Access to AD LDS (ADAM)

Note: This step only applies to AD LDS (ADAM) users. Use the account chosen in Step 4 above.

1. Launch the AD LDS (ADAM) command line interface.
2. Enter:

   ```
   dsacls [\\SERVER:PORT\DISTINGUISHED_NAME] /g [USER]:ga /i:t"
   ```

   For example:

   ```
   dsacls \\localhost:50000\ou=pm,dc=passlogix,dc=com /g PLX\PMWeb:ga /i:t
   ```

3. To verify that the account was given access, type:

   ```
   dsacls \\SERVER:PORT\DISTINGUISHED_NAME
   ```

   The output shows the security information for the directory object. The Anonymous Account should appear in the list with full access.

5.7.7 Configuring Provisioning Gateway for SSL Connectivity

Before configuring Provisioning Gateway for SSL connectivity on Windows Server 2008/2008 R2 or Windows Server 2012, you must obtain an X.509 Certificate from a trusted certificate authority (CA). This trusted CA must be installed in the list of trusted Root CAs. The certificate must be valid for the current date and its subject must exactly match the network name (either its host name or fully qualified URL containing a host name and domain suffix) that Provisioning Gateway client instances will use when connecting to the Password Reset server instance. The instructions in this section assume that a valid certificate has been obtained and is ready to be installed.

Note: The following articles from the Microsoft Web site can be referred to for information on installing certificates and setting up SSL:

· "How to: Obtain an X.509 Certificate"
http://msdn2.microsoft.com/en-us/library/ms819929.aspx

· "How to: Set Up SSL on a Web Server"
http://msdn2.microsoft.com/en-us/library/aa302411.aspx

If you use Microsoft Certificate Services to obtain the X.509 certificate, choose a Server Authentication Certificate. Also, enable the Mark keys as exportable and Use local machine store options under the Key Options section.

The steps required to enforce SSL-only connections to the Provisioning Gateway server are as follows:

1. Installing the X.509 Certificate in Microsoft IIS
2. Modifying the Provisioning Gateway Server Configuration File
3. Restricting Provisioning Gateway Connectivity to SSL Only
4. Testing the New Connectivity Configuration

5.7.7.1 Installing the X.509 Certificate in Microsoft IIS

1. Launch Microsoft IIS Manager.
2. In the **Connections** pane on the left, select the target server instance.
3. In the **Home** pane in the center, double-click the **Server Certificates** icon.
4. In the **Actions** pane on the right, click **Complete Certificate Request...**.
5. In the Complete Certificate Request dialog that appears, do the following:
   a. In the **File** name containing the certificate authority's response field, browse to or provide the full path and file name of the target X.509 certificate.
   b. In the **Friendly name** field, enter a descriptive name for the certificate.
   c. Click **OK**.

   The certificate appears in the target machine's **Server Certificates** list.
6. Bind the installed certificate to the https protocol for the selected site. In the **Connections** pane on the left, expand the target machine node and drill down to and select the **Default Web Site** node.
7. In the **Edit Site** section in the **Actions** pane on the right, click **Bindings**.
8. In the "Site Bindings" dialog that appears, click **Add**.
9. In the "Add Site Binding" dialog that appears, do the following:
   a. From the **Type** drop-down list, select **https**.
   b. From the **Certificate** drop-down list, select the certificate you installed earlier in this procedure.
   c. Leave the remaining settings at their defaults.

d. Click **OK** to save your changes and dismiss the Add Site Binding dialog.

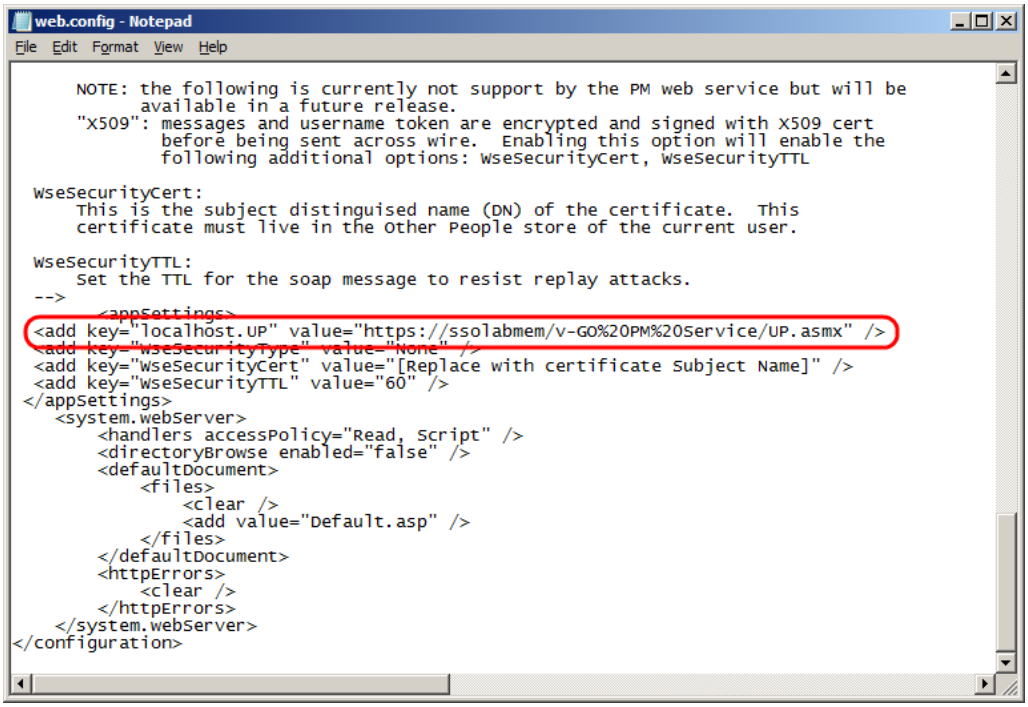
10. Click **Close** to dismiss the Site Bindings dialog.

5.7.7.2 Modifying the Provisioning Gateway Server Configuration File

You must update the following configuration file to use the HTTP-over-SSL (HTTPS) protocol when calling the Provisioning Gateway Web pages:

`%PROGRAMFILES%\Passlogix\v-GO PM\Console\web.config`

1. Locate the `<appSettings>` section.
2. Modify the `localhost.UP` key value as follows:
   a. Change `http` to `https`.
   b. Replace `localhost` with the **Issued To** value from your X.509 certificate. (You recorded this value in the previous part of this procedure.)
   c. (Optional) If you are using a custom port to connect to this service, append the port number at the end of the host name, separated by a semicolon.
   For example: `https://sssolabmem.ssolab.com:1880`.
3. Save and close the file.



5.7.7.3 Restricting Provisioning Gateway Connectivity to SSL Only

1. Launch Microsoft IIS Manager if it's not already open.
2. In the Connections pane on the left, select the target machine node.
3. Under the target machine node, drill down to and select the **Sites > Default Web Site** node.
4. In the center pane, double-click the **SSL Settings** icon.
5. In the SSL Settings screen in the center pane, select the **Require SSL** check box and leave the **Client certificates** option at its default value.

6. In the Actions pane on the right, click **Apply** to save your changes.

5.7.7.4 Testing the New Connectivity Configuration

Using a Web browser directly on the Provisioning Gateway server machine (do not perform this test from a remote machine), access the Provisioning Gateway Web service using the new SSL-enabled URL (i.e., using the https protocol header in place of http).

Note that you must have been granted the appropriate administrative privileges in order to actually log on to the Provisioning Gateway Console; instructions for granting the required priviledges are provided in the Provisioning Gateway section of the *Enterprise Single Sign-On Suite Administrator's Guide*.

The URL is follows:

```
https://<new_host_name>:<new_port>/vGo%20PM%20Console/logon.aspx
```

If the URL fails to load, or a certificate error is displayed, check your configuration, such as virtual directory permissions and certificate options, and correct it if necessary, then try again.

5.7.8 Configuring Provisioning Gateway Server for Connectivity with Oracle Privileged Account Manager

Provisioning Gateway server acts as an adapter between Oracle Privileged Account Manager (OPAM) and Logon Manager and is required if you chose to install the "Privileged Accounts" component of the Provisioning Gateway client that enables single sign-on functionality for OPAM-protected resources.

Before you complete the steps below, you must import the OPAM SSL certificate into the Trusted Root Certification Authorities store of the Provisioning Gateway server. This certificate is required to enable SSL connectivity between the OPAM instance and Provisioning Gateway, as OPAM does not allow unencrypted (non-SSL) connectivity.

> **Note:** When importing the certificate, you must install the certificate for the computer account, and not the currently logged in user account.

The certificate's location on the OPAM server is:

```
<Middleware>\wlserver_10.3\server\lib\CertGenCA.der
```

You can also create and use a custom certificate, if your environment requires it.

To enable this integration, you must configure Provisioning Gateway server to connect to the desired OPAM server in order to perform account checkin and checkout. Do the following:

1. Open the `web.config file` located in the `<PG_Server_Install_Directory>\Service` directory.
2. Locate the <appsettings> section and add the following lines at the end of it (but before the closing </appsettings>) tag:

```
<add key="OpamUrl" value ="<OPAM_Server_URL>" />

<add key="OpamUsername" value="<OPAM_Account_Name>" />

<add key="OpamPassword" value="<OPAM_Account_Password>" />
```

where:

<OPAM_Server_URL> is the full URL of the OPAM server you want to use,

<OPAM_Account_Name> is the user name of the OPAM account you wish to use to connect to the OPAM server.

<OPAM_Account_Password> is the password for the above OPAM account.

3. Save and close the web.config file.
4. Encrypt the modified web.config file by executing the following commands from the command prompt:

```
aspnet_regiis.exe -pe "appSettings" -app "/v-go pm service"

aspnet_regiis.exe -pa "NetFrameworkConfigurationKey" "NT
Authority\Network Service"
```

5.7.9 Configuring Oracle Internet Directory for Provisioning Gateway

If you are deploying Provisioning Gateway with Oracle Internet Directory as the repository, you must perform the following tasks before you install Provisioning Gateway:

1. Create a user group in Oracle Internet Directory for Provisioning Gateway administrators and add the Provisioning Gateway administrators' accounts to that group.
2. Add the orclPrivilegeGroup object class to the group.
3. For each People container in your repository, grant read, write, modify, and delete permissions to the group.

6

Installing Universal Authentication Manager

This section describes the steps necessary for installing Universal Authentication Manager.

It covers the following topics:

- Prerequisites for Installing Universal Authentication Manager
- Configuring Universal Authentication Manager for Synchronization with Microsoft Active Directory
- Configuring Universal Authentication Manager for Synchronization with Microsoft AD LDS (ADAM)
- Upgrading an Existing Universal Authentication Manager Installation
- Installing the Universal Authentication Manager Client-Side Software
- Performing an Unattended (Silent) Installation
- Completing the Installation of Universal Authentication Manager

6.1 Prerequisites for Installing Universal Authentication Manager

Before you install Universal Authentication Manager, ensure the prerequisites listed in this section have been satisfied.

Note: When installing on Windows XP, you must install the latest root certificate update from Microsoft, otherwise the installation will fail.

For details and instructions, see the following Microsoft Knowledge Base article:

`http://support.microsoft.com/kb/931125`

6.1.1 Prepare the Universal Authentication Manager Repository

Before installing Universal Authentication Manager in enterprise mode, you must prepare your repository for use with Universal Authentication Manager as described in one of the following sections:

- Configuring Universal Authentication Manager for Synchronization with Microsoft Active Directory
- Configuring Universal Authentication Manager for Synchronization with Microsoft AD LDS (ADAM)

6.1.2 Prerequisites for Universal Authentication Manager Logon Methods

Universal Authentication Manager requires and supports various third-party software, hardware, and middleware for the logon methods. The general prerequisites are listed below. For a detailed list of supported and versions for this release, refer to the Oracle Enterprise Single Sign-On Suite *Release Notes*.

6.1.2.1 Prerequisites for Using Smart Cards

The following third-party software and hardware components are required to use smart cards with Universal Authentication Manager:

- Supported smart card middleware software (PKCS#11, MiniDriver/Base CSP, .NET)
- Supported smart card readers and drivers
- Supported smart cards
- Each card must have an embedded serial number.
- If using Smart Card PIN mode, each card must have a valid digital certificate and a key pair, which can be generated either by third-party tools or Universal Authentication Manager. Oracle recommends using the method that conforms more closely to your organization's security policies. Cards without a valid certificate and key pair can only be used with a Universal Authentication Manager-generated PIN.

  Note: To have Universal Authentication Manager generate a key pair, you must configure it to do so via Universal Authentication Manager registry settings, as described in the Oracle Enterprise Single Sign-On Universal Authentication Manager Administrator's Guide. Universal Authentication Manager does not generate digital certificates and one is not required in such scenario.

- Your card's middleware must conform to the Microsoft Base CSP standard or be both fully PKCS#11-compliant and provide a CSP module.
- If using Windows XP and Microsoft Base CSP-compliant middleware, the Microsoft Base CSP framework must be installed.
- Sagem smart cards are not supported in this release of Universal Authentication Manager.
- After the smart card middleware is installed, you must merge the appropriate registry file with it. The registry files are available in the Universal Authentication Manager installation folder in the /SmartCard subfolder. Double-click the registry file to merge it. Starting with the 11.1.2.2.0 release, the files are compatible with both 32-bit and 64-bit systems; do not use files from an earlier release on 64-bit systems, as they will not work. The following table displays the registry file for each supported smart card:

Card	Family/Type	Middleware	Registry File
RSA smart card 5200	PKCS11	RSA Authentication Client 2.0	smart_providers_ pkcs11_ rsa.reg
NetMaker Net iD - CardOS 1	PKCS11	NetMaker Net iD 4.6	smart_providers_ pkcs11_ netid.reg

Card	Family/Type	Middleware	Registry File
ORGA JCOP21 v2.2	PKCS11	SafeSign/RaakSign Standard 3.0.23	smart_providers_ pkcs11_ safesign.reg
Oberthur ID-ONE Cosmo	PKCS11	SafeSign/RaakSign Standard 3.0.23	smart_providers_ pkcs11_ safesign.reg
Athena IDProtect	PKCS11	SafeSign/RaakSign Standard 3.0.23	smart_providers_ pkcs11_ safesign.reg
Athena ASECard Crypto	PKCS11	Athena ASECard Crypto 4.33	smart_providers_ pkcs11_ athena.reg
HID Crescendo 700	PKCS11	HID RaakSign Standard 2.3	smart_providers_ pkcs11_ raaksign.reg
Gemalto Cyberflex 64K (v2c) SPE Required / SPE Optional	PKCS11	Gemalto Access Client 5.5 Xiring CCID Driver version 1.00.0002 or later / XISIGN reader Gemalto PC-PinPad version 4.0.7.5 or later / PC PinPad reader	smart_providers_ pkcs11_ gemalto.reg
IBM JCOP21id	PKCS11	SafeSign Identity Client 2.2.0	smart_providers_ pkcs11_ safesign.reg
DigiSign JCOP with MyEID Applet	PKCS11	Fujitsu mPollux DigiSign Client 1.3.2-34 (1671)	smart_providers_ pkcs11_ fujitsu.reg
Oberthur ID-One Cosmo 64 v5.2D Fast ATR with PIV application SDK	PKCS11	ActivIdentity ActivClient 6.1	smart_providers_ pkcs11_ actividentity.reg
Cyberflex 64K	PKCS11	Gemalto Access Client 5.5	smart_providers_ pkcs11_ gemalto.reg
HID Crescendo 200	MS Base CSP/MiniDriver	HID Global MiniDriver for MS Base smart card CSP	smart_providers_ basecsp.reg
Gemalto .NET v2+	MS Base CSP/MiniDriver	Gemalto MiniDriver for Microsoft Windows XP	smart_providers_ basecsp.reg
Oberthur ID-ONE Cosmo	MS Base CSP/MiniDriver	Oberthur ID-ONE MiniDriver for MS Base smart card CSP	smart_providers_ basecsp.reg
Athena ASECard Crypto ILM	MS Base CSP/MiniDriver	Athena ASECard Crypto ILM MiniDriver for MS Base smart card	smart_providers_ basecsp.reg

6.1.2.2 Prerequisites for Using Proximity Cards

The following third-party hardware components are required to use Proximity Cards with Universal Authentication Manager.

- Supported Proximity Card readers and drivers
- Supported Proximity or Contactless Cards and tokens

6.1.2.3 Prerequisites for Using Fingerprint Readers

The following third-party hardware components are required to use a fingerprint reader with Universal Authentication Manager.

- Supported fingerprint readers and drivers
- For the Fingerprint logon method, BIO-key BSP version 1.10 or later must be installed.

> **Note:** You must obtain a license for using the BIO-key BSP directly from BIO-key. Oracle does not provide licensed copies of the BIO-key BSP.
>
> For the latest list of supported cards and readers, please contact BIO-key directly.

6.1.3 Prerequisites for Unattended ("Silent") Installations

In order to successfully install Universal Authentication Manager in unattended ("silent") mode, the Windows Management Instrumentation (WMI) service must be running before the installer is executed.

To check whether the WMI service is running, and start it if necessary, do the following on each target machine:

1. Open the System Management Console.
2. Open the **Services** snap-in.
3. Navigate to the **Windows Management Instrumentation** service and check its status and startup mode.

Depending on the status, do one of the following:

- If the status is **Started**, the WMI service is running; proceed to the next section.
- If the status is blank, check the service's startup type and start it as follows:
  1. Double-click the service.
  2. In the properties box that appears, set the startup type to **Manual** or **Automatic**, as dictated by your environment and click **Apply**.
  3. Click **Start**. The status changes to **Started**.
  4. Click **OK** to close the service properties dialog box.

6.2 Configuring Universal Authentication Manager for Synchronization with Microsoft Active Directory

Note: Before completing the procedures in this section, note that:

- Oracle recommends that you install Universal Authentication Manager in local mode and switch it to enterprise (synchronization) mode (as described in the *Oracle Enterprise Single Sign-On Universal Authentication Manager Administrator's Guide*) only after you have prepared the repository and configured synchronization settings. Otherwise, Universal Authentication Manager data structures may not be correctly created or permissions correctly set within the repository.
- When deploying Universal Authentication Manager in enterprise mode, users must not enroll in any logon methods until synchronization with the repository has been properly configured and tested. Otherwise, enrollment data will be lost.
- Only Microsoft Active Directory and Microsoft AD LDS (ADAM) are supported as repositories.

In order to allow Universal Authentication Manager to centrally store and manage policies and enrollment data, you must prepare an Active Directory-based repository and configure Universal Authentication Manager for synchronization with that repository by performing the following tasks:

- Preparing the Repository when Logon Manager is Already Deployed
- Creating a Universal Authentication Manager Service Account
- Extending the Schema
- Enabling Data Storage Under User Objects
- Initializing Universal Authentication Manager Storage
- Understanding the Universal Authentication Manager Repository Data Structures and Permissions
- Configuring the Universal Authentication Manager Synchronizer
- Configuring Universal Authentication Manager Synchronization for Administrative Users

When assigning user groups, keep the following in mind:

- User groups used should be in the same domain,
- Use security groups, not distribution groups,
- Universal Authentication Manager will only support a single Active Directory domain.

6.2.1 Preparing the Repository when Logon Manager is Already Deployed

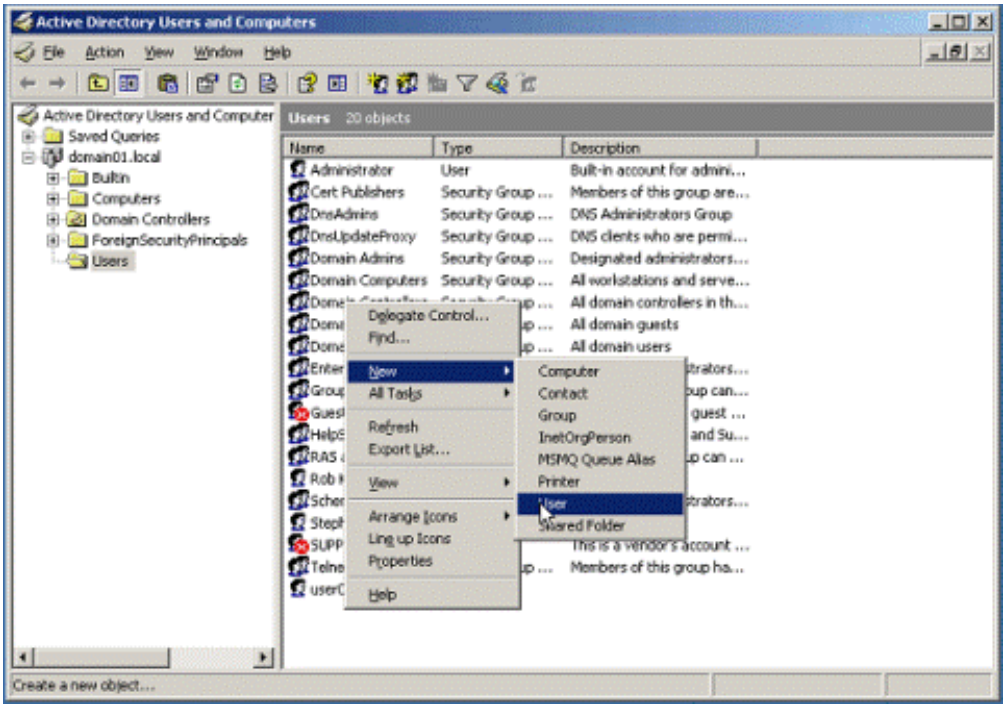
If Logon Manager is already installed and synchronizing with your Active Directory-based repository, Universal Authentication Manager will be sharing Logon Manager's repository container to store its own policies and settings. In such cases, you do not need to extend the schema or enable data storage under user objects. Instead, complete the following steps:

- Complete the steps in Initializing Universal Authentication Manager Storage.
- Complete the steps in Configuring the Universal Authentication Manager Synchronizer.

6.2.2 Creating a Universal Authentication Manager Service Account

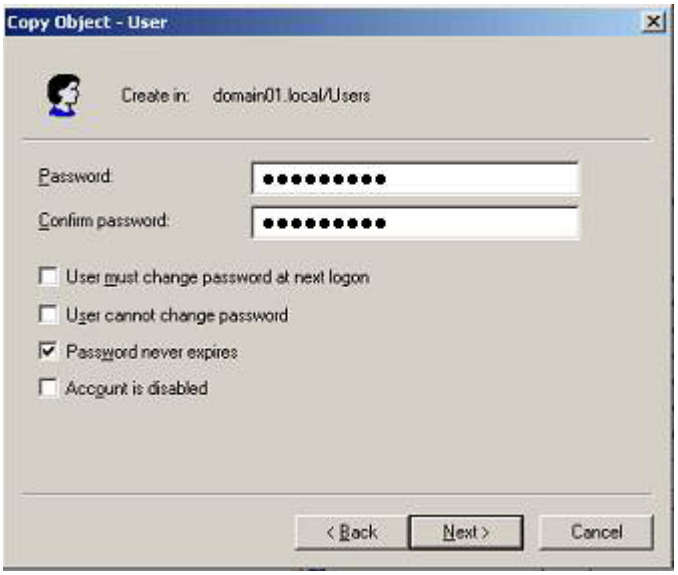
In order for Universal Authentication Manager to read and write data in the repository, you must give it the privileges to do so. This is accomplished by creating a service account that Universal Authentication Manager uses to interact with its repository. This account should be a standard domain account (member of Domain Users); no other permissions are necessary.

1. On the workstation that will serve as your domain controller, launch Active Directory Users and Computers.
2. Right-click in the Users container and select **New > User**. The User account is a regular member of the Domain Users group.



3. Enter a name for the user or group account (for this example, the name is `uamservice`) and click **Next**.

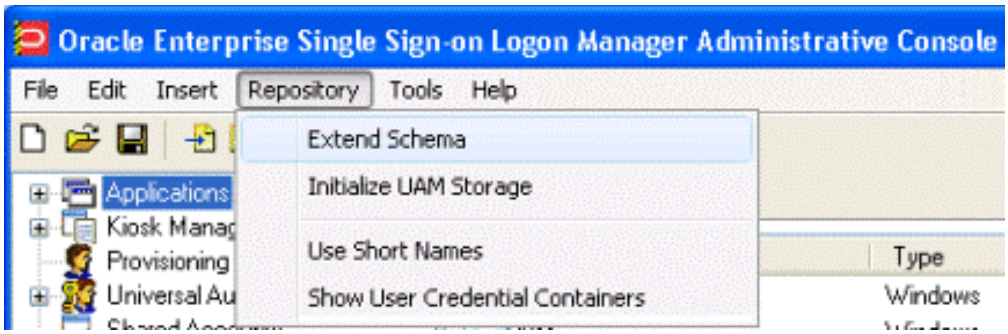
4. Enter a password, select the **Password never expires** box, and deselect the **User must change password at next logon** box.



6.2.3 Extending the Schema

Note: If you are not sure whether you have already extended the schema, simply complete the steps below; performing the schema extension multiple times will not harm your repository or the data it contains.

1. Launch the Oracle Enterprise Single Sign-On Administrative Console.
2. From the **Repository** menu, select **Extend Schema**.



3. In the "Connect to Repository" dialog box, do the following:
   a. Enter a **Server Name** (for this example, the name is `DC01`).
   b. Select **Microsoft Active Directory Server** from the drop-down menu.
   c. Select the **Use secure channel (SSL) check box** if your environment is configured for SSL connectivity.
   d. Enter the **Port** number (default SSL port is 636; default non-SSL port is 389).
   e. Enter the **Username/ID** and **Password** of an administrative account with Domain and Schema Administrator permissions.
   f. Click **OK** when finished.

6.2.4 Enabling Data Storage Under User Objects

After extending the schema, you must allow Universal Authentication Manager to store enrollment data under each respective user's user object within the repository. To do so, complete the following steps:

> **Note:** If Logon Manager is already installed and synchronizing with your repository, you do not need to enable this option, as it is already enabled; proceed to the next section.

1. In the left-hand tree, right-click the Repository node and select Connect To... from the context menu.
2. In the "Connect to Repository" dialog box, do the following:
   a. Enter a **Server Name** (for this example, the name is `DC01`).
   b. Select **Microsoft Active Directory Server** from the drop-down menu.

c. Select the **Use secure channel (SSL) check box** if your environment is configured for SSL connectivity.

d. Enter the **Port** number (default SSL port is 636; default non-SSL port is 389).

e. Enter the **Username/ID** and **Password** of an administrative account with Domain and Schema Administrator permissions.

f. Click **OK** when finished.

3. From the **Repository** menu, select **Enable Storing Credentials Under User Object**.

4. In the prompt that appears, click **OK**.

5. In the confirmation dialog that appears, click **OK** to dismiss it.

The data structures have now been created and the required permissions set. For more information on what's done in the repository during this step, see the next section.

Note: Once the Universal Authentication Manager service account has been created, it can also be configured manually or automatically on multiple end-user machines using the command-line tool `DeployTool.exe`. For more information, see the Universal Authentication Manager section of the *Oracle Enterprise Single Sign-On Suite Administrator's Guide*.

6.2.5 Initializing Universal Authentication Manager Storage

1. After successfully extending the schema, return to the **Repository** menu and select **Initialize UAM Storage**.

2. From the drop-down menu, select the server that you just created. The other fields are filled in automatically.

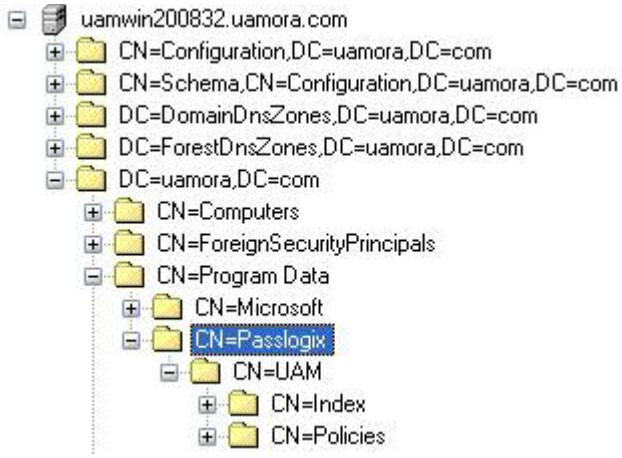
3. Click **OK**.
4. In the Select User or Group window, start typing the name of your service account, then click **Check Names**. The service account name is filled in automatically.

5. Click **OK** and wait for the success message.

6.2.6 Understanding the Universal Authentication Manager Repository Data Structures and Permissions

When you invoke the **Initialize UAM Storage** command described earlier, Universal Authentication Manager does the following within your repository:

1. Modifies the schema to ensure that vgoUser and `vgoConfig` classes may be placed inside `Container` objects.
2. Builds the default container structure `Program Data/Passlogix/UAM` with subcontainers `Policies` and `Index` as shown below:



Note: Never manually modify the contents of the index and policies containers.

The containers can be named differently if your environment requires so; however, you will need to manually configure all Universal Authentication Manager client instances to point to the custom-named containers. Oracle highly recommends you leave the container names at their defaults.

3. Grants the Universal Authentication Manager service account generic read, write, modify, and delete permissions to the index container (as well as all other permissions inherited from its parent) so that the Universal Authentication Manager service can read, create, modify, and delete objects in the index container.
4. Grants the Universal Authentication Manager service account generic read permissions (as well as any permissions inherited from its parent) so that the Universal Authentication Manager service can read objects within the policies container.
5. Updates the domain root DSE object to grant the Universal Authentication Manager service account permissions to create and delete `vgoConfig` and `vGoUser` objects under `User` objects across the entire domain. (If the user objects have been relocated to a custom location, the permissions can be set directly at the target container instead of at the root.)
6. Updates the domain root DSE object to grant the Universal Authentication Manager service account generic read permissions to all `vgoConfig` objects across the domain so that the Universal Authentication Manager service can read all `vgoConfig` objects regardless of their location in the repository.

6.2.7 Configuring the Universal Authentication Manager Synchronizer

You are now ready to configure the Universal Authentication Manager to allow Universal Authentication Manager to synchronize with the repository. Complete the following steps:

1. Launch the Oracle Enterprise Single Sign-On Administrative Console.
2. In the left-hand tree navigate to **Global Agent Settings > [TargetSettingsSet>] > Synchronization**.
3. If Logon Manager is not installed and synchronizing with the repository, add a configuration node for the Active Directory synchronizer to your settings set as follows (otherwise skip to the next step):
   a. Right-click the **Synchronization** node and select **Manage synchronizers** from the context menu.
   b. In the window that appears, click **Add**.
   c. In the list of available synchronizers, select **Active Directory**, enter `ADEXT` as the name, and click **OK**.
   d. Click **OK** to dismiss the dialog. The **ADEXT** node appears under the **Synchronization** node.
4. Do one of the following:
   - If Logon Manager is installed and synchronizing with the repository, do not modify the value of the Base location(s) for configuration objects field; instead, skip to the next step.
   - If Logon Manager is not installed and synchronizing with the repository, in the **Base location(s) for configuration objects** field, select the check box, click the ... button, enter the fully qualified DN of the Universal Authentication Manager policies container in the window that appears, then click **OK** to save your changes.
5. In the **Base location(s) for UAM storage index** field, select the check box, click the ... button, and enter the fully qualified DN of the Universal Authentication Manager index container, then click **OK**.
6. If it is not already set, select the check box next to the **Location to store user credentials** option and select **Under respective directory user objects** from the drop-down list.
7. Configure other synchronization settings as desired; for more information on each setting, see the Console help.
8. Export your settings to a `.REG` file for distribution to end-user workstations:
   a. From the **File** menu, select **Export**.
   b. In the dialog that appears, click **HKLM Registry Format**.
   c. In the "Save" dialog that appears, navigate to the desired location and provide a name for the `.REG` file, then click **Save**.
9. Distribute the `.REG` file to your Universal Authentication Manager workstations and merge it into their Windows registries.

Note: The Console produces a `.REG` file compatible only with 32-bit systems. If you are merging the `.REG` file on a 64-bit system, you must include the `/reg:32` switch in your import command to merge the registry data into the correct location within the registry; otherwise, Universal Authentication Manager will not function. For example:

```
reg.exe import MyRegistryFile.reg /reg:32
```

6.2.8 Configuring Universal Authentication Manager Synchronization for Administrative Users

The rights necessary to store credentials under user objects are granted at the tree root and inherited down to user objects. If you are deploying Universal Authentication Manager in enterprise mode in an environment where members of protected user groups, such as `Administrators`, will be using it, you must grant the Universal Authentication Manager service account through the `AdminSDHolder` object the permissions necessary to create and delete `vGOUserData` and `vGOSecret` objects.

> **Note:** If Logon Manager is already installed and synchronizing with the same repository that Universal Authentication Manager is utilizing, you will also need to grant these permissions to the `AdminSDHolder` object itself, which was most likely done during Logon Manager deployment. This granting will appear as "SELF" in the affected administrative user's permissions list, as well as in the `AdminSDHolder` object's permissions list.

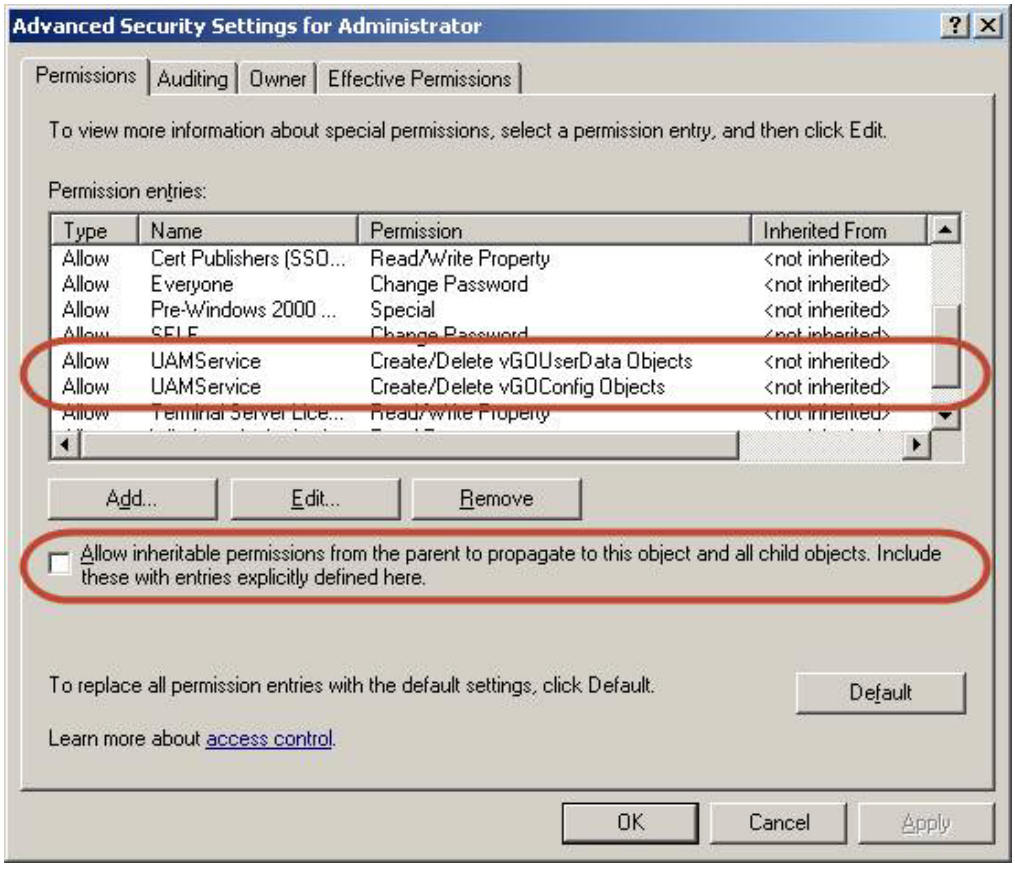
Without this explicit permission application, administrative users will be blocked from storing their Universal Authentication Manager data in the repository due to automatic inheritance of restrictive rights from the AdminSDHolder object. This is because the object's ACL, which governs the ACLs of all protected groups, prohibits rights inheritance by default. More information about this issue is available in the following MS Knowledge Base article:
http://support.microsoft.com/kb/817433.

The following protected user groups are known to be affected by this problem:

- Enterprise Admins
- Schema Admins
- Domain Admins
- Administrators
- Account Operators
- Server Operators
- Print Operators
- Backup Operators
- Cert Publishers

To verify that you are experiencing this particular issue, do the following:

1. Log in to the primary domain controller as a domain administrator.
2. Open the "Active Directory Users and Computers" MMC snap-in.
3. From the **View** menu, select **Advanced Features**.
4. Navigate to the affected user object, right-click it, and select **Properties**.
5. In the dialog that appears, select the **Security** tab.
6. Click **Advanced**. The "Advanced Security Settings" dialog appears:



7. In the dialog, check whether:
   - The **Allow inheritable permissions…**check box is not selected.
   - The permissions highlighted in the figure in step 6 are not present in the list.

   If the above conditions are true, the user object is not inheriting the necessary permissions from the directory root.

To rectify this issue, you must manually modify the ACL of the AdminSDHolder object to grant the right to create objects of type `vGOConfig` and `vGOUserData`. The steps are as follows:

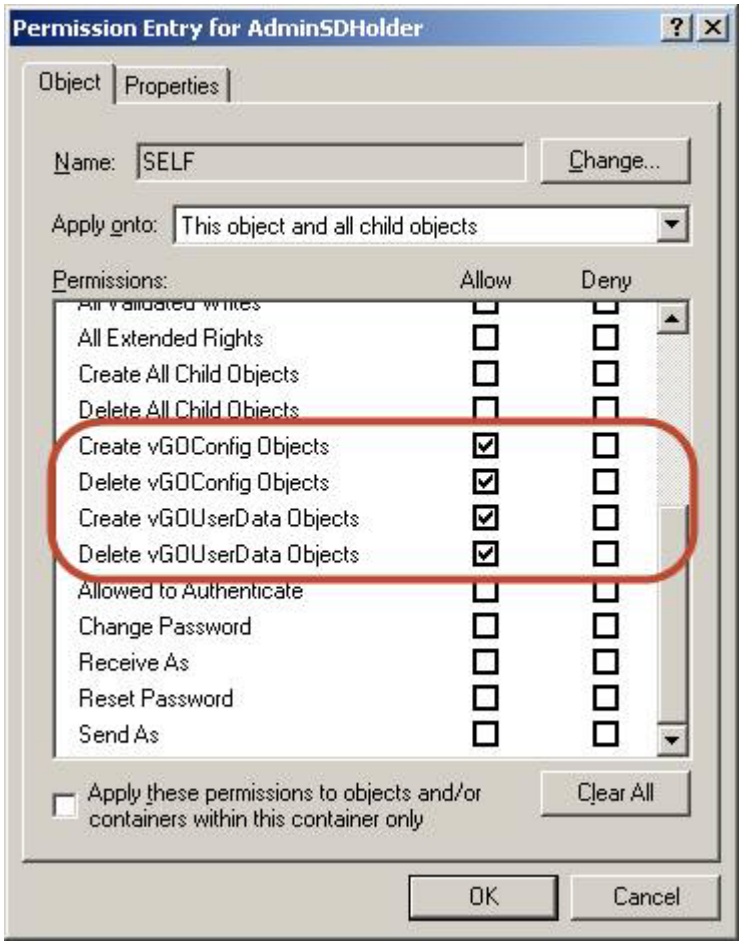
1. Log in to the primary domain controller as a domain administrator.
2. In the Microsoft Management Console, open the "Active Directory Users and Computers" snap-in.
3. From the **View** menu, select **Advanced Features.**
4. Navigate to the **AdminSDHolder** container located in `cn=AdminSDHolder,cn=System,dc=<domainName>,dc=<domainSuffix>`
5. Right-click the AdminSDHolder container and select Properties.
6. In the "Properties" dialog, select the Security tab and click Advanced.
7. In the "Advanced Security Settings" dialog, click Add… .
8. In the "Select User, Computer, or Group" dialog, enter the name of the Universal Authentication Managerservice account and click OK.
9. In the "Permission Entry" dialog, do the following:

a. From the **Apply onto:** drop-down list, select **This object and all child objects**.

Note: If the create and delete permissions for `vGOUserData` objects do not appear in the permissions list, select User objects from the **Apply onto:** drop-down list instead. This variation occurs between different versions and patches of Active Directory and the underlying operating system.

---

b. In the list of permissions, select the **Allow** check box for the permissions shown below:



c. Click **OK**.

10. Trigger the SD propagator (SDPROP) process to immediately propagate the changes throughout the network. Instructions for launching the SD propagator process are provided in the following Microsoft Knowledge Base article: http://support.microsoft.com/kb/251343.

Note: If you encounter a version of this procedure that calls to apply the above permissions onto "This object only," disregard it. It is deprecated and has been superseded by the steps above.

You can trigger the SD propagator process by kicking off the **RunProtectAdminGroupsTask** task.

6.3 Configuring Universal Authentication Manager for Synchronization with Microsoft AD LDS (ADAM)

Note: Before completing the procedures in this section, note that:

- Oracle recommends that you install Universal Authentication Manager in local mode and switch it to enterprise (synchronization) mode (as described in the Universal Authentication Manager section of the *Oracle Enterprise Single Sign-On Suite Administrator's Guide*) only after you have prepared the repository and configured synchronization settings. Otherwise, Universal Authentication Manager data structures may not be correctly created or permissions correctly set within the repository.
- When deploying Universal Authentication Manager in enterprise mode, users must not enroll in any logon methods until synchronization with the repository has been properly configured and tested. Otherwise, enrollment data will be lost.
- Only Microsoft Active Directory and Microsoft AD LDS (ADAM) are supported as repositories.

In order to allow Universal Authentication Manager to centrally store and manage policies and enrollment data in Microsoft AD LDS (ADAM), you must prepare a Microsoft AD LDS (ADAM) instance and configure Universal Authentication Manager for synchronization with that repository by performing the following tasks:

- Preparing the Repository when Logon Manager is Already Deployed
- Creating the AD LDS (ADAM) Instance and Partition
- Configuring the AD LDS (ADAM) Default Naming Context
- Creating a Universal Authentication Manager Service Account
- Extending the Schema
- Creating the People Container
- Initializing Universal Authentication Manager Storage
- Understanding the Universal Authentication Manager Repository Data Structures and Permissions
- Configuring the Universal Authentication Manager Synchronizer

When assigning user groups, keep the following in mind:

- User groups used should be in the same domain,
- Use security groups, not distribution groups,

- Universal Authentication Manager will only support a single Active Directory domain.

6.3.1 Preparing the Repository when Logon Manager is Already Deployed

If Logon Manager is already installed and synchronizing with your AD LDS (ADAM)-based repository, Universal Authentication Manager will be sharing Logon Manager's repository container to store its own policies and settings. In such cases, you do not need to extend the schema or create the People container. Instead, complete the following steps:

- Complete the steps in Initializing Universal Authentication Manager Storage.
- Complete the steps in Configuring the Universal Authentication Manager Synchronizer.

Universal Authentication Manager requires that the `People` container is located in its default location. If you have configured Logon Manager to use a `People` container located elsewhere (e.g. not in the root of the AD LDS (ADAM) partition), Universal Authentication Manager will not be able to share that container with Logon Manager; you will need to create a separate `People` container at the root of the AD LDS (ADAM) partition for Universal Authentication Manager.

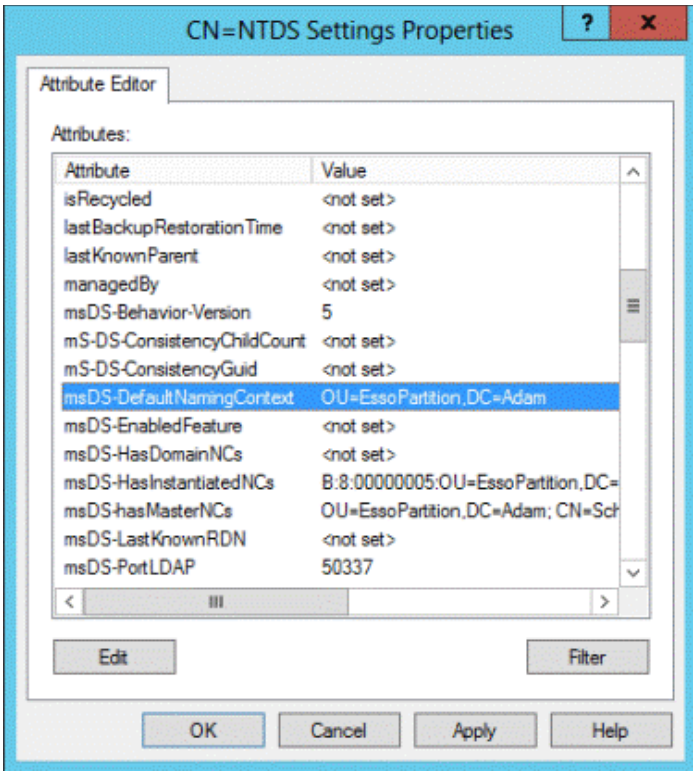
6.3.2 Creating the AD LDS (ADAM) Instance and Partition

If you have not already done so, create an AD LDS (ADAM) instance and partition by following the steps in the "Creating an AD LDS (ADAM) Instance" section of the guide Deploying Logon Manager with a Directory-Based Repository.

6.3.3 Configuring the AD LDS (ADAM) Default Naming Context

After you have created your AD LDS (ADAM) instance and partition, you must point the instance's default naming context to the target partition so that Universal Authentication Manager is able to locate its data within the repository.

1. Launch the **ADSIEdit** tool and connect to the "Configuration" context of the target AD LDS (ADAM) instance.
2. In the left-hand tree, navigate to **Configuration > CN=Sites > CN=SiteName > CN=InstanceName** .
3. Under the instance node, double-click the **CN=NTDS Settings** child node.
4. In the properties dialog that appears, select the **msDS-DefaultNamingContext** attribute and click **Edit**.
5. In the editor dialog that appears, enter the fully qualified distinguished name of the target AD LDS (ADAM) partition, then click **OK** to save your changes.

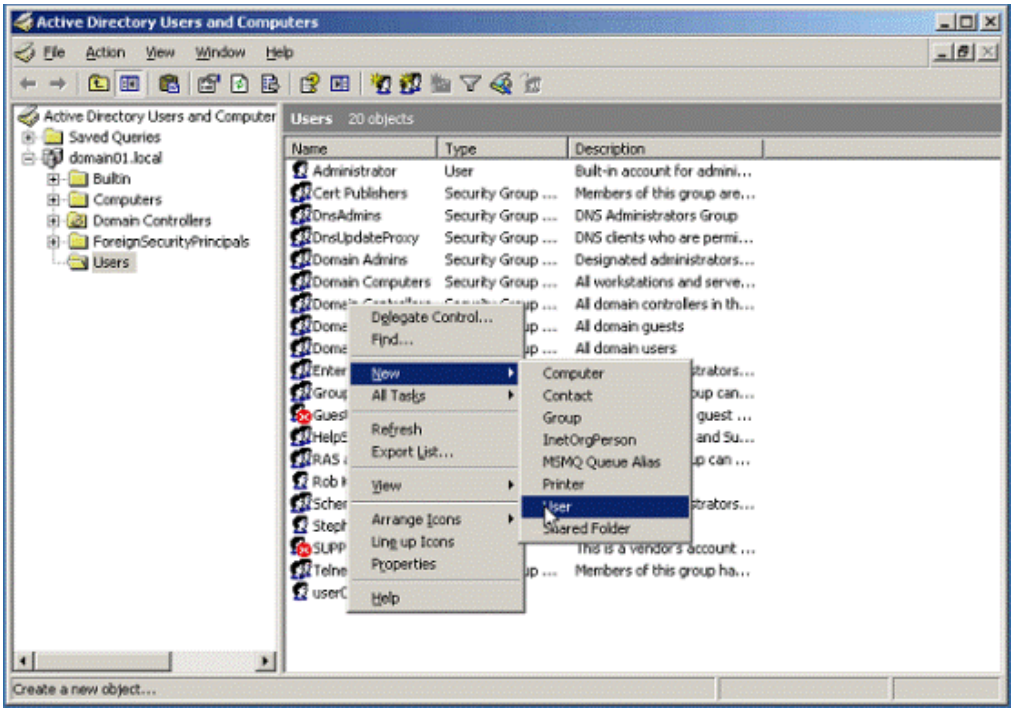


6. Click **OK** to save your changes and dismiss the properties dialog.
7. Restart the affected AD LDS (ADAM) instance by restarting the corresponding service in the Windows Services Manager.

6.3.4 Creating a Universal Authentication Manager Service Account

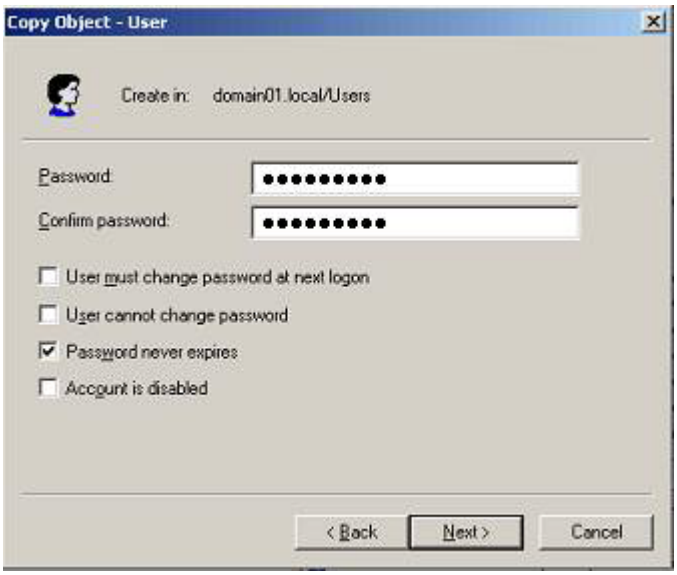
In order for Universal Authentication Manager to read and write data in the repository, you must give it the privileges to do so. This is accomplished by creating a service account that Universal Authentication Manager uses to interact with its repository. This account should be a standard domain account (member of Domain Users); no other permissions are necessary. However, you must add the account to the target AD LDS (ADAM) instance's "Readers" group.

1. On the workstation that will serve as your domain controller, launch Active Directory Users and Computers.
2. Right-click the `Users` container and select **New > User**. The `User` account is a regular member of the `Domain Users` group.

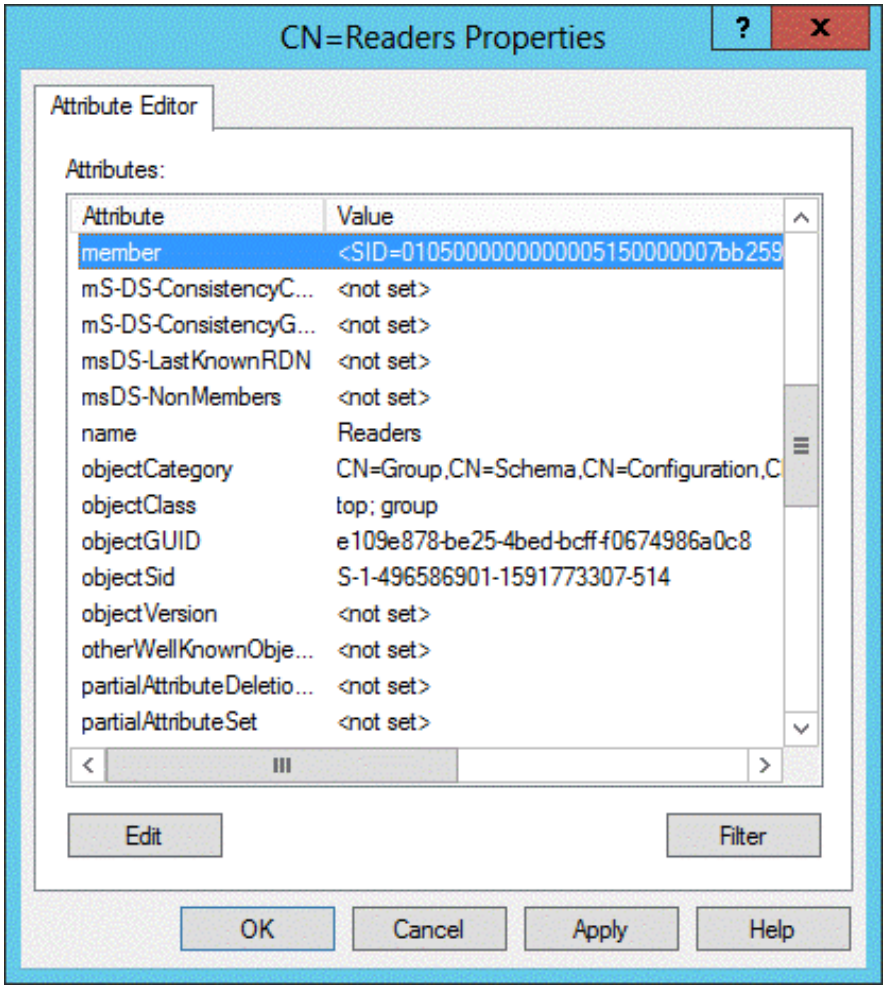


3. Enter a name for the user or group account (for this example, the name is uamservice) and click **Next**.

4. Enter a password, select the **Password never expires** box, and deselect the **User must change password at next logon** box.



5. Add the Universal Authentication Manager service account to the AD LDS (ADAM) instance's `Readers` group:
   a. Start the `ADSIEdit` tool (available from the Microsoft Web site) and connect to the data partition of the target AD LDS (ADAM) instance.
   b. In the left-hand tree, expand the target partition and select the **CN=Roles** node.
   c. In the right-hand pane, double-click the **CN=Readers** role.
   d. In the properties dialog that appears, select the member attribute and click **Edit**.
   e. In the attribute editor dialog that appears, click **Add Windows Account**.
   f. In the dialog that appears, enter the name of the Universal Authentication Manager service account and click **Check Names.**
   g. Once the name validates successfully, click **OK** to dismiss the account selection dialog.
   h. Click **OK** to save your changes and dismiss the attribute editor dialog.

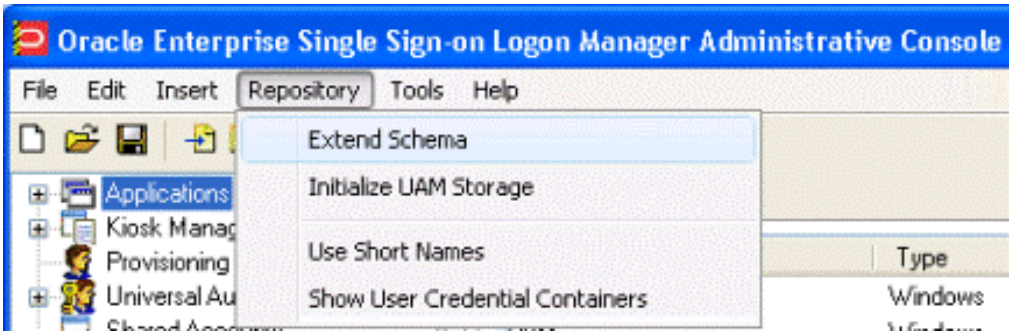


i. Click **OK** to save your changes and dismiss the properties dialog.

6.3.5 Extending the Schema

Note: If you are not sure whether you have already extended the schema, simply complete the steps below; performing the schema extension multiple times will not harm your repository or the data it contains.

1. Launch the Oracle Enterprise Single Sign-On Administrative Console.
2. From the **Repository** menu, select **Extend Schema**.



3. In the "Connect to Repository" dialog box, do the following:
   a. Enter a **Server Name**.
   b. Select **Microsoft AD LDS (ADAM)** from the drop-down menu.
   c. Select the **Use secure channel (SSL) check box** if your environment is configured for SSL connectivity.
   d. Enter the **Port** number (default SSL port is 636; default non-SSL port is 389).
   e. Enter the **Username/ID** and **Password** of an administrative account with Domain and Schema Administrator permissions.
   f. Click **OK** when finished.

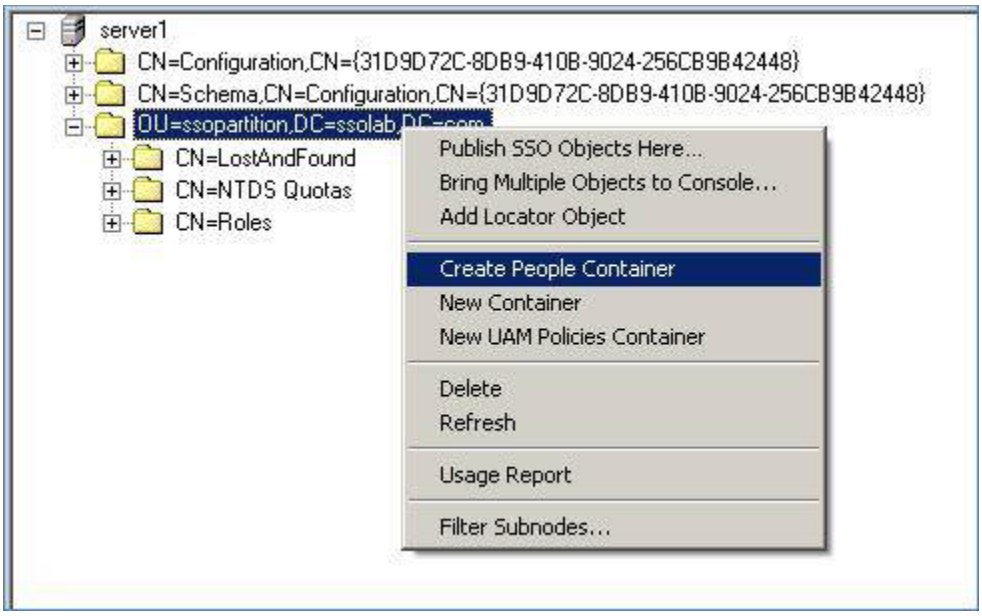
6.3.6 Creating the People Container

In order to allow Universal Authentication Manager to store enrollment data in AD LDS (ADAM), you must create an OU named `People` at the root of your AD LDS (ADAM) partition. You must not rename or move this container or Universal Authentication Manager synchronization will not function.

If Logon Manager is already installed and synchronizing with the repository and it is using a custom People container location, you must still create the People container for Universal Authentication Manager at the root of the AD LDS (ADAM) partition.

Oracle recommends that you maintain separate `People` containers for Logon Manager and Universal Authentication Manager when sharing an AD LDS (ADAM) instance.

1. In the ESSO Suite Administrative Console, select the **Repository** node in the tree.
2. Click the **Click here to connect** link in the right-hand pane. The Console displays the "Connect to Repository" dialog. Fill in the fields as explained in step 3 in the previous section and click **OK** to connect.
3. In the tree, right-click the root of the target AD LDS (ADAM) instance, and select **Create People Container** from the context menu.



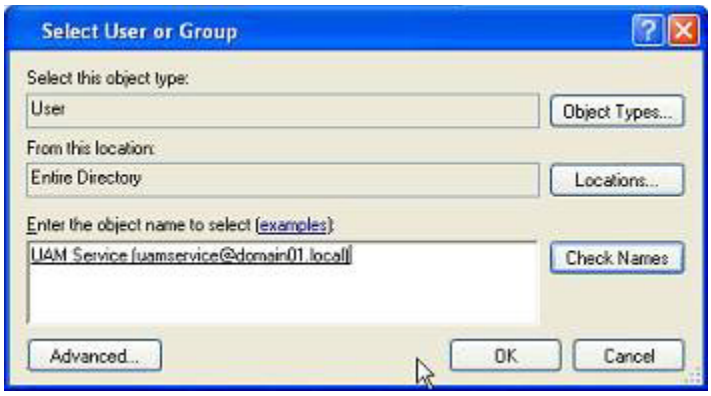
4. Verify that the `People` container now exists at the root of the AD LDS (ADAM) instance's sub-tree.

6.3.7 Initializing Universal Authentication Manager Storage

1. After successfully extending the schema, return to the **Repository** menu and select **Initialize UAM Storage**.

2. From the drop-down menu, select the server that you just created and click **OK**. (The other fields are filled in automatically.)

3. In the "Select User or Group" window, start typing the name of your service account, then click **Check Names**. The service account name is filled in automatically.



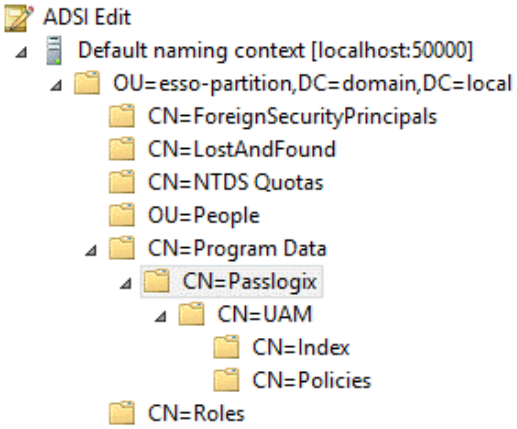
4. Click **OK** and wait for the success message.

The data structures have now been created and the required permissions set. For more information on what's done in the repository during this step, see the next section.

6.3.8 Understanding the Universal Authentication Manager Repository Data Structures and Permissions

When you invoke the **Initialize UAM Storage** command described earlier, Universal Authentication Manager does the following within your repository:

1. Modifies the schema to ensure that vgoUser and `vgoConfig` classes may be placed inside `Container` objects.
2. Builds the default container structure `Program Data/Passlogix/UAM` with subcontainers `Policies` and `Index` as shown below:



Note: Never manually modify the contents of the index and policies containers.

The containers can be named differently if your environment requires so; however, you will need to manually configure all Universal Authentication Manager client instances to point to the custom-named containers. Oracle highly recommends you leave the container names at their defaults.

3. Grants the Universal Authentication Manager service account generic read, write, modify, and delete permissions to the index container (as well as all other permissions inherited from its parent) so that the Universal Authentication Manager service can read, create, modify, and delete objects in the index container.
4. Grants the Universal Authentication Manager service account generic read permissions (as well as any permissions inherited from its parent) so that the Universal Authentication Manager service can read objects within the policies container.
5. Updates the root DSE object of the AD LDS (ADAM) partition to grant the Universal Authentication Manager service account permissions to create and delete `vgoConfig` and `vGoUser` objects under User objects across the entire AD LDS (ADAM) partition. (If the user objects have been relocated to a custom location, the permissions can be set directly at the target container instead of at the root.)
6. Updates the root DSE object of the AD LDS (ADAM) partition to grant the Universal Authentication Manager service account generic read permissions to all `vgoConfig` objects across the AD LDS (ADAM) partition so that the Universal Authentication Manager service can read all `vgoConfig` objects regardless of their location in the repository.

6.3.9 Configuring the Universal Authentication Manager Synchronizer

You are now ready to configure the Universal Authentication Manager to allow Universal Authentication Manager to synchronize with the repository. Complete the following steps:

1. Launch the Oracle Enterprise Single Sign-On Administrative Console.
2. In the left-hand tree navigate to **Global Agent Settings > [TargetSettingsSet>] > Synchronization**.

3. If Logon Manager is not installed and synchronizing with the repository, add a configuration node for the AD LDS (ADAM) synchronizer to your settings set as follows (otherwise skip to the next step):
   a. Right-click the **Synchronization** node and select **Manage synchronizers** from the context menu.
   b. In the window that appears, click **Add**.
   c. In the list of available synchronizers, select **Microsoft AD LDS (ADAM)**, enter `ADAMSyncExt` as the name, and click **OK**.
   d. Click `OK` to dismiss the dialog. The **ADAMSyncExt** node appears under the **Synchronization** node.
4. If Logon Manager is installed and synchronizing with the repository, do not modify the value of the **Servers**, **SSL**, or **Base location(s) for configuration objects** fields; instead, skip to the next step. If Logon Manager is not installed and synchronizing with the repository, do the following:
   a. In the **Servers** field, select the check box.
   b. Click the **...** button.
   c. In the window that appears, enter the full address(es) and port(s) of your AD LDS (ADAM) instances, one per line, in the format `<server>:<port>`.
   d. Click **OK**.
   e. In the **Base location(s) for configuration objects** field, select the check box.
   f. Click the **...** button.
   g. In the window that appears, enter the fully qualified DN of the Universal Authentication Manager Policies container.
   h. Click **OK**.
   i. If your environment is not using SSL, select the check box next to the **SSL** field and select **No** from the drop-down field. Oracle highly recommends utilizing SSL in your environment for maximum security.
5. In the **Base location(s) for UAM storage index** field, select the check box, click the **...** button, and enter the fully qualified DN of the Index container, then click **OK**.
6. In the **Prepend Domain** field, select the check box and select **Yes** from the drop-down menu.
7. Configure other synchronization settings as desired; for more information on each setting, see the Console help.
8. Export your settings to a `.REG` file for distribution to end-user workstations:
   a. From the **File** menu, select **Export**.
   b. In the dialog that appears, click **HKLM Registry Format.**
   c. In the "Save" dialog that appears, navigate to the desired location and provide a name for the `.REG` file, then click **Save**.
9. Distribute the **.REG** file to your Universal Authentication Manager workstations and merge it into their Windows registries.

Note: The Console produces a `.REG` file compatible only with 32-bit systems. If you are merging the `.REG` file on a 64-bit system, you must include the `/reg:32` switch in your import command to merge the registry data into the correct location within the registry; otherwise, Universal Authentication Manager will not function. For example:

```
reg.exe import MyRegistryFile.reg /reg:32
```

6.4 Upgrading an Existing Universal Authentication Manager Installation

Upgrading from versions of Universal Authentication Manager earlier than 11.1.2.1.0 to version 11.1.2.2.0 is not supported. You must fully uninstall any such versions of Universal Authentication Manager before installing the current version. The new version will ignore all repository data stored by any earlier versions, thus deletion of the old data is not required

Upgrading from version 11.1.2.1.0 to version 11.1.2.2.0 is fully supported and does not require any special actions.

6.4.1 Migrating from Logon Manager with Strong Authenticators to Universal Authentication Manager

Each client workstation with Logon Manager may only be configured to use one primary logon method. Logon Manager supports several native primary logon methods, including strong authenticators such as smart cards or proximity cards. If a strong authenticator is deployed and configured as the Logon Manager primary logon method, each end user must convert to using Universal Authentication Manager as the primary logon method.

End users must manually change the Logon Manager Primary Logon Method from the strong authenticator to the Universal Authentication Manager Authenticator using the **Logon Manager Agent Settings** tab to **Change Primary Logon Method**.

6.5 Installing the Universal Authentication Manager Client-Side Software

Note: Oracle recommends that you install any hardware devices, middleware, and drivers prior to installing Universal Authentication Manager.

Oracle recommends against installing Universal Authentication Manager on the same workstation as the Oracle Enterprise Single Sign-On Administrative Console to avoid lockout. You should have at least one workstation running the Oracle Enterprise Single Sign-On Administrative Console without Universal Authentication Manager.

Installing Universal Authentication Manager requires you to have local administrator permissions.

During the installation, you will be prompted to select a client mode (local or enterprise). For more information on the Universal Authentication Manager client modes, see the Universal Authentication Manager section of the the *Enterprise Single Sign-On Suite Administrator's Guide*.)

If you are installing Universal Authentication Manager on Windows 7, the Microsoft Windows Password and PKI smart card credential providers will be disabled and the Universal Authentication Manager credential provider will be enabled in their place.

If you want to perform an unattended ("silent") installation, see Performing an Unattended (Silent) Installation.

To install and configure Universal Authentication Manager:

1. Close all programs.
2. Launch the installer file appropriate to your platform.

   Note: If you are installing in a language other than English and would like to launch the installer in the desired language, execute the following command:

   ```
   msiexec /I <packagename>.msi TRANSFORMS=<language>.mst
   ```

   where `<packagename>` is the name of the Universal Authentication Manager installer MSI package, and `<language>.mst` is the name of the corresponding language transform file (included in the installer archive).

3. On the Welcome Panel, click **Next**.
4. The "Program Features" screen prompts you to select the features to install. Select the features you want by clicking the red [x] next to the feature and clicking **This feature will be installed on local hard drive**. You must select at least one **Logon Method** to proceed with the installation. The available options are:
   - **Application** - the core application.
   - **Logon Methods** - supported authentication methods.

- **ESSO-UAM Authenticator for ESSO-LM** - authentication plug-in for Logon Manager allowing integration between Logon Manager and Universal Authentication Manager.
- **Languages** - localizes the user interface into the selected language(s).

To change the destination folder, click **Change** and navigate to the desired location.

5. Select the desired client mode. (For more information on the client modes, see the Universal Authentication Manager section of the *Enterprise Single Sign-On Suite Administrator's Guide*.)
   - **Local Client Mode.** Universal Authentication Manager runs locally and does not synchronize with the repository.
   - **Enterprise Client Mode.** Universal Authentication Manager runs in an Enterprise environment and synchronizes with the repository.
6. If the installer detects a third-party GINA, it prompts you to choose between keeping the current GINA and registering the Universal Authentication Manager GINA. Oracle recommends that, if you choose to chain the GINAs, you verify in a test environment that the configuration is stable. See for more information.
7. In the "Summary" screen, click **Install**.
8. When the "Completed" screen appears, click **Finish**.
9. After installation is complete, you may be prompted to restart the machine.
   - If you installed the Client in Local Mode, click **Yes** now.
   - If you installed the Client in Enterprise Mode, click **No** and proceed to Configuring the Universal Authentication Manager Service Account to configure the required service accounts.

6.6 Performing an Unattended (Silent) Installation

In order to install Oracle Enterprise Single Sign-On products successfully in unattended ("silent") mode, the Windows Management Instrumentation (WMI) service must be running before you execute the installer. To check whether it is running and start if it is not, see Prerequisites for Unattended ("Silent") Installations.

6.6.1 Command Line Syntax

Universal Authentication Manager supports standard MSIEXEC.exe command line parameters. The command line to perform an unattended installation uses the following sequence:

```
MSIEXEC.exe [Install Flag] [MSI Installer Filename] [Custom Properties]
[User Interface Level Flag]
```

Where:

`Install Flag`. `/i` = install, `/x` = uninstall, `/a` = admin install

`Filename`. Name of the MSI package to install

6.6.2 Custom Universal Authentication Manager Installer Properties

The custom installer includes the ability to configure the following options:

- Option to select local (default) or enterprise mode

- Option to configure Logon Manager to use Universal Authentication Manager as its Primary Logon Method
- Ability to select which GINA to use
- Ability to configure custom features to install
- Ability to install in the desired language

Use the following custom parameters to configure these installer options:

- `CLIENTMODE`
  - `0` = Local Client Mode (default)
  - `1` = Enterprise Client Mode
- `GINACHOICE` (Windows XP only)
  - `0` = Keep the current GINA (default)
  - `1` = Register Universal Authentication Manager GINA
- `ADDLOCAL`
  - `"Application"` (Required)
  - `"SmartCard"`
  - `"ProximityCard"`
  - `"Fingerprint"`
  - `"ChallengeQuestions"`
  - `"UAMAuth"`

To configure which features are installed, use the standard `"ADDLOCAL"` command line option.

Note: Do NOT use the `ADDLOCAL` property with ORCA, which is command-line only.

Installable Language Packs (English is always installed)

- English
- Brazilian Portuguese
- French
- German
- Italian
- Japanese
- Korean
- Simplified Chinese
- Spanish
- Czech
- Finnish
- Dutch

- Polish
- Portuguese
- Traditional Chinese
- Danish
- Greek
- Hungarian
- Norwegian
- Romanian
- Russian
- Slovak
- Swedish
- Thai
- Turkish

6.6.3 Examples

To install Universal Authentication Manager with Smart Card and Proximity Card, in enterprise mode, using the Universal Authentication Manager GINA, with the German, Norwegian, and Turkish language packs:

```
msiexec /i "ESSO-UAM.msi" ADDLOCAL
="Application,SmartCard,ProximityCard,German,Norwegian,Turkish"
CLIENTMODE=1 GINACHOICE=1
```

To install Universal Authentication Manager with Smart Card only, in Local Client mode, and using the default GINA:

```
msiexec /qn /i "ESSO-UAM.msi" ADDLOCAL ="Application,SmartCard"
CLIENTMODE=0 GINACHOICE=0
```

To install Universal Authentication Manager with Fingerprint only, in Local Client mode:

```
msiexec /qn /i "ESSO-UAM.msi" ADDLOCAL ="Application,Fingerprint"
CLIENTMODE=0
```

To install Universal Authentication Manager with Challenge Questions, Proximity Card, Smart Card, and Fingerprint, in Enterprise Client mode, using the default GINA:

```
msiexec /i "ESSO-UAM.msi"
ADDLOCAL="Application,ChallengeQuestions,ProximityCard,SmartCard,Fingerpri
nt" CLIENTMODE=1 GINACHOICE=0
```

6.7 Completing the Installation of Universal Authentication Manager

You must complete the tasks listed below in order to successfully configure Universal Authentication Manager.

- Configuring the Universal Authentication Manager Service Account
- First-Time Logon for Enterprise Mode Users
- Selecting the Desired GINA Library (Windows XP Only)

- Recovering from Use of an Incompatible GINA (Windows XP Only)

6.7.1 Configuring the Universal Authentication Manager Service Account

When running the Client in Enterprise mode, you must follow the instructions in this section to configure each Universal Authentication Manager client so that they will be able to synchronize with an Enterprise repository.

Note: Some steps in this section need to only be performed once. Other steps must be performed every time Universal Authentication Manager is installed or upgraded.

6.7.1.1 Step 1: Grant the Service Account Local Administrator Privileges

The Universal Authentication Manager service account must be a Local Administrator on each client system. This step only needs to be done once per client, and should be done immediately after the client has been installed. These steps can be done before or after rebooting the system. You can add the Universal Authentication Manager Service Account to the local Administrators group on each workstation. Complete the following steps:

1. Click **Start > Run**, enter `compmgmt.msc` and click **OK**. The Computer Management console opens.
2. Expand **Systems Tools**, then expand **Local Users and Groups,** and select **Groups**.
3. In the right pane, right-click **Administrators** and select **Add to Group....**
4. Click **Add**. Enter the username of the Universal Authentication Manager service account that you created, and click **OK**.

6.7.1.2 Step 2: Configure the Service

You must configure the Universal Authentication Manager authentication service to run under the Universal Authentication Manager service account, and to automatically grant the account the **Log On As Service** local privilege. This step must be performed after every Universal Authentication Manager installation. Complete the following steps:

1. Click **Start > Run** and type `services.msc` and click **OK**. The **Services** console opens.
2. Double-click the **ESSO-UAM Authentication Service**.
3. In the properties dialog that appears , select the **Log On** tab, then select **This account**. Enter the name of the Universal Authentication Manager service account into the **This account** field, then enter and confirm the password.
4. Click **Apply**. The first time this step is done, you will receive a message that the **Log On As Service** right has been granted.

6.7.1.3 Step 3: Restart the Service

Restart the service to verify the new settings are working and the ESSO-UAM Authentication Service can start. If the service cannot start, you can try to revert to the Local System, restart the service, review and correct the settings, and try again.

To restart the service, right-click the service and click **Restart**.

Note: Do not leave the service in a stopped state. If the service is left in a stopped state, users may not be able to log on.

6.7.1.4 Reverting Your Changes After Uninstalling Universal Authentication Manager

To undo these steps and return to a clean system:

1. Uninstall Universal Authentication Manager or set the ESSO-UAM Authentication Service back to Local System and restart.
2. Click **Start > Run**, enter `compmgmt.msc` and click **OK**. The Computer Management console opens.
3. Expand **Systems Tools**, then expand **Local Users and Groups** and select **Groups**.
4. In the right pane, right-click **Administrators** and select **Add to Group....**
5. Highlight the Universal Authentication Manager service account and click **Remove**.
6. Click **Start > Run**, enter `secpol.msc` and click **OK**. The Local Security Policy console appears.
7. Double-click the Universal Authentication Manager service account.
8. In the properties dialog that appears, expand **Local Policies** and expand **User Rights Assignment**.
9. Double-click the **Log on as a Service** policy.
10. Select the Universal Authentication Manager service account and click **Remove**.

6.7.2 First-Time Logon for Enterprise Mode Users

It is recommended that you require Enterprise Mode users to perform their first-time logon in connected mode. If the workstation is not connected to the Active Directory Domain Controller, users will be able to log on but not enroll, because Windows cannot resolve the username while disconnected.

If users perform a first-time logon in disconnected mode, they might receive the following message when attempting to access to the Client application: "You cannot enroll in Universal Authentication Manager until you log on to Windows with the computer connected to the Windows network."

6.7.3 Selecting the Desired GINA Library (Windows XP Only)

On Windows XP systems, the Universal Authentication Manager GINA automatically chains with the Logon Manager/Password Reset GINA and with the Microsoft GINA.

During installation or when performing maintenance, the Universal Authentication Manager installer resolves the GINA chain according to the following logic:

- If the current GINA is MSGINA, Universal Authentication Manager will automatically chain to it.
- If the current GINA is SSOGINA (used by Logon Manager and Password Reset), Universal Authentication Manager configures SSOGINA to chain to UAMGINA, which then chains to MSGINA.
- If the installer detects an unknown GINA, which was installed by a third-party product, it displays the "Third Party GINA Detected" screen, and prompts the

administrator to choose between keeping the existing GINA configuration (default) or having Universal Authentication Manager attempt to register and chain with the third party GINA.

Note: Using the third-party GINA will limit the functionality of the Universal Authentication Manager GINA to varying degrees, depending on the specific GINA. Oracle recommends replacing the third-party GINA with the Universal Authentication Manager GINA.

It is possible that choosing to chain the Universal Authentication Manager GINA with an unsupported GINA might result in an unrecoverable error. If you choose to attempt chaining to an unsupported GINA, be sure to verify that it will work by trying it in a test environment beforehand.

6.7.4 Recovering from Use of an Incompatible GINA (Windows XP Only)

On Windows XP systems, if the Universal Authentication Manager installer detects an unsupported GINA, it presents you with the following choices:

- Keep the current GINA
- Register Universal Authentication Manager GINA

If you opt to register the Universal Authentication Manager GINA, Universal Authentication Manager attempts to register UAMGINA and chain it to the unsupported GINA. If the third-party GINA is incompatible with UAMGINA, upon restart you might be unable to log on. In order to regain control of your workstation, perform the following steps to modify the registry manually:

1. Restart workstation, boot in Safe Mode and log on as a local administrator.

   Note: Do not restart in Safe Mode with Networking or Safe Mode with Command Line. Refer to Microsoft documentation for more information about restarting your workstation in the different Safe Modes.

   ---

2. Launch the Windows Registry Editor.
3. Select the GINA configuration that you want to use from the following list. If you plan to uninstall Universal Authentication Manager after recovery, deleting the `OrigGinaName` entry will prevent an unintended modification of the GinaDLLregistry entry.

   To restore the standard Windows logon:

   a. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` and delete the `GinaDLL` registry entry.

   b. Restart.

   To configure for Universal Authentication Manager GINA only:

   a. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` and ensure that the `GinaDLL` registry entry is set to `UamGina.dll`.

   b. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix\UAM\Gina` and delete any `ChainToGinaName` registry entries.

c. Restart.

To restore any previously configured third-party GINA:

a. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix\UAM\Gina` and copy the value of any `OrigGinaName` registry entry to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL`, or set `GinaDLL` to the name of the third-party GINA library.

b. Restart.

7

Installing Anywhere

This section describes the steps necessary for installing Anywhere. It covers the following topics:

- Prerequisites for Installing Anywhere
- Prerequisites for Unattended ("Silent") Installations
- Installing the Anywhere Console

Before installing Anywhere, please read Appendix A: Deploying Oracle Enterprise Single Sign-On Suite Products for Offline Use via Anywhere.

7.1 Prerequisites for Installing Anywhere

Before you install Anywhere, ensure the prerequisites listed in this section have been satisfied.

> **Note:** Please refer to the latest release notes to find out about last-minute requirements or changes that might affect your installation.

7.1.1 Prerequisites for Installing the Anywhere Console

> **Note:** When installing on Windows XP, you must install the latest root certificate update from Microsoft, otherwise the installation will fail.
>
> For details and instructions, see the following Microsoft Knowledge Base article:`http://support.microsoft.com/kb/931125`

- Anywhere reads the configuration of the other Oracle products from which you will create the Anywhere deployment package. Prior to installing Anywhere, install the products that you intend to deploy. Follow the installation and setup instructions for these products from their respective installation and setup guides. The deployment package must include Logon Manager and might include Oracle Enterprise Single Sign-On Provisioning Gateway (Provisioning Gateway).
- Install these products on a clean workstation. If you are deploying Provisioning Gateway, install its Administrative Console on a different workstation.

> **Note:** The Visual C++ Runtime Library and .NET 2.0 Framework are prerequisites for running Anywhere. The installation package includes the Visual C++ Runtime Library, however you must make the .NET 2.0 Framework available to users. See the Oracle Enterprise Single Sign-On Suite *Release Notes* for a complete list of software and hardware requirements.

- Configure the Agents as you want the end users to work with them. End users do not have the option to alter the installation. If you want different users to install different packages, create a separate deployment package for each installation.
- There are two types of XML files associated with Anywhere:
  - o The Anywhere configuration XML. Configures the application itself. This file includes assemblies' dependencies and component files, required permissions, and the location where Anywhere places updates as you create them.
  - The deployment configuration XML. Configures the Anywhere deployments that you create. This file includes the target location of the application XML, the version of the application that the Agents will run, and the location (Web page or network file share) where Anywhere checks for updates.

7.2 Prerequisites for Unattended ("Silent") Installations

In order to successfully install Anywhere in unattended ("silent") mode, the Windows Management Instrumentation (WMI) service must be running before the installer is executed.

To check whether the WMI service is running, and start it if necessary, do the following on each target machine:

1. Open the System Management Console.
2. Open the **Services** snap-in.
3. Navigate to the **Windows Management Instrumentation** service and check its status and startup mode.

Depending on the status, do one of the following:

- If the status is **Started**, the WMI service is running; proceed to the next section.
- If the status is blank, check the service's startup type and start it as follows:
  1. Double-click the service.
  2. In the properties box that appears, set the startup type to **Manual** or **Automatic**, as dictated by your environment and click **Apply**.
  3. Click **Start**. The status changes to **Started**.
  4. Click **OK** to close the service properties dialog box.

7.3 Installing the Anywhere Console

ReadPrerequisites for Installing Anywhere before proceeding with the Anywhere Console installation.

To install the Anywhere Console:

1. Launch the ESSO-Anywhere Console.msi installer file.

2. Select **Complete** setup. Anywhere does not require any setup customization. Select the **Custom** option only to specify a directory other than the default. Click **Next** .
3. Click **Install** at the prompt.
4. Click **Finish** when the installation is completed.

See the *Oracle Enterprise Single Sign-On Suite Administrator's Guide* for instructions on creating your deployment package.

8

Troubleshooting Oracle Enterprise Single Sign-On Suite Installations

This section provides descriptions of most commonly encountered Oracle Enterprise Single Sign-On Suite installation issues and their solutions.

8.1 Windows Installer Error 1720

If an error 1720 occurs during the installation of any of the Oracle Enterprise Single Sign-On Suite components software installation, then the currently logged-on user does not have sufficient rights to install software on that machine. You must log on to the machine as a user with Administrator rights or contact your organization's IT support personnel.

8.2 Troubleshooting Provisioning Gateway Installations

The following are the most common issues that can be encountered during the installation of Provisioning Gateway, along with their solutions.

8.2.1 Provisioning Gateway Does Not Support File Synchronization

Provisioning Gateway will not function correctly if it is deployed with the file synchronizer.

The Agent is configured to store its user data as a flat file on a network drive, FTP server, NFS share, or local disk drive. Provisioning Gateway will not function in this scenario because it requires a directory in order to distinguish and provision individual user accounts.

8.2.2 Multiple Locators Require an Entlist at Each Locator Site

If two users are stored in different containers, a matching application configuration list (entlist) must exist in each locator site in order for provisioning to work down to the client. The matching entlists must exist under both containers that store the user credentials.

8.2.3 Using Active Directory or AD LDS (ADAM) and IIS Web Services on Different Servers

If IIS and Active Directory (or the AD LDS (ADAM) instance) are on different computers, then you must provide the IIS Web services with a user account that is in

the same domain as (or a trusted domain of) Active Directory or AD LDS (ADAM), and that is provided with read/write access to the directory.

8.2.4 Internet Security Settings (Windows Domain and Citrix MetaFrame® Users)

In order for Windows domain users and Citrix MetaFrame users to access Provisioning Gateway, you must add the Provisioning Gateway Web service to the workstation's Local Intranet zone.

8.2.5 Deploying Provisioning Gateway With Multiple Oracle Internet Directory (OID) Servers

When Provisioning Gateway is deployed with multiple Oracle Internet Directory (OID) servers load-balanced in an active-active (all servers active) topology, Provisioning Gateway cannot resolve the client-server session state due to multiple servers being involved in the session. This will cause Provisioning Gateway to behave erratically. To avoid this issue, do one of the following:

- For simple failover support, load-balance your deployment using an active-standby topology. In this configuration, only one OID server is handling connections from Provisioning Gateway clients at any given moment. Backup servers, synchronized with the active server via replication, are ready to take over if the active server fails. You must configure your network to automatically re-route the connections from the failed server to one of the backup servers when a failure occurs.
- (Recommended) Use the Oracle Real Application Cluster (RAC) technology to create an OID server cluster. A cluster will appear as a single server to Provisioning Gateway clients, while providing the performance and high availability of a fully load-balanced deployment. In case of server failure, operation continues uninterrupted, and servers can be replaced on the fly. Servers can also be added at any time, providing quick and easy scalability.

8.3 Troubleshooting Password Reset Installations

This section describes how to troubleshoot most common Password Reset installation problems.

8.3.1 Server Error in "/vGOSelfServiceReset/ManagementClient" Application

When you install .NET 2.0 on a computer running a newly installed operating system, the Network Service account must be granted read/write access or you will encounter a server error when you access the Password Reset 7.0 Management Console.

To avoid the server error, grant the Network Service account read/write access to the following folder:

C:\Windows\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files

This is not a Password Reset-specific issue. All ASP.NET applications will receive this error if the configuration is not set correctly.

8.3.2 Group Security Policy: Password History Setting Should Be Increased

Password Reset uses the password history setting of the Windows XP Group Security Policy. You should allow for one additional prior password in addition to the Enforce password history setting. For example, if the setting is 3 (ensuring that a user's last

three prior passwords cannot be reused), Password Reset uses one of these, so the actual setting is 2. Oracle recommends a higher setting for Enforce password history for optimal security.

9

Uninstalling Oracle Enterprise Single Sign-On Suite Components

To uninstall one or more Oracle Enterprise Single Sign-On Suite components, do the following:

1. From the **Start** menu, open the **Control Panel**.
2. Depending on your operating system:
   - Open **Add/Remove Programs**.
   - Open **Programs and Features**.
3. In the list of installed software, select the desired component and click **Remove** or **Uninstall**.
4. Confirm any messages that you might receive asking if you are sure you want to remove the program.
5. Follow any additional prompts to complete the uninstallation process.
6. Repeat steps 3 through 5 for each additional component you want to uninstall.

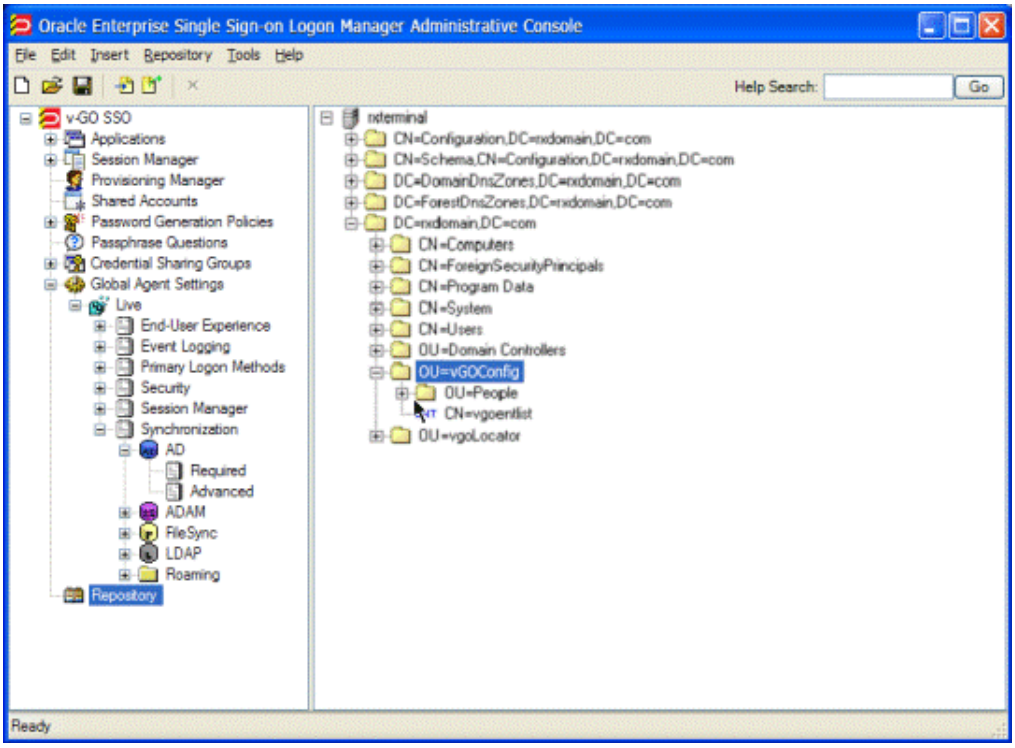
10

Appendix A: Deploying Oracle Enterprise Single Sign-On Suite Products for Offline Use via Anywhere

Anywhere reads the configuration of the other Oracle products from which you will create the Anywhere deployment package.

To create a product configuration file that Anywhere will read:

1. Carefully review the information in Prerequisites for Installing Anywhere.
2. Install the Oracle Enterprise Single Sign-On Administrative Console. For more information on configuring the Oracle Enterprise Single Sign-On Administrative Console, see the Oracle Enterprise Single Sign-On Administrative Console help.
3. Install the Logon Manager Agent.
4. Install the additional Oracle components as required. For more information, see the individual Agent installation and setup sections.
5. Configure the Logon Manager Agent and Provisioning Gateway Agent, if applicable, as you want. See the Oracle Enterprise Single Sign-On Suite Administrator's Guide and the Agent installation and setup sections for more information.
6. When you have completed your configuration, select **Global Agent Settings > Live > Write to Live HKLM**.
7. When you create the Anywhere deployment, you will have the option to use the Live HKLM settings, or an exported registry file. If you plan to use a registry file, select the set of Global Agent Settings you have configured, right-click, and Export to a .REG file. The following graphic depicts a sample configuration.



Note: Oracle recommends that you thoroughly test the registry settings before you export them for inclusion in the package.

If you want to sign your package using a digital certificate, follow the instructions for generating an X.509 certificate in the following MSDN article:
http://msdn2.microsoft.com/en-us/library/ms819929.aspx

11

Appendix B: Packaging Oracle Enterprise Single Sign-On Suite for Mass Deployment

The most convenient way to mass-deploy Oracle Enterprise Single Sign-On Suite is to create a customized MSI package and distribute it to end-user machines using a deployment tool of your choice.

An end-user machine that has been configured and tested for production acts as a configuration "master" from which the target Agent configuration will be derived for inclusion in the package. Below is a high-level overview of the required steps. The steps are described in detail later in this guide.

For information on the installable components, see MSI Package Components.

11.1 Overview of the Packaging Process

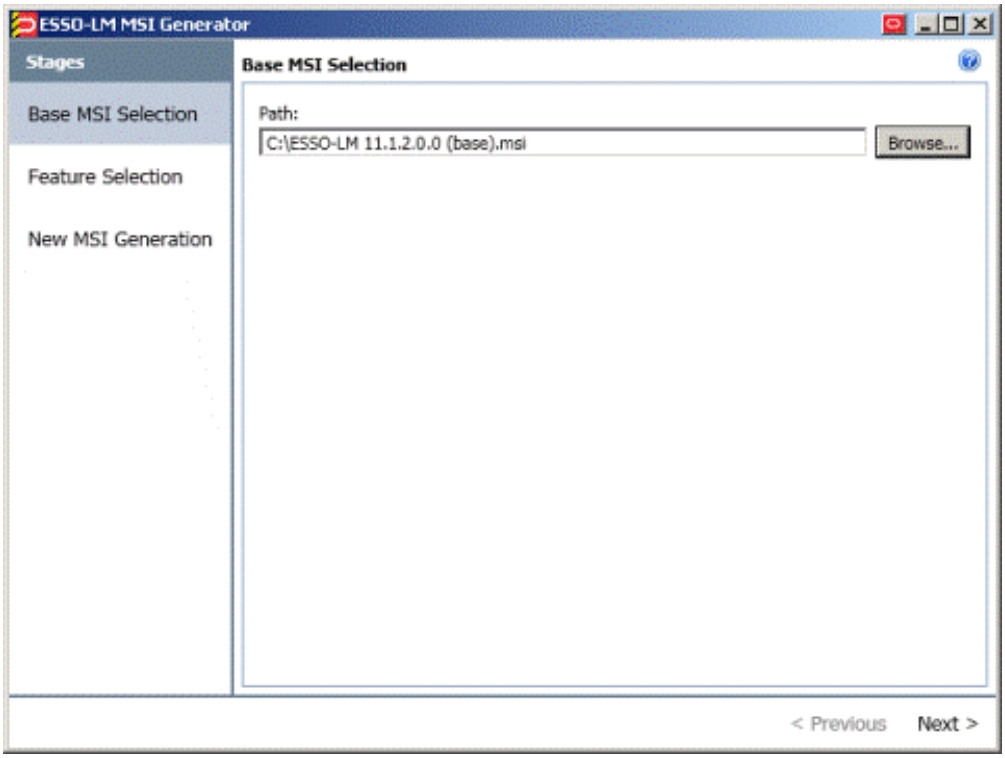
1. Obtain the latest installer for the Oracle Enterprise Single Sign-On Suite component(s) you want to deploy.
2. Obtain the latest versions of this, as well as the following documents:
   - *Deploying Logon Manager with a Directory-Based Repository*
   - *Oracle Enterprise Single Sign-On Suite Administrator's Guide*
3. If performing an unattended ("silent") installation, complete the steps in Pre-Requisites for Unattended ("Silent") Installations.
4. Install the Logon Manager Agent and the Oracle Enterprise Single Sign-On Administrative Console on the "master" machine.
5. Configure Logon Manager settings using the Console. Make sure you have thoroughly read and understood the Logon Manager Best Practices guides listed above before you begin.
6. Generate the custom MSI package using the Oracle Enterprise Single Sign-On Administrative Console:
   a. Select the Logon Manager components that you want installed on the end-user machines. (For example, if your environment calls for a single primary logon method, you may want to exclude all but the desired authenticator.)
   b. Select the customized set of global Logon Manager settings you have configured in step 4.
   c. Generate the final MSI package. This package will contain the components selected in step 6a and configuration settings from step 4.

d. Test the package by deploying it on a pilot group of machines. Identify and correct any issues that may arise. Document the solutions as necessary.

e. Once the pilot deployment is successful, deploy the MSI package enterprise-wide using a third-party tool of your choice.

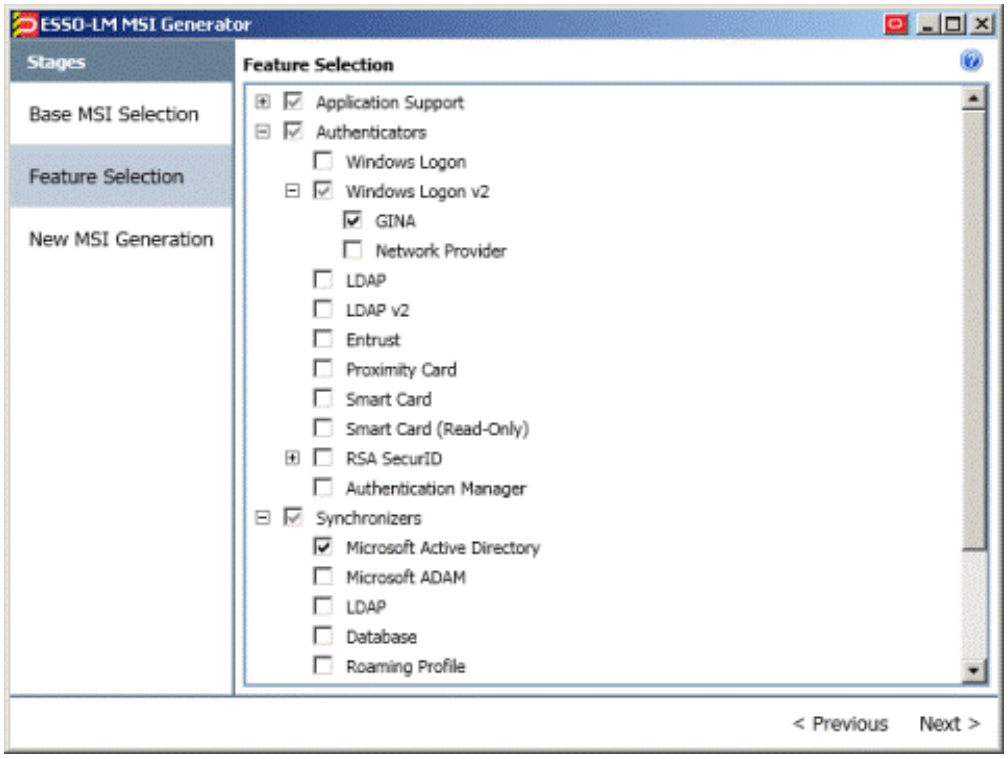
11.2 Creating a Customized Agent Installation Package

1. Place the base Logon Manager Agent MSI package in a working directory on the "master" machine.
2. Start the Oracle Enterprise Single Sign-On Administrative Console.
3. Create and configure the desired set of Global Agent settings:
   a. In the tree in the left-hand pane, right-click the **Global Agent Settings** node and select **Import --> From Live HKLM**.
   b. When the "Live" settings set appears in the tree, right-click it, select Rename from the context menu, give the set a descriptive name, and hit Enter.
   c. Configure Logon Manager as desired. For detailed information on each setting, see the *Oracle Enterprise Single Sign-On Suite Administrator's Guide*.
4. Create the customized MSI package for deployment to end-user machines:
   a. From the Tools menu, select Generate Customized MSI.
   b. In the "Logon Manager MSI Generator" wizard that appears, click **Browse** and navigate to the Logon Manager Agent base MSI package, then click **Next**.



   c. In the "Feature Selection" screen, select the Logon Manager components that you want to include in the package. Expand each category node to find the

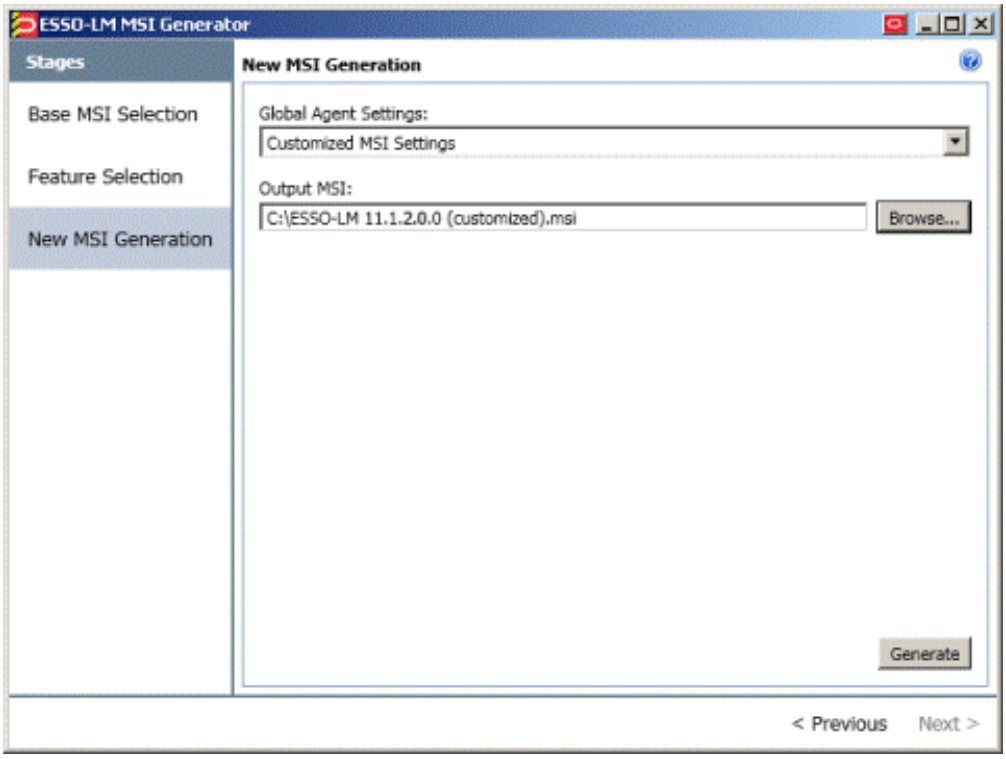
desired component(s), then select the check box next to each desired component. When you have finished, click **Next**.



d. In the "New MSI Generation" screen, select the set of global Agent settings you have created in step 3 from the "Global Agent Settings" drop-down list.

e. Click **Browse** and provide the target path and file name for the customized MSI package.

f. Click **Generate**.



g. Close the "Logon Manager MSI Generator" wizard.

h. Save the package settings to an XML file for future reference. From the **File** menu, select **Save**, enter a descriptive file name, and click **Save**.

11.3 Testing the Customized Package in a Pilot Deployment

Once you have generated your custom MSI package, test it by installing it on one or more pilot machines. Always install the package on a clean machine - that is, one that does not contain any

Logon Manager-related files or registry entries. If you are using the same machine to test multiple packages, you must sanitize it before installing a new package so that old settings and files do not remain; if the installer detects existing data, it will perform an upgrade instead of a normal installation, resulting in false problems and false positives during testing.

To sanitize your pilot machine:

1. Delete the Logon Manager installation directory and its contents:
   - On 32-bit systems: `\Program Files\Passlogix`
   - On 64-bit systems: `\Program Files (x86)\Passlogix`
2. Delete the Logon Manager user data directory:
   - On Windows XP: `\Documents and Settings\<user>\Application Data\Passlogix`
   - On Windows 7: `\Users\<user>\AppData\Roaming\Passlogix`
3. 32-bit systems only: delete the following registry keys and their children:
   - `HKEY_CURRENT_USER\Software\Passlogix`

- `HKEY_LOCAL_MACHINE\Software\Passlogix`

4. 64-bit systems only: delete the following registry keys and their children:
   - `HKEY_CURRENT_USER\Software\Passlogix`
   - `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Passlogix`

When testing the package, look for any deployment and configuration problems; Oracle highly recommends that you set up a dedicated test environment so that you can perform a full range of staging tests, including the chosen global Agent settings, administrative overrides, synchronization with your central repository, and response to applications. The last item will require that you create a set of pilot templates and test them against a selected set of applications. This will let you spot and correct any application response issues that would have otherwise arisen (and been much more costly to resolve) in production.

When the package has been fully tested and verified, use a deployment tool (such as Microsoft Systems Management Server) to deploy Logon Manager enterprise-wide.

12

Appendix C: Oracle Enterprise Single Sign-On Suite Configuration Reference

This section describes the registry settings you can use to customize the behavior of the Oracle Enterprise Single Sign-On Suite applications.

12.1 Additional Password Reset Configuration Procedures

This section describes additional procedures for configuring Password Reset that you may find useful during deployment.

12.1.1 Modifying the DCOM Permissions of the Password Reset Reporting Service

Password Reset sends reporting events to the SQL Reporting database through the SSO Reporting Service, which runs locally on the Web server. The local SSO Reporting Service sends those events to the SQL Reporting database at regular intervals.

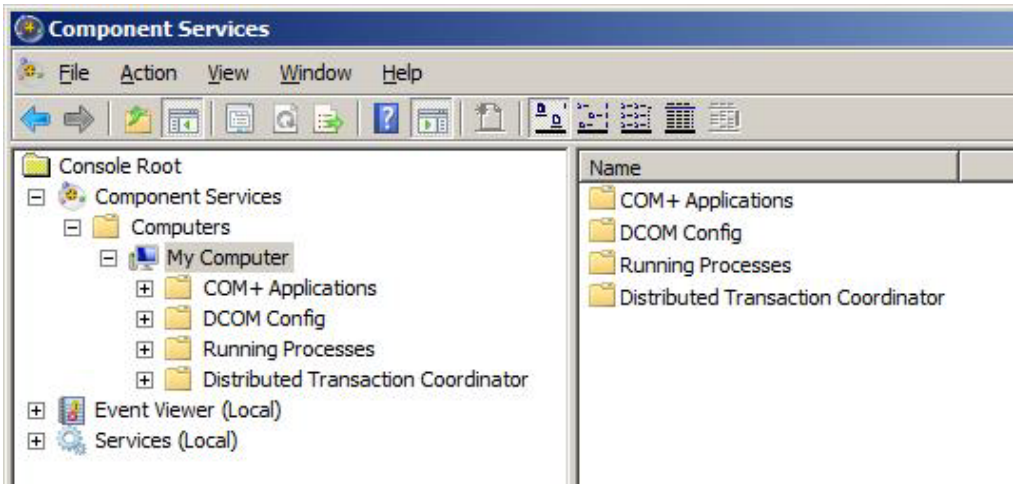
The default interval for transmitting events to the SQL Reporting database is 30 minutes. You can change this setting from the Reporting page of the Password Reset Management Console.

You can configure the Web server in one of two ways to enable reporting:

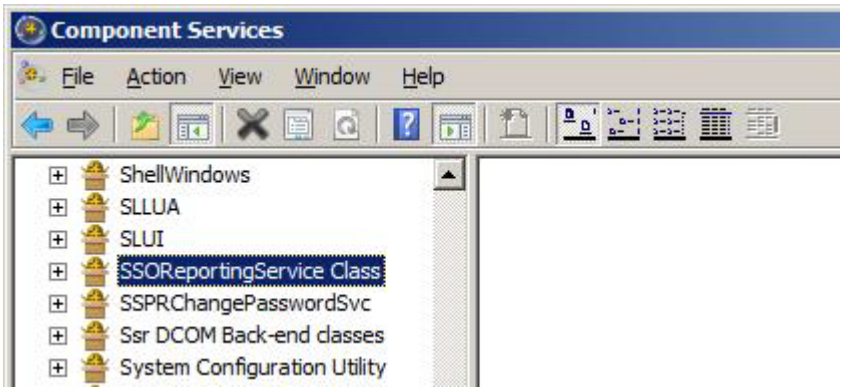
- (Recommended) Modify the DCOM permissions of the SSO Reporting Service to allow the Password Reset Reset account to launch and activate the SSO Reporting Service.
- Make the Password Reset Reset domain account a member of the local Administrators group.

To modify the DCOM permissions:

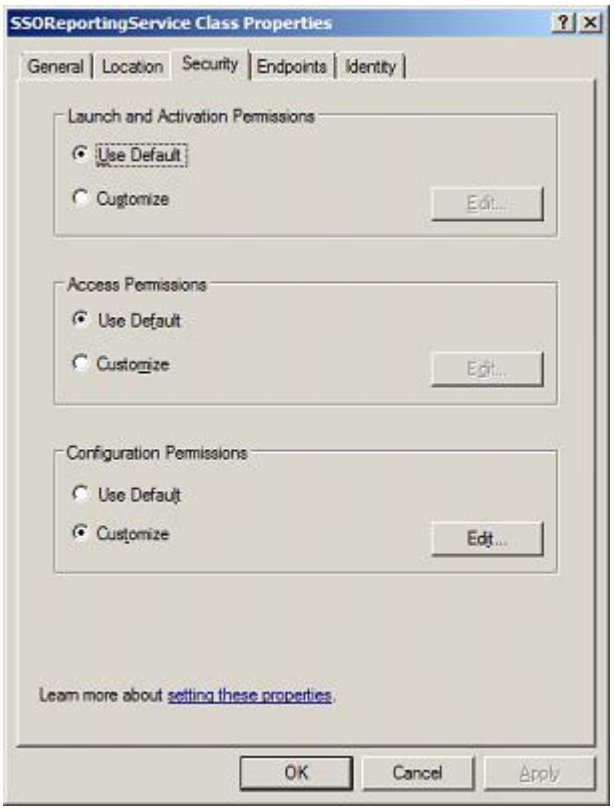
1. Click **Start > Run**. At the command prompt, type `dcomcnfg` and press **Enter** to launch the Component Services management tool.



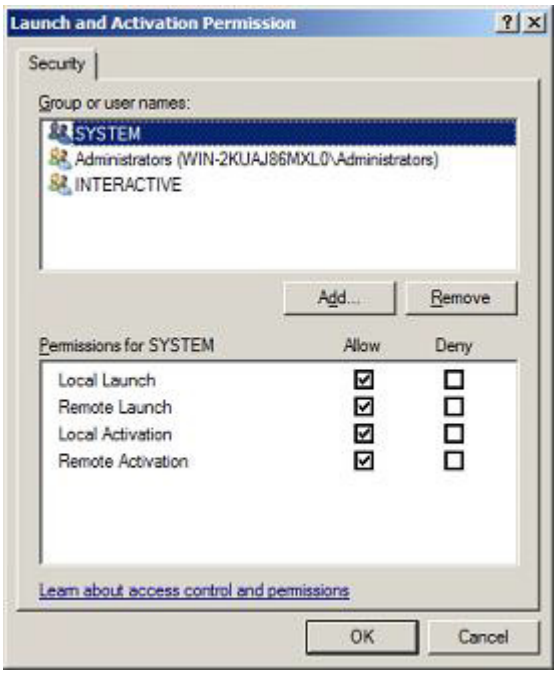
2. Navigate to the DCOM Config node: **Console Root > Component Services > Computers > My Computer > DCOM Config**.



3. Right-click the **SSOReportingService Class** node and select **Properties**.
4. Select the **Security** tab.

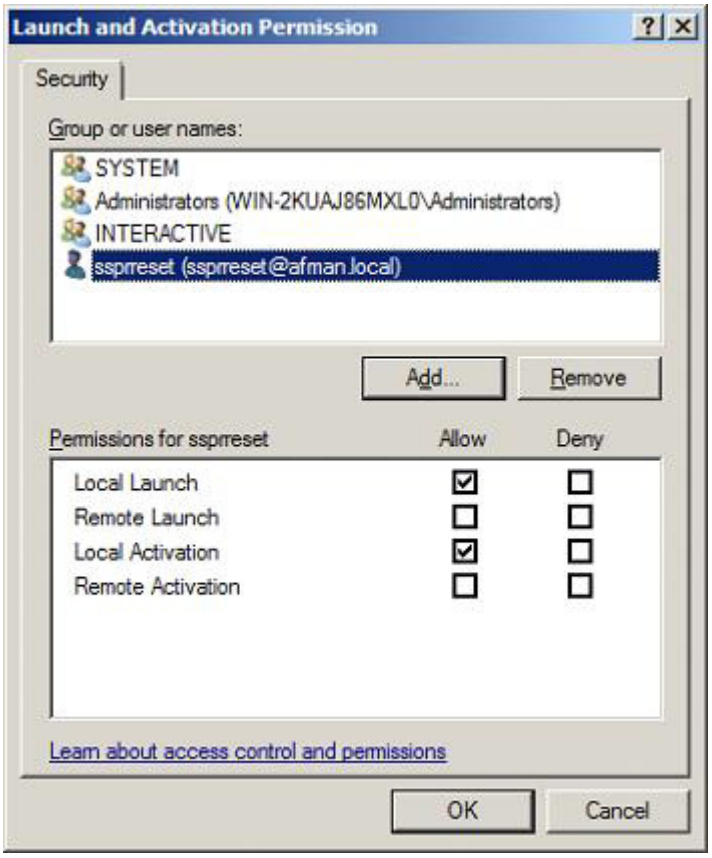


5. In the "Launch and Activation Permissions" section, click **Customize**, then click **Edit**.
6. In the "Group or user names:" section, click **Add**.



7. Enter the name of the Password Reset reset domain account and click **OK**.

8. Verify that the Password Reset reset account has "Local Launch" and "Local Activation" permissions.

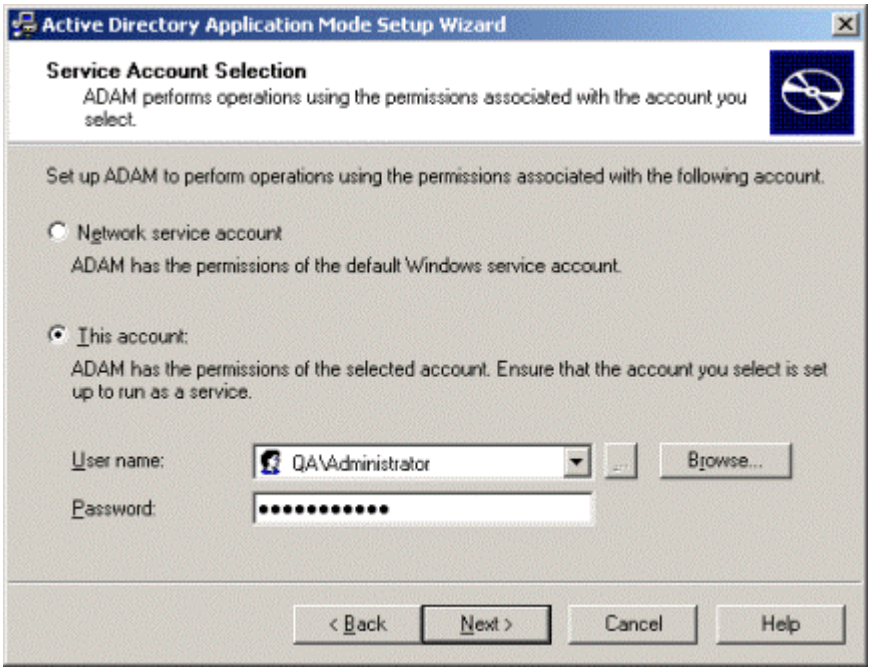


9. 9. Click **OK** twice to finish.

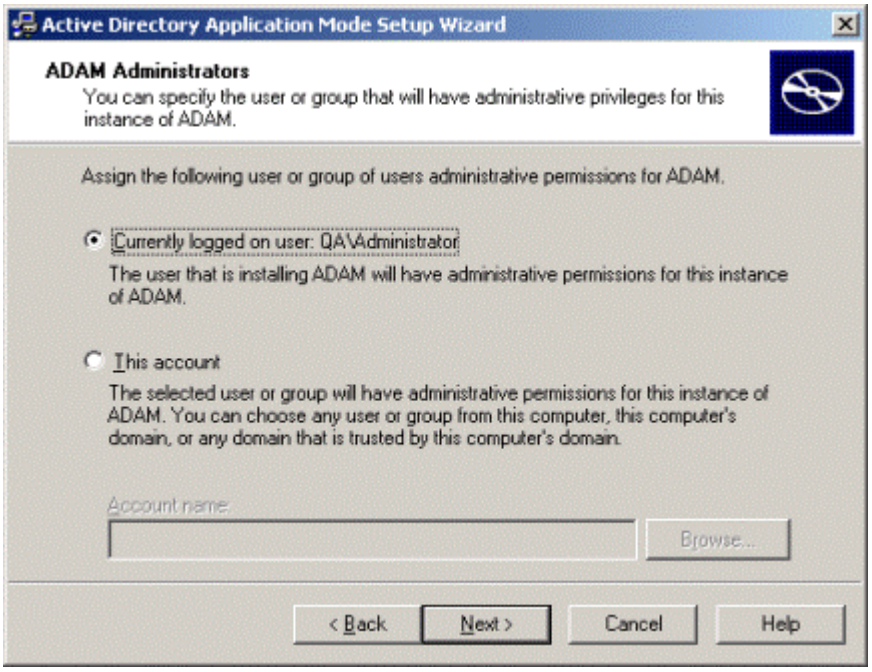
12.1.2 Installing and Configuring an AD LDS (ADAM) Instance for Password Reset

1. Run the AD LDS (ADAM) installer. Select **A unique instance** and click **Next**.
2. Provide your **Instance name** and click **Next**.
3. Specify port numbers of **10000** and **10001** (ten thousand range, for easy recall) and click **Next**.
4. Specify the root DN and click **Next**.

5. Specify an easy-to-find base location (for example, `%RootDrive%\ADAM\Instance`) and click **Next**.
6. Specify the run privileges as appropriate for your environment and click **Next**.



7. Specify the Administrative Permissions as appropriate for your environment and click **Next**.



8. Select **Do not import LDIF files for this instance of ADAM** and click **Next**.
9. In the "Ready to Install" screen, click **Next**.
10. In the "Complete" screen, click **Finish**.