Oracle® Fusion Middleware

Accessing Applications with Oracle Enterprise Single Sign-On Suite

11g Release 3 (11.1.2.3)

E54938-02

October 2016

ORACLE

Oracle Fusion Middleware Accessing Applications with Oracle Enterprise Single Sign-On Suite, 11g Release 3 (11.1.2.3)

E54938-02

Contents

Preface

Oracle Enterprise Single Sign-On Suite User's Guide introduces you to single sign-on, password management, and authentication tasks.

Audience

This guide is intended for anyone using Oracle Enterprise Single Sign-On Suite client programs to manage passwords and enrollments for logon methods, in either a workstation or kiosk environment. It discusses end-user operation of the following programs:

- Oracle Enterprise Single Sign-On Logon Manager (Logon Manager) and Kiosk Manager
- Oracle Enterprise Single Sign-On Anywhere (Anywhere)
- Oracle Enterprise Single Sign-On Password Reset (Password Reset)
- Oracle Enterprise Single Sign-On Universal Authentication Manager (Universal Authentication Manager)

In addition, a user with any role can refer to this guide for an introduction and conceptual information about Oracle Enterprise Single Sign-On Suite. You should be familiar with Windows conventions, using the internet, and the enrollment procedures for the logon methods you will use with Universal Authentication Manager.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

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

- *Release Notes*

- *Oracle Enterprise Single Sign-On Suite Installation Guide*
- *Oracle Enterprise Single Sign-On Suite Administrator's Guide*
- *Oracle Enterprise Single Sign-On Suite Secure Deployments Guide*
- *Oracle Enterprise Single Sign-On Suite User's Guide*
- *Configuring and Diagnosing Logon Manager Application Templates*
- *Deploying Logon Manager with a Directory-Based Repository*
- *Oracle Enterprise Single Sign-On Provisioning Gateway* Administrator's Guide

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

Introduction to End-User Components

Oracle Enterprise Single Sign-On Suite is designed to give you quick and simple access to all your accounts that use passwords, while requiring you to remember only one—your Windows password. Whether you spend your entire workday at one workstation, travel to different sites, are one of several users who share a workstation (such as a kiosk), or use cards, tokens, or biometrics to log on to your system, your Windows password is all you will ever have to remember.

Additionally, your administrator can provide you with a pre-configured deployment of these components, which you can access from a server, and install on any workstation in your enterprise. This option allows you to update or roll back the configuration whenever necessary, all with a few mouse clicks.

Finally, if you forget your Windows password, Password Reset provides a simple solution that lets you reset your password quickly, without waiting for an administrator or your helpdesk to do it for you.

Following is an overview of the components that comprise Oracle Enterprise Single Sign-On Suite, with a brief description of their functions. See each component's section for complete information about using it.

1.1 Oracle Enterprise Single Sign-On Logon Manager

The heart of the suite is the Logon Manager Agent. Within Logon Manager, you can view the accounts that your administrator has preconfigured for you. Depending on your administrator's preferences, you will also be able to:

- Add, delete, and modify accounts.
- Change certain settings, such as whether the Agent automatically recognizes an application and submits credentials.
- Select or change the language of the interface.
- Select or change your primary logon method.

You can also add applications on-the-fly, as you encounter them during your workday. Logon Manager recognizes a new application and captures your credentials as you enter them. If there is an application for which you never want to add a logon, you can disable it so that the Agent never responds to it again.

Additionally, if you use applications that require a password change at regular intervals, Logon Manager can change these passwords automatically when the application requests the change.

1.1.1 Kiosk Manager

If you share a kiosk with several colleagues, Kiosk Manager protects your confidential information by locking the workstation and closing your open applications when your account has been inactive for a specified period of time. You can also lock sessions manually, and unlock them using either traditional credential entry, or a strong authenticator (such as a card or token) if you use one.

1.2 Oracle Enterprise Single Sign-On Anywhere

Anywhere is a convenient, portable solution that allows you to download a deployment package configured by your administrator, and install Logon Manager and other client programs to use immediately, wherever you are. There is nothing to configure; it installs exactly as you need it. You receive notifications when updates are available, at which time you simply download and install the new deployment.

1.3 Oracle Enterprise Single Sign-On Password Reset

Password Reset is a Web-based, standalone component of the suite. When you first enroll in Password Reset, you take an enrollment interview that your administrator sets up. You are presented with questions, and Password Reset stores your answers for use at a later date. If you forget your Windows password, you click a button to launch the reset quiz. During the quiz, you are given the opportunity to answer the same questions that you answered in the enrollment interview. When you answer enough questions correctly, Password Reset automatically presents a screen in which you can enter and confirm a new password. The process is quick, and you never have to wait for an administrator or helpdesk to get back to you.

1.4 Oracle Enterprise Single Sign-On Universal Authentication Manager

Universal Authentication Manager enables enterprises to replace the use of native password logon to Microsoft Windows and Active Directory networks with stronger and easier to use authentication methods. The Universal Authentication Manager system also enhances enterprise security beyond traditional password authentication by providing two-factor authentication methods. Universal Authentication Manager enables users to rapidly and securely enroll credentials that will be used to identify and authenticate them.

At its core, Universal Authentication Manager offers a flexible, adaptable, and truly universal authentication solution, capable of integrating with a wide variety of authentication methods through its framework and APIs. Out-of-the-box, Universal Authentication Manager offers four built-in and configurable authentication methods: smart cards, passive proximity cards, biometric fingerprint, and a challenge questions quiz. Native Windows passwords are also supported.

With a similar interface to that of Logon Manager, Universal Authentication Manager offers the ease of use and enhanced security of the following authentication methods, out of the box:

- Smart cards
- Proximity cards
- Fingerprints
- Challenge questions

Universal Authentication Manager leverages Password Reset's challenge questions as an authentication method, supports native Windows passwords, and integrates with Logon Manager and a wide variety of authenticators that your administrator can configure. Using the Logon Methods tab, you can enroll and check the status of whichever authenticator(s) you are using.

To learn more about using each Oracle Enterprise Single Sign-On component, continue to the specific component's chapter.

2

Accessing Applications Using Logon Manager

Logon Manager lets you use a single password to log on to any password-protected application on your desktop, your network, and the Internet. It works "out-of-the-box" (without programming or additional network infrastructure) with virtually all applications, including Windows, Web, proprietary, and host/mainframe applications.

Logon Manager is *intelligent agent* software. It remembers your credentials—your username/ID, password, and other information-for each application or Web site and automatically responds to its logon requests.

2.1 Getting Started Using Logon Manager

After Logon Manager is installed, the Logon Manager Tray Icon appears on your Windows system tray in the lower-right corner of your screen.

If you do not see this icon, start Logon Manager:

1. Click **Start**, then **Programs**.
2. Point to **Oracle**, then **Logon Manager**.
3. Click **Logon Manager**.

The Logon Manager Tray Icon now appears in your Windows system tray. See the System Tray Icon Menu Options.

After the Logon Manager software is installed on your workstation, the Setup Wizard guides you through the procedure for providing your primary logon information.

This procedure is performed the first time you start the program.

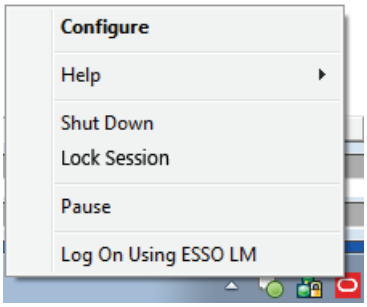
The remainder of this chapter covers these topics:

- The System Tray Icon Menu
- The Title Bar Button Menu
- Selecting Your Primary Logon Method
- Creating and Managing Accounts
- Settings
- Managing Passwords

- Using Kiosk Manager

2.1.1 The System Tray Icon Menu

Click the Logon Manager Tray Icon in your Windows system tray to display a shortcut menu of program functions, which are described below.



Note: The Lock Session option is available only for configurations that include Kiosk Manager.

If you do not see the system tray icon, start Logon Manager:

1. Click **Start**, then **Programs**.
2. Point to **Oracle**, then **Logon Manager**.
3. Click **Logon Manager**.

2.1.1.1 System Tray Icon Menu Options

The following table provides a list of System Tray Menu options and their functions.

Option	Function
Configure	Launches the Logon Manager, which displays stored accounts, allows you to add, delete and modify accounts, and manage configuration settings.
Help	Displays a submenu of options: ■ Oracle Enterprise Single Sign-On Logon Manager: Launches the Logon Manager help. ■ About: Displays version information about Logon Manager.
Shut Down	Shuts down Logon Manager.
Pause	Turns off Logon Manager logons, including the Auto-Prompt and Auto-Recognize features, and the Log On Using Logon Manager menu option, below. **Note:** You administrator has the option to limit the length of time that you can pause Logon Manager, or disable it completely.
Lock Session	Locks the current session (if Kiosk Manager is installed).

Option	Function
Log On Using Logon Manager	Engages Logon Manager to supply information to a logon request. You can use this option to engage Logon Manager when Auto-Recognize is disabled. **Note:** If Auto-Recognize is enabled, Logon Manager automatically recognizes logon requests and supplies your stored logon information. If you have not already set up the application or Web site logon, Logon Manager prompts you to do so.

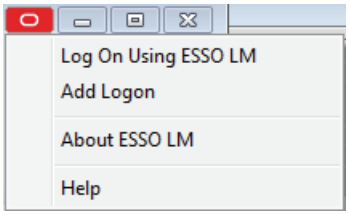
2.1.1.2 Shutting Down Logon Manager

To shut down Logon Manager, click the system tray icon and select **Shut Down** from the shortcut menu.

2.1.2 The Title Bar Button Menu

You can put the Logon Manager Title Bar Button on all application window title bars. The button lets you log on quickly to applications and Web sites you've already configured and add new accounts as you work.

You can set the Title Bar Button to display a shortcut menu for using or adding logons, or you can omit the menu and use the Title Bar Button as a one-click logon command.



2.1.2.1 Showing or Hiding the Title Bar Button

To show or hide the Title Bar Button:

1. Open Logon Manager.
2. Click the **Settings** panel, and select the **Display** tab.
3. Check **Display the Logon Manager button on all window title bars** to activate the title bar button.
4. Check **Provide a dropdown menu from title bar button** to activate the shortcut menu, or clear the check box to deactivate the menu. If you clear this option, clicking the Title Bar Button initiates a logon to the active application.
5. When you have completed your changes, do one of the following:
   - Click **Apply** to confirm your changes and close Logon Manager.
   - Click **Apply** to confirm your changes (without closing Logon Manager), and select another Settings tab.
   - Click **Cancel** to discard your changes.

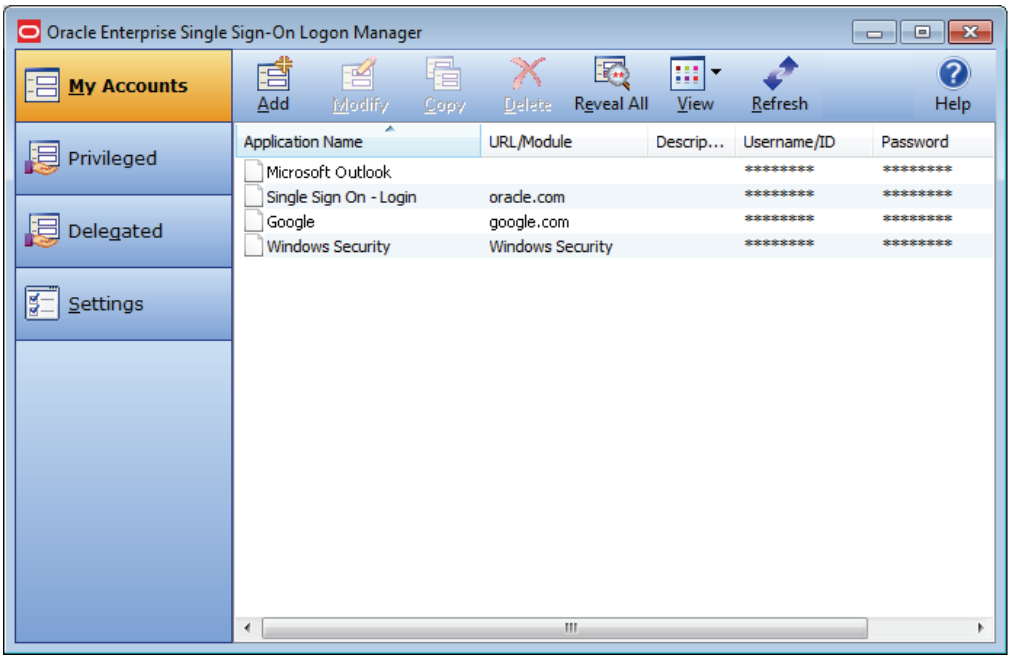
Note: To hide the Title Bar Button and menu at any time, click the Title Bar Button on any application title bar and select **Hide Title Bar Button.**

2.2 Using Logon Manager

Logon Manager displays stored accounts, and allows you to add, delete, and modify accounts and manage configuration settings.

To display the Logon Manager, click the Logon Manager Tray Icon in the Windows system tray to display the shortcut menu. Click **Configure**.

- As you add or create accounts, the available accounts are displayed in the My Accounts tab of Logon Manager.
- Logon Manager configuration options are available in the Settings panel.



2.2.1 My Accounts Panel

The My Accounts panel displays all of your stored accounts, and allows you to add, delete, copy, and modify accounts. For faster access, the **Modify**, **Copy**, and **Delete** controls are also available in a context menu accessible by right-clicking the desired application in the list. The following table lists the controls on this panel.

Icon	Label	Purpose
	Add	Launches the New Logon dialog to set up a new account.
	Modify	Launches the **Modify Account** dialog, which allows you to modify account information or automatic behavior for individual accounts. You can also access this function by right-clicking the desired application and selecting **Modify** from the context menu that appears.
	Copy	Duplicate a selected account. The new account appears in the list with a "(2)" at the end of the application name. You can also access this function by right-clicking the desired application and selecting **Copy** from the context menu that appears.

Icon	Label	Purpose
	**Delete**	Remove a selected account from Logon Manager. A confirmation request appears: "Are you sure you want to delete the selected item from your system?" Select **Yes** or **No**. You can also access this function by right-clicking the desired application and selecting **Delete** from the context menu that appears. Use **Shift+Click** or **Control+Click** to select several items to delete at one time.* **Multiple item selection is new as of version 11.1.1.5.0.*
	**Reveal All**	This icon becomes active when the Details view is selected, and at least one account is defined. Reveal All displays all Username/IDs and passwords in Logon Manager. (This feature is only available if the administrator has activated it.)
	**View**	Allows you to change how accounts display, if at least one account is defined. Can display as Icons, as a List, or with full Details (similar to Windows Explorer View options). When Details is selected, the Reveal All option is enabled. (This feature is available if the administrator has not deactivated it.)
	**Refresh**	Updates account settings with changes from your administrator. (This feature is available if the administrator has not deactivated it.)
	**Help**	Launches the Logon Manager help file.

2.2.1.1 Accounts That Share Credentials

Your administrator might configure two or more accounts to share the same username and password in a credential sharing group. If the credentials for one account change, the credentials for the other accounts in the credential sharing group also change.

In some cases, where you need multiple credentials for a single application (for example, having multiple mail accounts in Microsoft Outlook), you may need to exclude those additional "identities" (each with different credentials) from this feature. In such an instance, you have the option to exclude the new account. This capability is configured by your administrator.

2.2.1.2 Accounts Without Configured Credentials

Some accounts may appear in Logon Manager in gray, italicized text with a gray icon. If you attempt to use such an account or modify it (by selecting it and clicking **Modify**), this message appears:

Credential corresponds to an application that is not currently configured in Logon Manager.

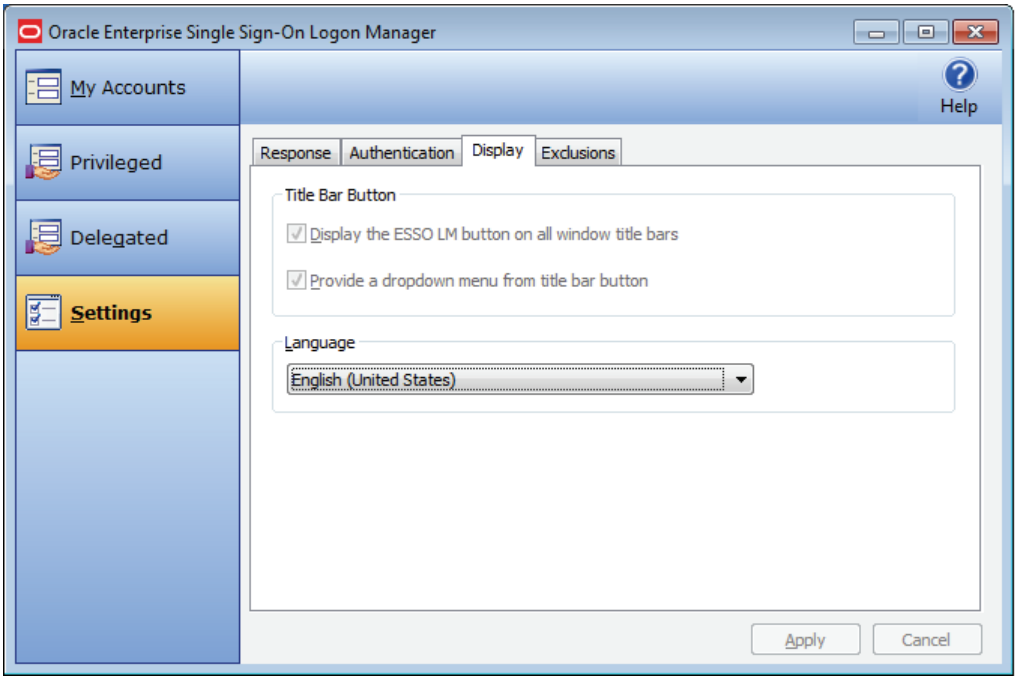
This message typically appears when Logon Manager has been upgraded from a previous version. It means that your credentials are safely stored, but the application configuration (that tells Logon Manager where to put the credentials) needs to be upgraded as well. Contact your administrator to acquire the updated accounts.

2.2.1.3 Language Settings

Logon Manager can run in many different languages, depending on which version you are running, and which language packs are installed.

Depending on your configuration, you can change the language of the Agent through the Logon Manager.

1. Open Logon Manager.
2. Select the **Settings** panel and then the **Display** tab.
3. Select from the list of available languages in the **Language** dropdown.



All Logon Manager dialogs and help screens will display in the selected language.

2.3 Using the Setup Wizard to Configure Logon Manager

Before you begin using Logon Manager, the Setup Wizard checks to make certain that Logon Manager has all the information it needs. This is also called the First Time Use Wizard (FTU). You must provide the information requested in order to use Logon Manager.

> **Note:** If you cancel the Setup Wizard, it will re-appear each time you try to start Logon Manager until you have completed the setup.

2.3.1 Setup Wizard Tasks

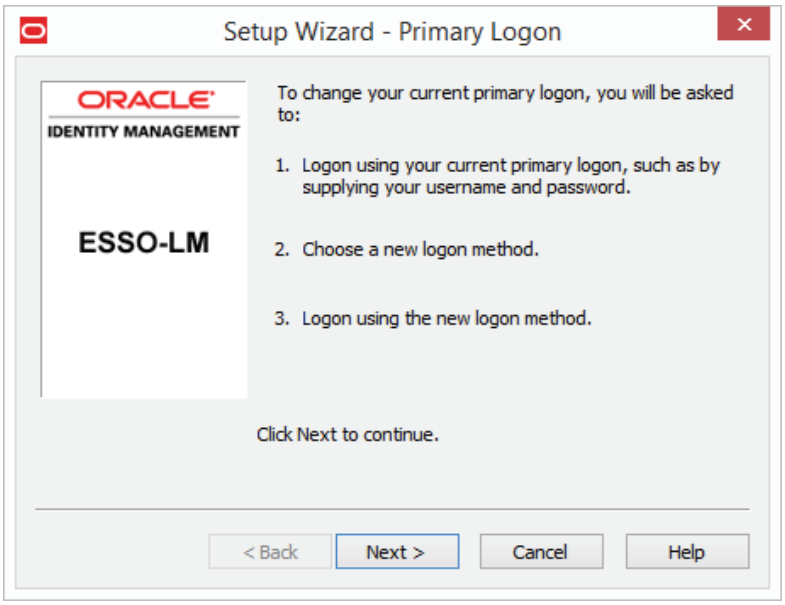
The wizard takes you through either or both of the following tasks:

- Establishing yourself as a new Logon Manager user by selecting how you will log on.
- Adding account information for specific applications

> **Note:** The Setup Wizard may skip either of the above tasks, depending on the installation options selected and your network's configuration.

2.3.2 Setup Tasks to Perform

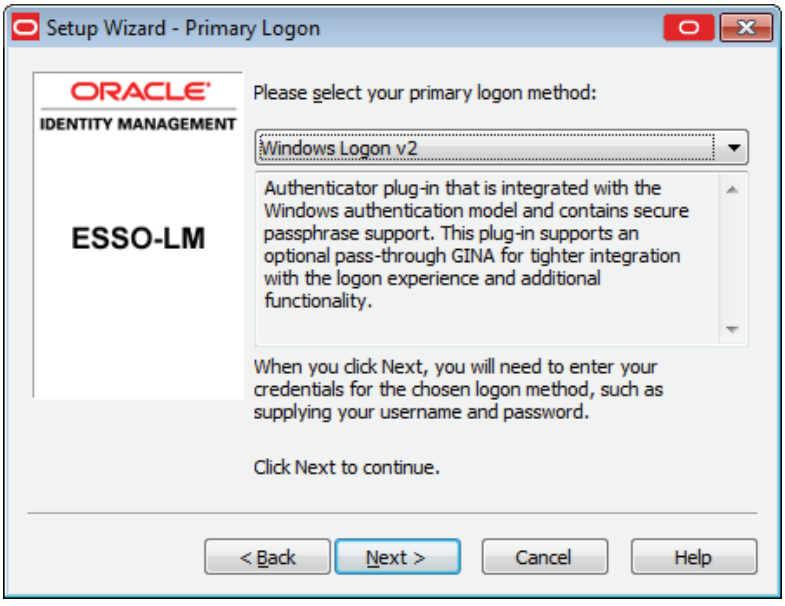
This page lists the setup tasks necessary for your local installation of Logon Manager.



Click **Next** to begin setup.

2.3.2.1 Selecting Your Primary Logon Method

Logon methods, also referred to as authenticators, are ways to access your password-protected applications. You can select to install more than one authenticator, but the primary logon method you select determines the first authenticator that Logon Manager uses.



When you first set up Logon Manager, you are prompted to choose your primary logon method. The credentials you provide to the authenticator—your username/ID, password, and other information—identify you as an authorized user of your workstation and network.

In most cases, your primary logon is Windows Logon v2, and your primary account credentials are your Windows username/ID, password, and network domain.

Logon Manager lets you use your primary logon method for any other situation in which you need a password, including most Windows applications, host/mainframe applications, and password-protected Web sites. It uses your primary logon information to verify that you are the same user that initially logged on.

1. From the drop-down list box, choose the authenticator you will use as your primary logon method. In a typical installation, this is Windows Logon v2. This means you will use your Windows password to access password-protected applications.
2. Depending on your network resources and administration, you may have other primary logon methods to choose from. The available authenticators for Logon Manager are:
   - **Windows Logon v2.** Enables logging on to Logon Manager by logging on to Windows.

     If you choose Windows Logon v2, one or more passphrase questions may appear, depending on your system configuration. These are used for additional security. Enter the answer to the displayed question or questions (note the minimum length) and click **OK**.
   - **Windows Logon.** Enables logging on to Logon Manager by logging on to Windows. (This authenticator has been deprecated as of version 11.1.2.)
   - **LDAP.** Enables logging on to Logon Manager by logging on to an LDAP directory.
   - **LDAP v2.** Enables logging on to Logon Manager by logging on to an LDAP directory.

     If you choose LDAP v2, one or more passphrase questions may appear, depending on your system configuration. These are used for additional security. Enter the answer to the displayed question or questions (note the minimum length) and click **OK**.
   - **Entrust.** Enables logging on to Logon Manager by logging on to the Entrust PKI and Entelligence client.
   - **Proximity Card.** Supports authentication with HID Proximity Cards.
   - **Smart Card.** Enables logging on to Logon Manager using an MS-CAPI-capable smart card.

     If you choose Smart Card, one or more passphrase questions may appear, depending on your system configuration. These are used for additional security. Enter the answer to the displayed question or questions (note the minimum length) and click **OK**.
   - **Read-Only Smart Card.** Enables logging on to Logon Manager using a Read-Only Smart Card.
   - **RSA SecurID.** Enables logging on to Logon Manager using one-time passwords generated by RSA SecurID tokens.
   - **Authentication Manager.** Adds the capability to allow multiple logon methods to authenticate to Logon Manager. It supports a variety of strong authenticator options such as smart cards, proximity cards, and read-only smart cards.
   - **Universal Authentication Manager.** This option is available if you have also installed the Universal Authentication Manager client, and adds the capability

to authenticate to Logon Manager through the following strong authenticator options.

- **Windows Password.** Your standard Windows password.
- **Fingerprint.** Requires you to scan one or more fingerprints during enrollment.
- **Smart Card.** Enables logging on to Logon Manager using an MS-CAPI-capable smart card.

  If you choose Smart Card, one or more passphrase questions may appear, depending on your system configuration. These are used for additional security. Enter the answer to the displayed question or questions (note the minimum length) and click OK
- **Proximity Card.** Supports authentication with HID Proximity Cards.
- **Challenge Questions.** Offers an interview during enrollment, in which you will be presented with a series of pre-configured questions. At authentication, you must provide the same answers to one or more of these questions.

Note: If you select one of the Universal Authentication Manager logon methods above, and you have not previously enrolled with any of these methods, you will be prompted to enroll. You cannot use the selected logon method until you enroll.

---

3. When you have made your selection, click **Next** to continue.

   For more information about enrolling in and using Universal Authentication Manager, see Chapter 5, "Using Universal Authentication Manager for Strong Authentication."

2.3.2.2 After You Select a Primary Logon Method

Depending on your choice of authenticator(s), you may have to perform additional steps to complete the wizard.

- **For Windows logons:**

  If you choose Windows Logon as your primary logon method, a Windows network logon prompt appears. Enter your Windows Network password for the displayed username and domain and click **OK**.
- **For Smart Card logons:**

  If you choose Smart Card as your primary logon method, a smart card prompt appears. Insert the smart card and then enter your PIN. Click **OK**.
- **For Windows Logon v2, Smart Card, or LDAP v2:**

  If you choose Windows Logon v2, Smart Card, or LDAP v2, one or more passphrase questions may appear, depending on your system configuration. These are used for additional security. Enter the answer to the displayed question or questions (note the minimum length) and click **OK**.

Note: You can change your passphrase anytime later by selecting the **Change Passphrase** option whenever you confirm your primary logon method.

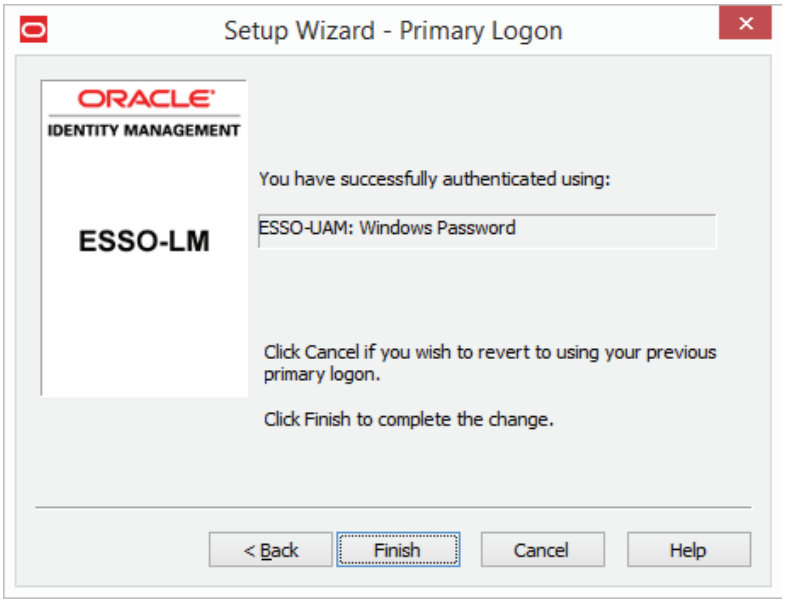
2.3.2.3 Adding Application Logons

Note: This page appears if your administrator has provided a list of pre-configured applications. This lets you store your logon credentials for each application.

1. Enter your Username/ID, Password, and any other requested information for each application you use. You may need to retype one or more items to confirm.
2. Click **Next** to continue.

2.3.2.4 Finishing Up the Setup Wizard

If you want to make changes before completing Setup, click **Back** to return to a previous Setup Wizard page.



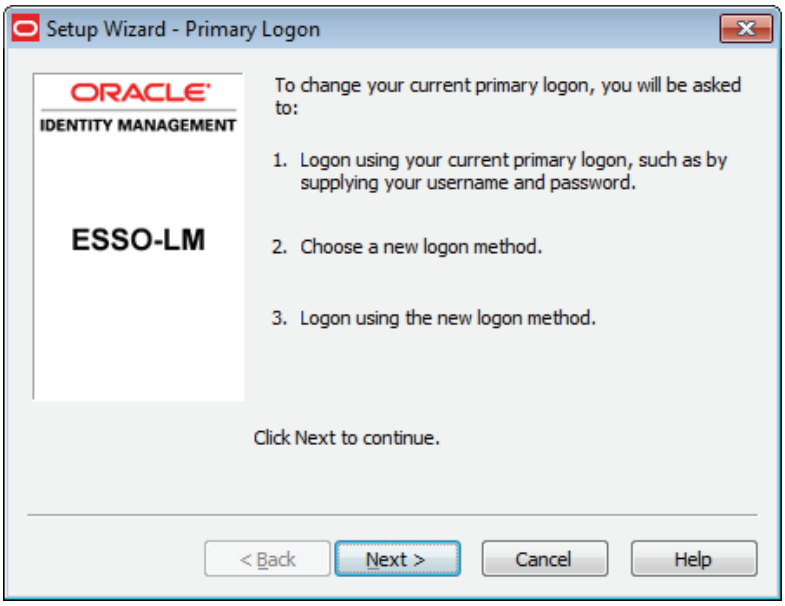
Otherwise, click **Finish** to complete setup.

2.3.3 Changing Your Primary Logon Method

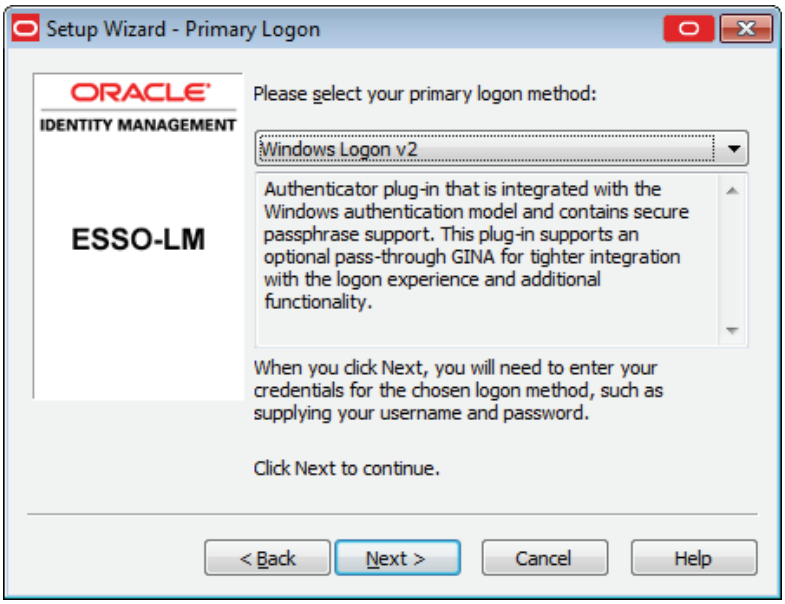
You can change your primary logon method at any time, and you can install or remove authenticators as needed.

Click the Logon Manager Tray Icon on the Windows system tray to display the shortcut menu and select **Configure**.

1. Select the **Settings** panel in Logon Manager.
2. Click the **Authentication** tab.
3. Under Primary Logon Method, click **Change**.
4. The Setup Wizard appears with a list of steps you'll follow to change your primary logon. Click **Next** to continue.



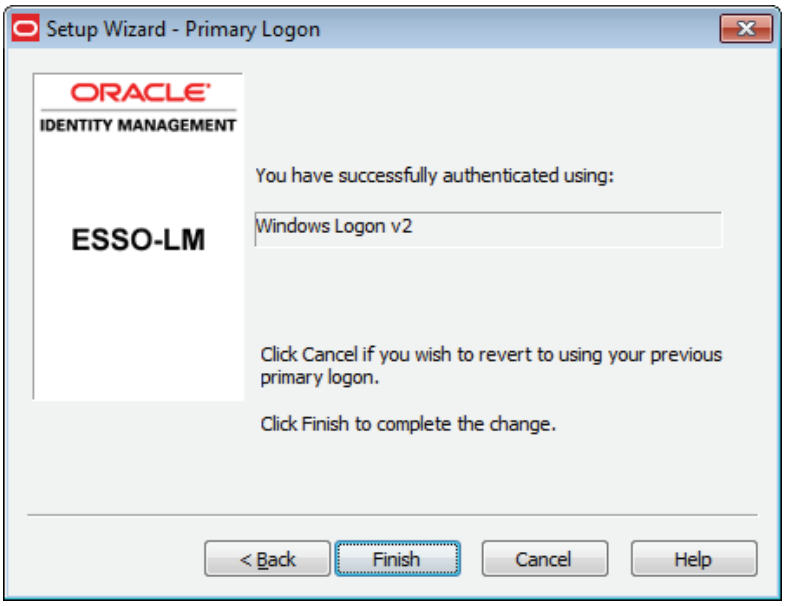
5. You are prompted for your current primary logon. Enter your primary logon password, then click **OK**.
6. The Setup Wizard displays the primary logon selection page. Select a primary logon method from the drop-down list box, then click **Next** to continue.



7. You receive a prompt for your new primary logon credentials. Enter your user ID and password, and enter or select any additional information, then click **OK**.

> **Note:** If your new primary logon is a smart card, you are prompted to insert the card into the reader and enter your personal identification number (PIN). If your new primary logon is a biometric device, you are prompted to place your finger on the fingerprint reader.

8. The Setup Wizard confirms that your new authentication is successful.

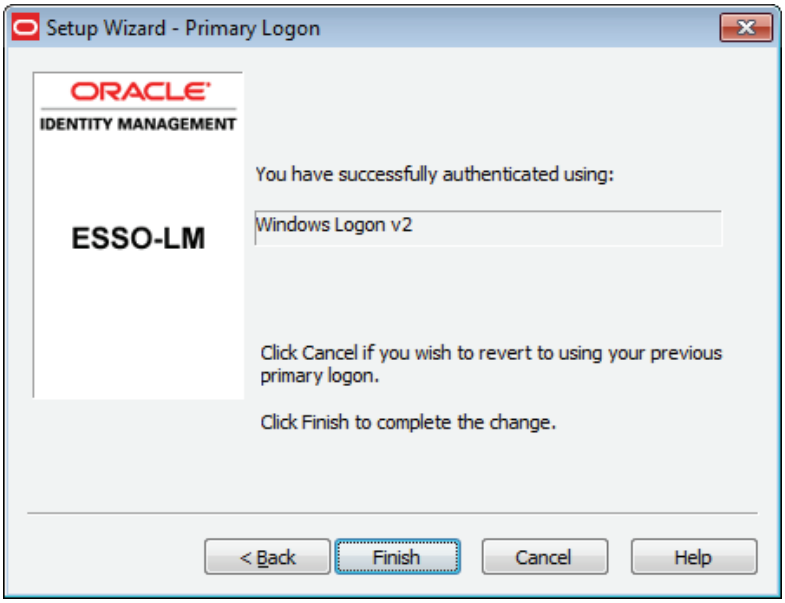


You can either:

- Click **Cancel** to cancel the change and restore your previous primary logon method.

  or

- Click **Finish** to complete your primary logon change. The Primary Logon Method dialog appears. Click **Close** to close it.



2.3.4 Confirming Your Primary Logon Method

You can configure Logon Manager to check periodically to make sure that you are the same user who initially logged on to a workstation.

When you start a password-protected application, if a specific interval of time has passed since the last automatic logon (the default is 15 minutes), Logon Manager asks for your primary logon password. If you are using a logon method other than a

password (smart card, token, biometric) as your primary logon, you are prompted for the appropriate authentication method (PIN, fingerprint, and the like).

Logon Manager also automatically performs this check when you modify your application passwords, perform other account management tasks, or if the application itself requires it.

You can change the interval, or turn this feature off, by changing the **Timer** setting in the Authentication tab of the Settings panel.

2.3.5 Installing Additional Primary Logon Methods

When you installed Logon Manager, you had the option of installing one or more authenticators. If you did not install all authenticators at that time, you can use this procedure to install them. Currently installed authenticators are listed in the Primary Logon Method dialog.

> **Note:** The following procedures for installing and removing primary logon methods are typically reserved for your administrator to perform.

1. Open Control Panel and double-click **Programs and Features**.
2. Select **Logon Manager**.
3. Click **Change**.
4. The Logon Manager InstallShield Wizard appears. Read the screen, then click **Next**.
5. Select the **Modify** option, then click **Next**.
6. Click the plus sign ("**+**") next to Authenticators to expand the list.
7. Click the **X** icon next to the authenticator you want to install.
8. From the shortcut menu, select **This feature will be installed on the local hard drive**.
9. Repeat steps 7 and 8 to install additional authenticators.
10. Click **Next**.
11. Read the screen, then click **Next**.
12. Follow the screen prompts.

2.4 Creating and Managing Accounts

An account is an application and the set of credentials that you use to authenticate to it. Depending on your configuration, you can have multiple logons for a single application, and each one is considered an account.

Logon Manager provides the means to create, modify, and delete accounts. It also allows you to exclude applications that you do not want the program to respond to (your administrator can also exclude programs as desired, in which case you will not have the option to configure a logon for them).

This section discusses how to work with accounts.

2.4.1 Creating Accounts

Logon Manager provides two ways for you to create accounts:

- You can create accounts with Logon Manager, which lets you configure, edit and manage credentials.
- You can create accounts "on the fly," as you launch applications that require credentials. This happens in one of two ways:
  - **Automatic credential capture.** By default, Logon Manager captures credentials automatically as you enter them, when you first encounter an application that requires a logon. Depending on your configuration, you might then be required to review and approve your credentials. See Automatic Credential Capture for more information.
  - **Using Auto-Prompt.** If your administrator disables automatic credential capture, Logon Manager detects an application's logon request and displays the New Logon dialog. You can then save your credentials as you log on. See Setting Up Accounts Using Auto-Prompt for more information.

Many applications require you to submit the same credential in more than one field, such as applications for which you must enter and confirm your password, or Web pages that have accounts in multiple locations. Other applications require you to enter credentials for additional fields besides your username and password. Your administrator must preconfigure such applications in order for you to take advantage of full Logon Manager functionality.*

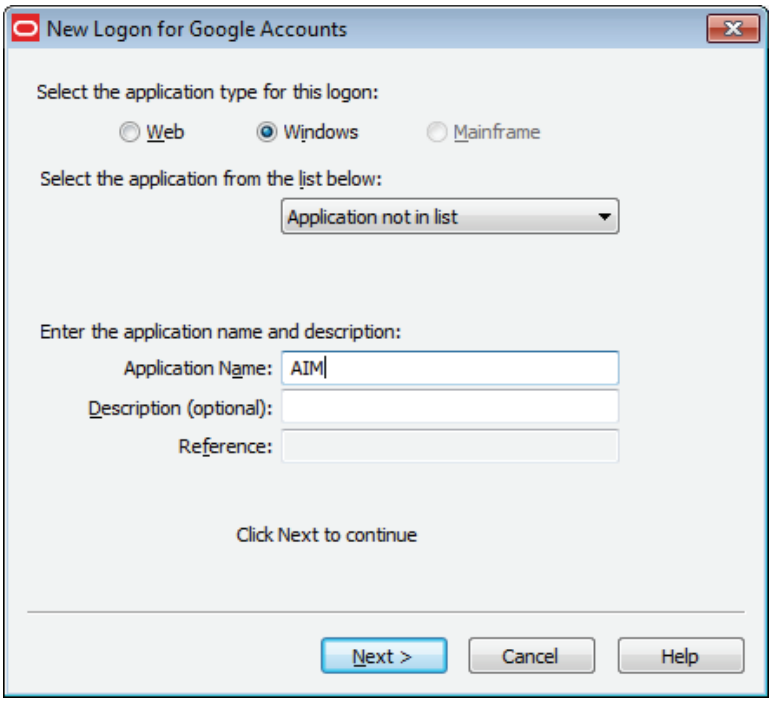
**This functionality is new as of version 11.1.1.5.0.*

2.4.1.1 Exclusions Configured by the Administrator

In certain instances, your administrator might configure your user account to be prohibited from accessing specific applications. If you attempt to add credentials for such an application, you will receive a message indicating that your account has been excluded for that application, and you will not be able to save Logon Manager credentials. Additionally, applications that the administrator excludes after you have created an account will cease responding, and will be removed from your Accounts list.

2.4.2 Using Logon Manager to Set Up Accounts That You Select

In Logon Manager, click **Add** to set up a new account. The New Logon dialog appears.



In most instances, your installation of Logon Manager already contains applications that your administrator has pre-configured. Any such application will be available for you to select during this procedure. The next sections describe how to use the New Logon dialog to add accounts for each application type.

The procedure is similar for each type. You identify the application and then provide your credentials—username/ID, password, and any other information the application requires you to enter.

If you attempt to add an account for a Windows application that is not configured in Logon Manager, you are asked to identify the username/ID and password fields by pointing and clicking on these fields.

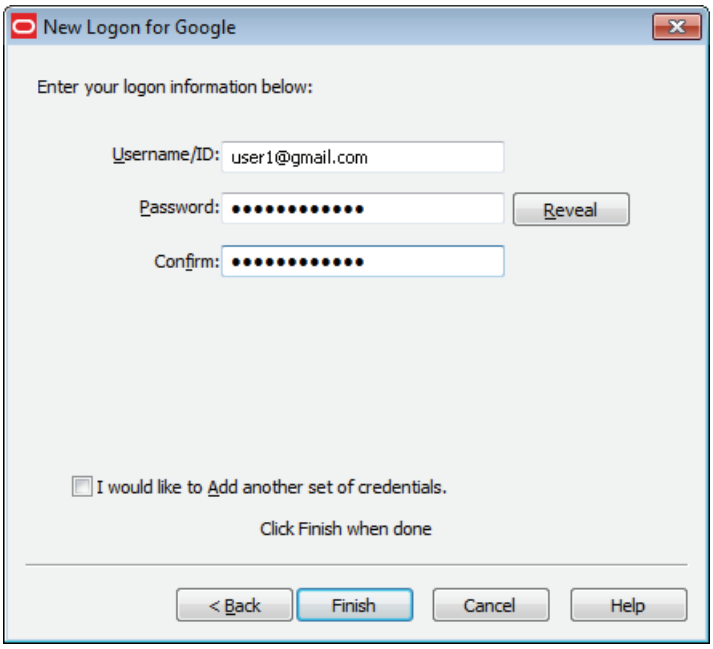
You are also given the option to create more than one account for a single application. This is useful for applications for which you have more than one set of credentials; for example, if you have multiple email accounts from one account.

When Logon Manager detects an application for which you have more than one account, it displays the Logon Chooser dialog, which lets you select the account to use.

2.4.2.1 Adding an Account for a Listed Windows Application

To add an account for a Windows application:

1. In the New Logon dialog, select the **Windows** option and select an application from the drop-down list box. If the application you want to add is not listed, see Adding an Account for an Unlisted Windows Application.
2. Click **Next**. The New Logon dialog appears, prompting you to enter credentials.



3. Enter your Username/ID for the application, enter your Password, and confirm it. You can display the password by clicking **Reveal**.

   Note: Depending on the requirements of the application you are setting up, you may be prompted for additional fields, such as Domain Name for Microsoft Outlook.

   Similarly, some applications may not require a username/ID. In such cases, the Username/ID box will be unavailable.

   If you are setting up an RSA SecurID application, you will be asked to enter your PIN and Software Token. Your PIN is set up through the RSA middleware. The Software Token field automatically populates as it detects the serial number of the available token.

4. Do one of the following:

   - Click **Finish**. Logon Manager returns you to the My Accounts panel, which now lists the account you have just created.

     or

   - If the setting is available, and you so choose, select **Add another set of credentials**, then click **Finish**. Logon Manager adds the account to the My Accounts panel and re-displays the New Logon dialog.

     Note: If you are adding a new account for an existing application that is part of a credential sharing group, select **Exclude from credential sharing group**. If this is the first account you have created for this application, leave this check box unselected. See Credential Sharing Groups for more information.

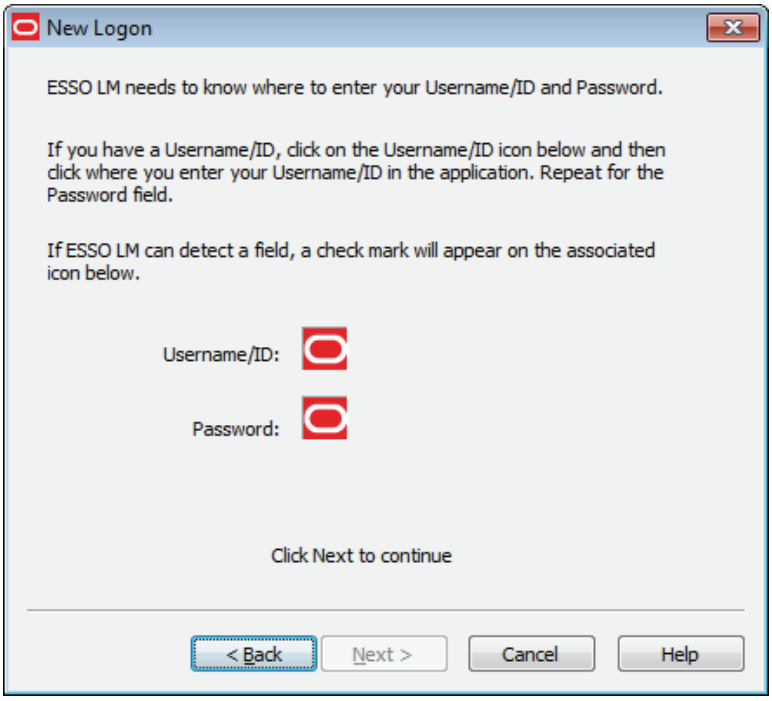
2.4.3 Adding an Account for an Unlisted Windows Application

Depending on your administrator's preference, you may be able to add logons for applications that aren't in your predefined applications list. The following describes this process.

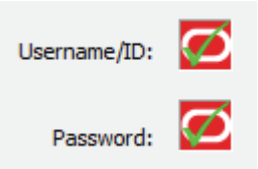
1. Open the Windows application for which you want to set up an account. This is the target application.

> **Note:** If the target application requires more than two fields for authentication, this procedure requires an administrator to create a template for it. Contact your administrator for assistance.

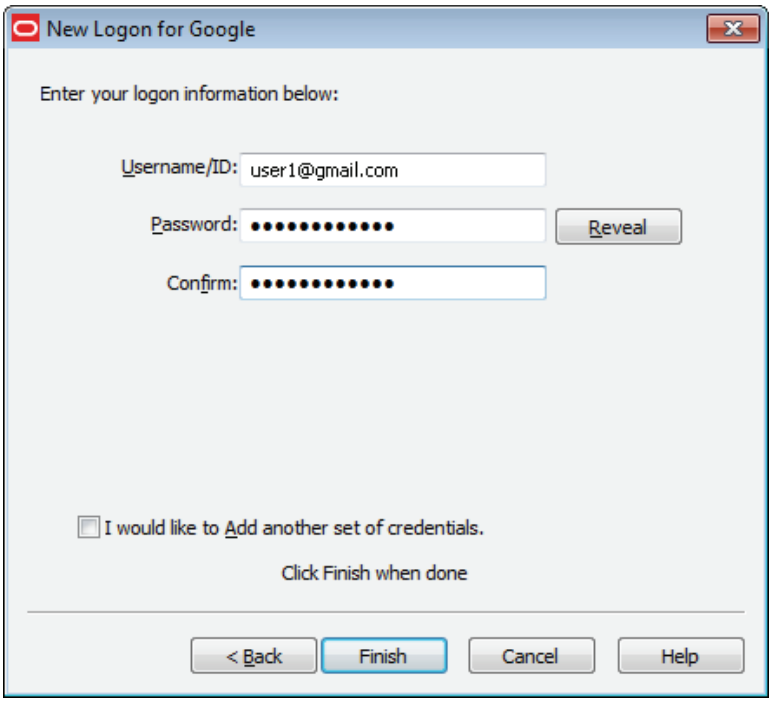
2. When the target application's logon dialog displays, switch back to Logon Manager. Arrange the windows so that both Logon Manager and the target application's logon dialog are visible.
3. In the New Logon dialog, select the **Windows** option and select **Application not in list** (the default) from the drop-down list box.
4. Enter the **Application Name** of the target application and (optionally) a **Description**.
5. Click **Next**.
6. The New Logon displays two icons.



7. Click the **Username/ID** icon, and click in the username or user ID field of the target application's logon dialog. A green check mark appears over the icon.
8. Click the **Password** icon, and click in the password field of the target application's logon dialog. A green check mark appears over the icon.



9. Click **Next**. The New Logon dialog appears, prompting you to enter credentials.



10. Enter your **Username/ID** for the application, and then your **Password**. Retype your password in the Confirm Password field. (You can display the password by clicking **Reveal**.)
11. Do one of the following:
    - Click **Finish**. Logon Manager returns you to the My Accounts panel, which now lists the account you have just created.

      or

    - If the setting is available and you so choose, select **Add another set of credentials**, to repeat the process. Then click **Finish**. Logon Manager adds the account to the My Accounts panel and re-displays the New Logon dialog.

Note: If you are setting up an RSA SecurID application, you will be asked to enter your PIN and Software Token. Your PIN is set up through the RSA middleware. The Software Token field automatically populates as it detects the serial number of the available token.

2.4.4 Adding an Account for a Web Site

1. In the New Logon dialog, select the **Web** option, then select a Web site from the drop-down list. If the Web site you want to add is not listed, see Adding an Account for an Unlisted Web Site.

2. Click **Next**. The New Logon dialog appears, prompting you to enter credentials.
3. Enter your **Username/ID** for the application, and then your **Password**. Retype your password in the Confirm Password field. (You can display the password by clicking **Reveal**.)
4. Do one of the following:
   - Click **Finish**. Logon Manager returns you to the My Accounts panel, which now lists the account you have just created.

     or
   - If the setting is available and you so choose, select **Add another set of credentials**, to repeat the process. Then click **Finish**. Logon Manager adds the account to the My Accounts panel and re-displays the New Logon dialog.

Note: If you are adding a new account for an existing application that is part of a credential sharing group, select **Exclude from credential sharing group**. If this is the first account you have created for this application, leave this check box unselected. See Accounts That Share Credentials for more information.

2.4.5 Adding an Account for an Unlisted Web Site

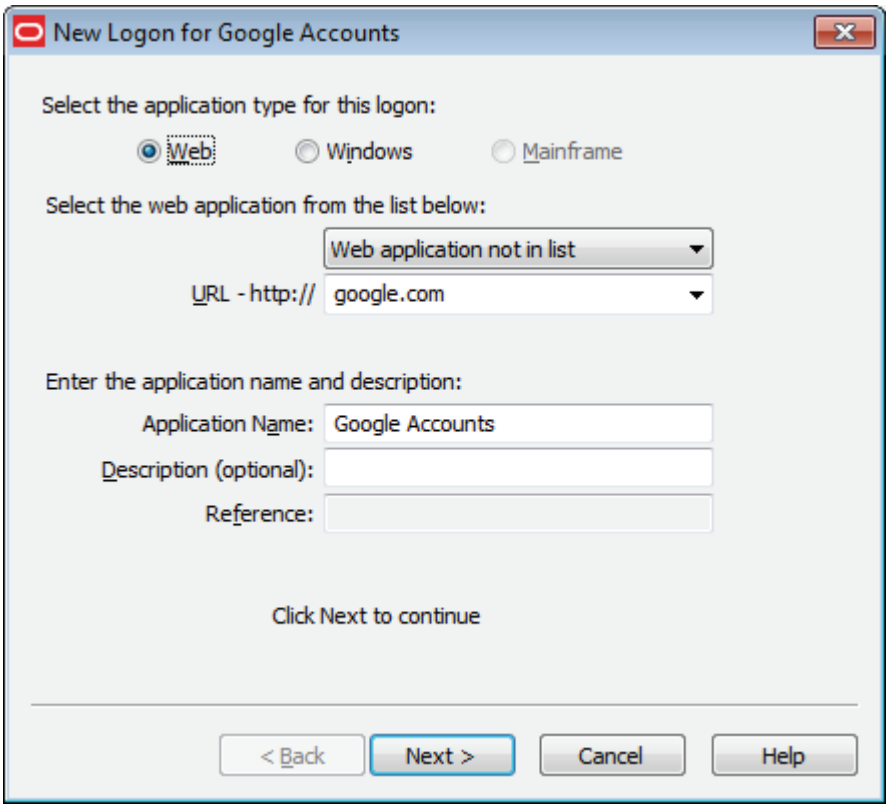
1. In the New Logon dialog, select the **Web** option. Select **Web application not in list** (the default option) from the drop-down list box. A text box for entering a Web address appears.

Note: If the target Web site requires more than two fields for authentication, this procedure requires administrator resources. Contact your administrator for assistance.

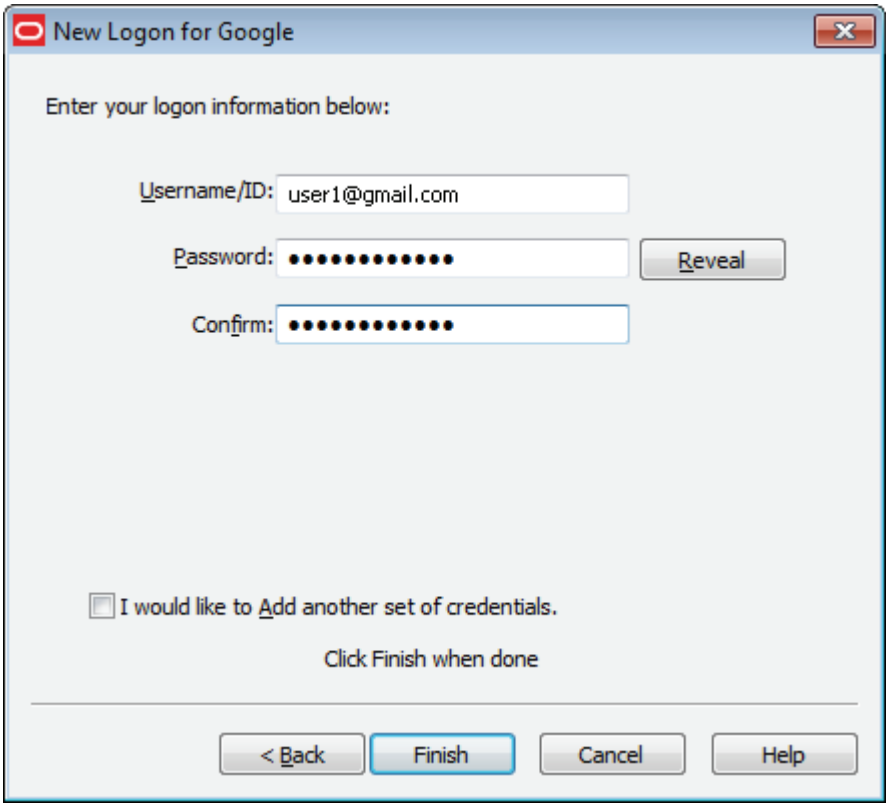
---

2. Enter the **URL** of the Web site for which you want to set up an account.

   Do not include the URL protocol, such as http:// or https:// in the URL.
3. Enter the **Application Name** and (optionally) a **Description**.
4. Click **Next**. The New Logon dialog appears, prompting you to enter credentials.

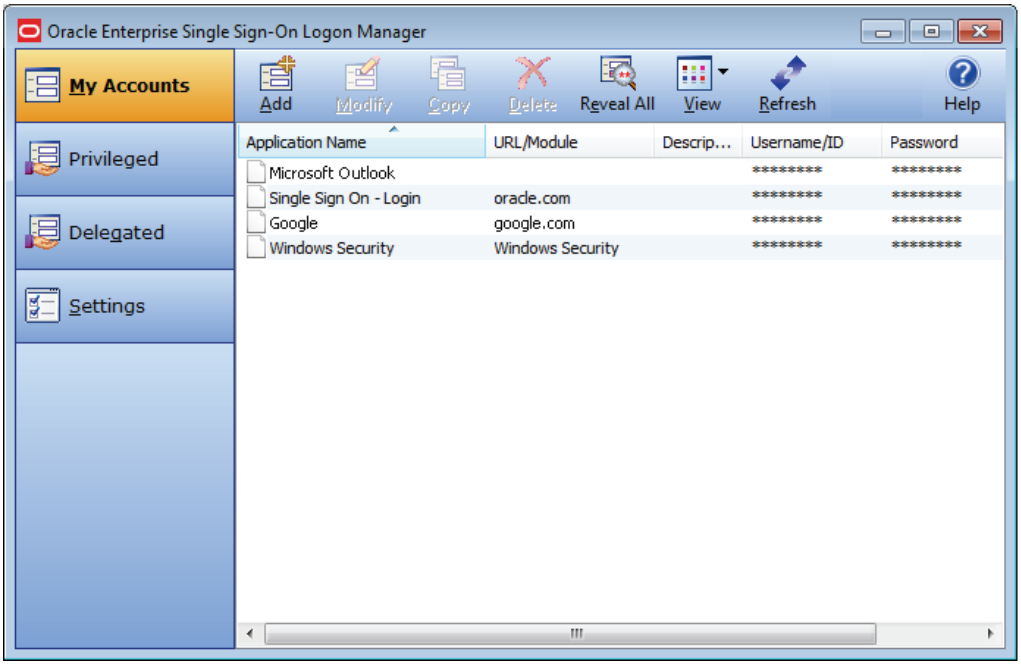


5. Enter your **Username/ID** for the application, and then your **Password**. Retype your password in the **Confirm Password** field. (You can display the password by clicking **Reveal**.)



6. Do one of the following:
   - Click **Finish**. Logon Manager returns you to the My Accounts panel, which now lists the account you've just created.

     or
   - If the setting is available and you so choose, select **Add another set of credentials**, to repeat the process. Then click **Finish**. Logon Manager adds the account to the My Accounts panel and re-displays the New Logon dialog.



2.4.6 Adding an Account for a Host/Mainframe Application

1. In the New Logon dialog, select the **Mainframe** option and select an application from the drop-down list box. Enter the target application in the Application Name field, and (optionally) a Description.
2. Click **Next**. The New Logon dialog appears, prompting you to enter credentials.
3. Enter your Username/ID for the application, and then your Password. Retype your password in the Confirm Password field. (You can display the password by clicking **Reveal**.)
4. Do one of the following:
   - Click **Finish**. Logon Manager returns you to the My Accounts panel, which now lists the account you've just created.

     or
   - If the setting is available and you so choose, select **Add another set of credentials**, to repeat the process. Then click **Finish**. Logon Manager adds the account to the My Accounts panel and re-displays the New Logon dialog.

2.4.7 Setting Up Accounts Using Auto-Prompt

To use the Auto-Prompt feature, it must be activated on the Response tab of the Settings panel.

1. Open Logon Manager.
2. Click the **Settings** panel, and select the **Response** tab.
3. Make sure that the Auto-Prompt check box is selected. If not, select it, then click **Submit**.

> **Note:** The Auto-Prompt feature is enabled by default upon installing Logon Manager. Your administrator might enable or disable Auto-Prompt for all users.

When Auto-Prompt is enabled, Logon Manager automatically detects when you have encountered a password-protected application or Web site. If you already provided credentials for that application or Web site, Logon Manager automatically enters your credentials in the appropriate fields and logs you on.

Example for an account for which you have already provided credentials:

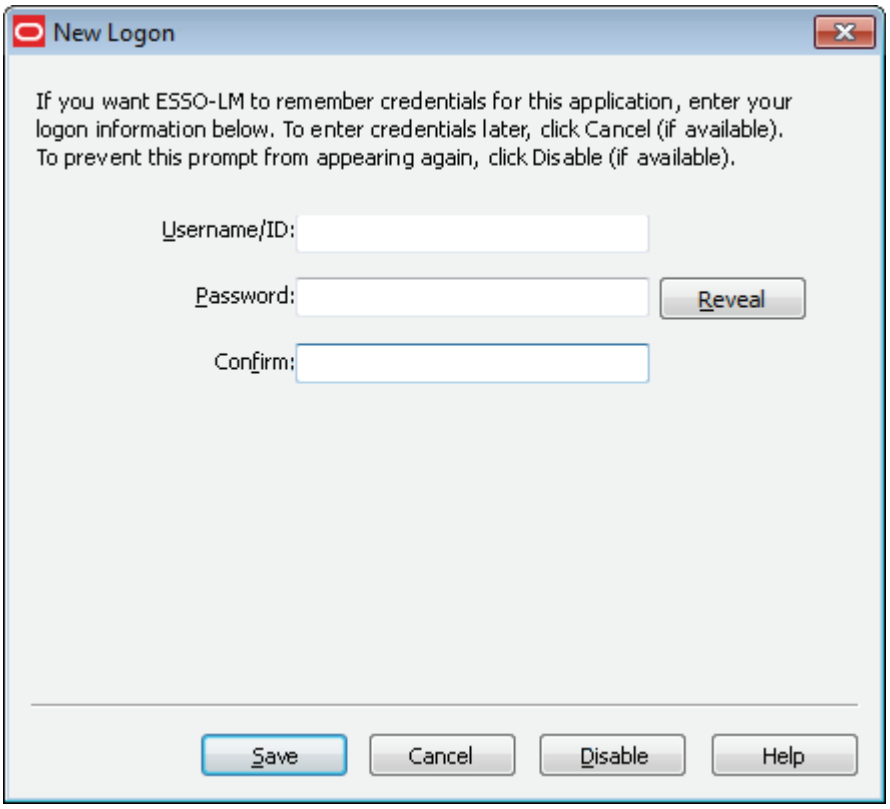
You launch Lotus Notes, an application for which you have already provided credentials. As soon as the program opens, Logon Manager recognizes this logon screen's request for credentials.

Logon Manager enters your password in the appropriate field and clicks the **OK** button, logging you on to Lotus Notes.

Example for an account for which you have not provided credentials:

By contrast, you launch an application or Web site for which you have not yet provided credentials.

When Logon Manager detects an application for which you have not previously stored credentials, it displays the New Logon dialog, prompting you to add account information for the application (unless your administrator has disabled the Auto-Prompt feature).



When presented with the New Logon dialog, do one of the following:

- If you want to add an account for the application, fill in the displayed fields and click **OK**. Logon Manager stores the information and automatically logs you on to this application whenever you launch it.
- If you want to defer adding an account for the application temporarily, click Cancel (if available). The next time you launch the application, Logon Manager prompts you to add an account.
- If you want to disable the new logon prompt for the detected application permanently, click Disable (if available). Logon Manager no longer prompts you to add an account for the application and adds it to the disabled application list on the Exclusions tab of the Settings panel.

> **Note:** If you choose to disable the application, you can re-enable it by selecting **Log On Using Logon Manager** from the Logon Manager tray icon.
>
> If you decide in the future that you want Logon Manager to prompt you for your credentials automatically the next time you launch the application, remove the application from the Exclusions list.

2.4.7.1 Credential Sharing Groups

Your administrator can create groups of accounts that use the same credentials, referred to as credential sharing groups. For the first account being added from the credential sharing group, the New Logon dialog, with empty fields, appears so that the user can enter credentials. Users from the group who create subsequent accounts receive the New Logon dialog with fields that are empty and editable, or

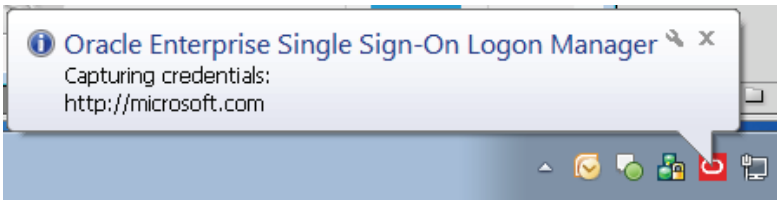
pre-populated and unavailable for editing, depending on your administrator's preferences.

If your administrator configures the credential sharing group so that members have the option to create an account outside the group, the New Logon dialog contains the setting, *Exclude account from credential sharing groups*. In that case, you have the ability to edit the shared credential fields with the information of your choice. Check **Exclude account from credential sharing groups** to make the shared fields available for editing.

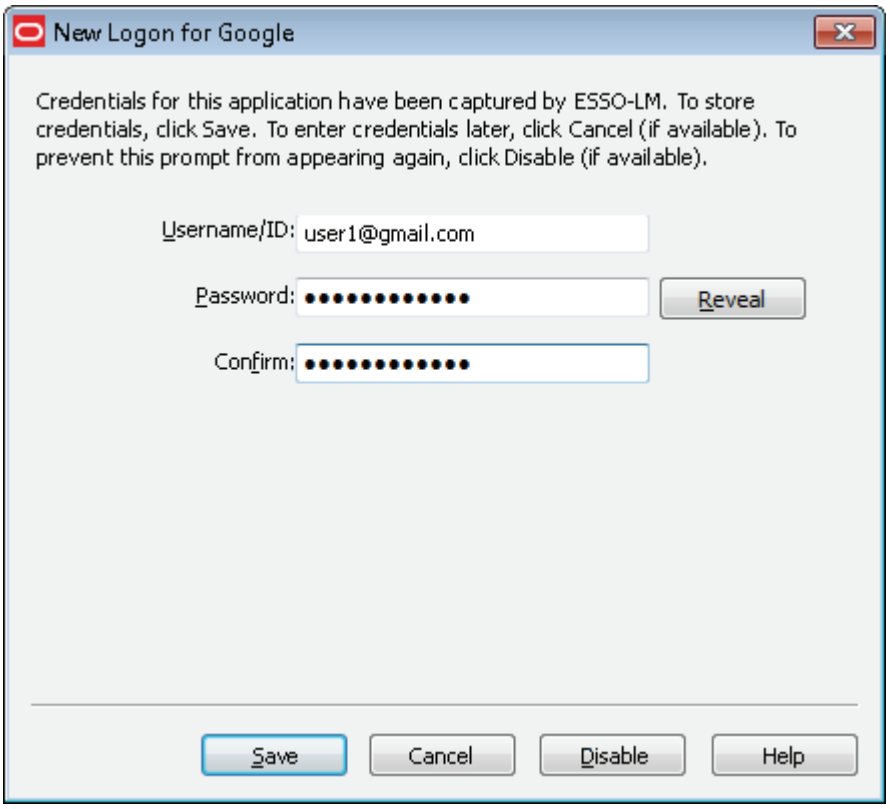
2.4.8 Automatic Credential Capture

Your administrator might configure applications to capture your credentials transparently. When you launch such an application, Logon Manager waits for you to enter credentials and captures them as you enter them. Depending on your administrator's configuration, when you finish entering credentials in this mode, one of the following occurs:

- Logon Manager captures your credentials without notifying you.
- A balloon tip appears in the system tray menu, notifying you that the credentials are being captured. You will not be required to verify them afterward.



- A balloon tip appears in the system tray menu, notifying you that the credentials are being captured, and then the New Logon dialog appears with fields already populated with your input. You can then verify that the information is correct, or edit it if necessary, and click **Save**.



If you previously added an application to the list on the Exclusions tab, or your administrator has excluded your user account from the application (see Exclusions Configured by the Administrator in the section, Managing Accounts, for more information), Logon Manager ignores the application. It does not capture any credentials that you add, and does not present the New Logon dialog or inform you that credentials have not been captured.

This feature is new as of version 11.1.1.5.0.

2.4.9 Modifying Accounts

You can modify account information or automatic behavior for individual accounts by clicking the **Modify** icon in the My Accounts view, or by double-clicking the account. From this dialog, you can:

- Change the **Username/ID**, **Password** or other fields that the account sends to the application.
- Edit the application information. Edit **Username/ID**, **Password**, **ApplicationName** and **Description**.
- Turn on or off the automatic response options for selected accounts.
- **Auto-Recognize.** This setting specifies whether Logon Manager should automatically provide credentials when an application requests them.

  When this feature is enabled, Logon Manager recognizes applications and Web sites and logs you on automatically.

  When this feature is not enabled, you must manually request that Logon Manager respond to the logon request. You can do this from the system tray icon menu. Select **Log On Using Logon Manager**.

The Auto-Recognize check box can have three different states:

- A blank checkmark means it is off for the selected application.
- A checkmark means it is on for the selected application.
- A green box means that the global setting defines the action for the selected application.

- **Auto-Submit.** This setting specifies whether Logon Manager should automatically submit the credentials to the application. For example, select **OK**, **Submit**, or **Enter** to initiate the logon.

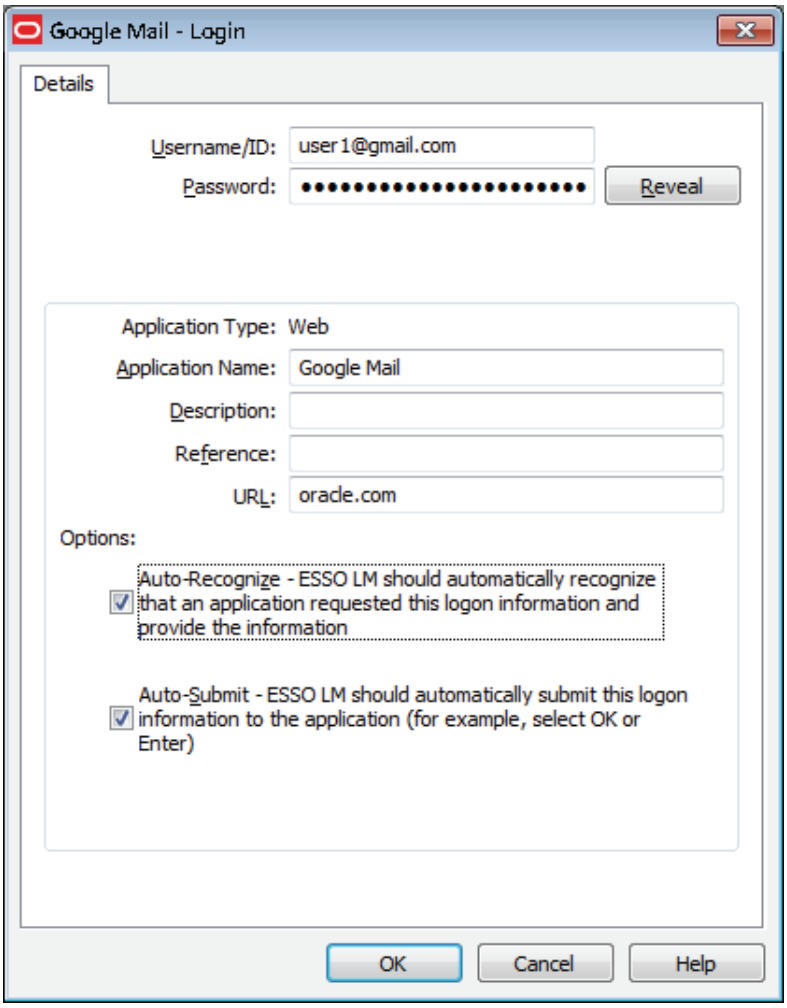
Note: Depending on your system configuration, the **Auto-Recognize** and **Auto-Submit** options may or may not be available.

To set Auto-Recognize globally for all applications, use the **Auto-Recognize** option in the Response tab of the Settings panel.

The setting in this dialog overrides the global **Auto-Recognize** setting.

2.4.9.1 Modifying an Account

1. Open Logon Manager.
2. On the **My Accounts** panel, select an account.
3. Highlight the account from the list, and either click the **Modify** icon or double-click the account. The modify dialog for the selected account appears.



Note: If the account is displayed in gray text, this message appears when you click **Modify**: "Credential corresponds to an application that is not currently configured in Logon Manager." See Accounts Without Configured Credentials for more information.

4. Modify the information as needed.
5. When you have completed your changes, click **OK**.

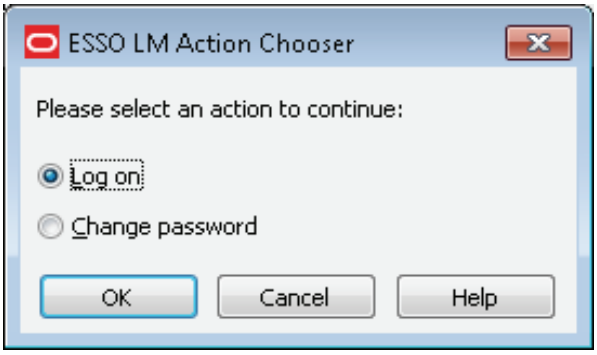
2.4.10 Special Logon Situations

After you have created accounts, and in the course of daily activities, there might be occasions when Logon Manager encounters an application for which it can respond in more than one way, or for which it needs additional information from you. When this happens, one of the following dialogs appears.

- Action Chooser
- Logon Chooser
- Retry Logon
- Logon Loop

2.4.10.1 Using the Action Chooser

When Logon Manager detects an application that displays its logon and password change fields in the same window, the Action Chooser dialog prompts you to choose whether you want to log on to the application or change your password for the application.



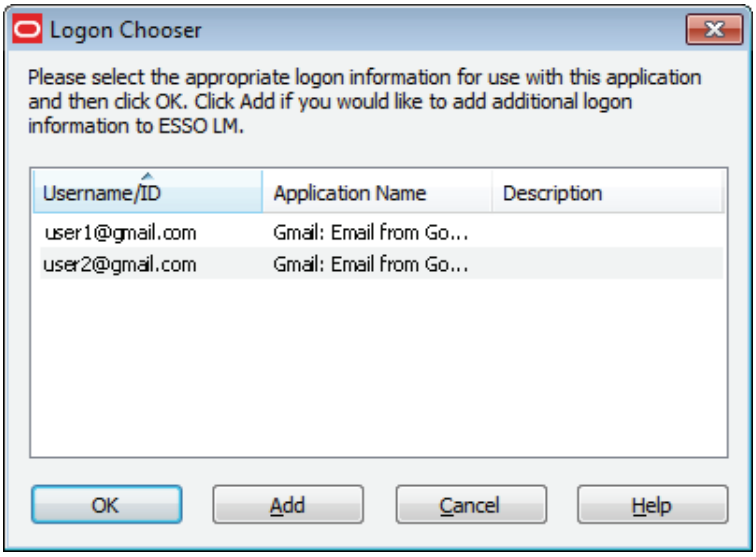
To choose the desired action:

1. Select the action.
2. Click **OK**.

2.4.10.2 Using the Logon Chooser

You might have two or more different credential sets for the same application. If so, you can set Logon Manager to recognize those accounts and prompt you to choose which one to log on with.

When you open the application or Web site, the Logon Chooser prompts you to select the account you want to use.



All columns can be sorted by clicking on the column name heading. Once a sort order is selected, the order is retained and the same column is sorted the next time this dialog appears.

Do one of the following:

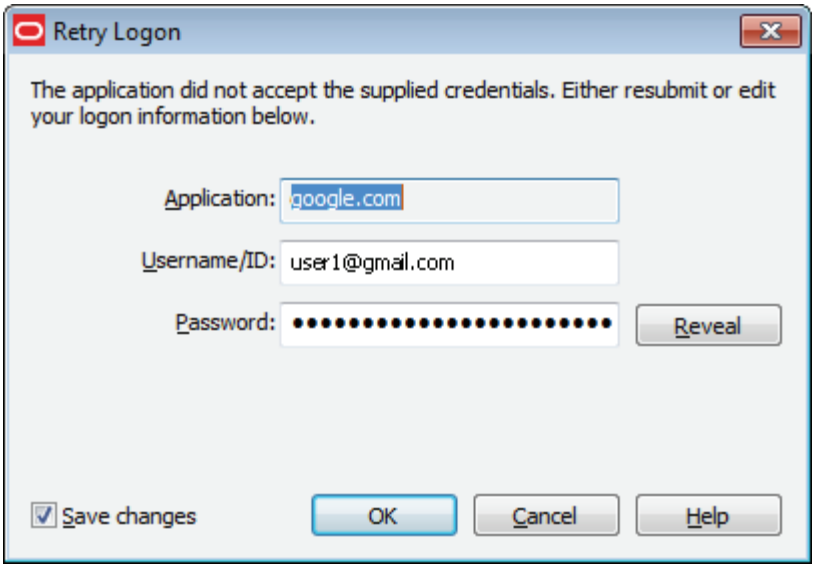
- Select the account you want to log on with and click **OK**.

- Click **Add** to add another account for this application.
- Click **Cancel** to close this dialog. Logon Manager will not log you on to the application.

2.4.10.3 Retry Logon Dialog

When you enable the Auto-Recognize function, Logon Manager automatically detects and responds to logon and password-change requests from applications and Web sites.

If you entered the wrong password when you set up the account, or perhaps changed the application's password from another workstation, Logon Manager will supply an incorrect password. When this happens, the application repeats the logon request and Logon Manager displays the Retry Logon dialog, prompting you to review the accuracy of your Username/ID, Password, and, if necessary, any additional logon fields.



The Retry Logon dialog box appears if you entered the wrong password, or if the password was changed from another computer. This dialog prompts you to review the accuracy of your Username/ID, Password, and, if necessary, any additional logon fields.

Do one of the following:

- Reveal the password you've entered by clicking **Reveal**.
- Edit your account information as needed and click **OK** to try logging on again.

> **Note:** The **Save Changes** check box ensures that Logon Manager uses the same credentials the next time it logs you on to this application or Web site. Uncheck this option if you do not want the new credentials you entered to be saved for future use.

- Click **Cancel** to stop any further logon attempts for the application or Web site until you either restart or modify the account in Logon Manager.

2.4.10.4 Logon Loop

Some applications, such as Web mail services, display their logon page upon logout, which causes Logon Manager to recognize the logon form and automatically log you back on to the application. This creates an endless "logon loop," preventing you from logging out of the application. To prevent this loop from occurring, the administrator can choose to enable the logon grace period feature, which forbids Logon Manager from logging on to an application within a set time period since the last logon.

Your administrator may also configure Logon Manager to ask whether you want to log on to an application again when you log out. In either case, Logon Manager will not automatically log you on to the application until the grace period expires or until you close and reopen the application, whichever happens first.

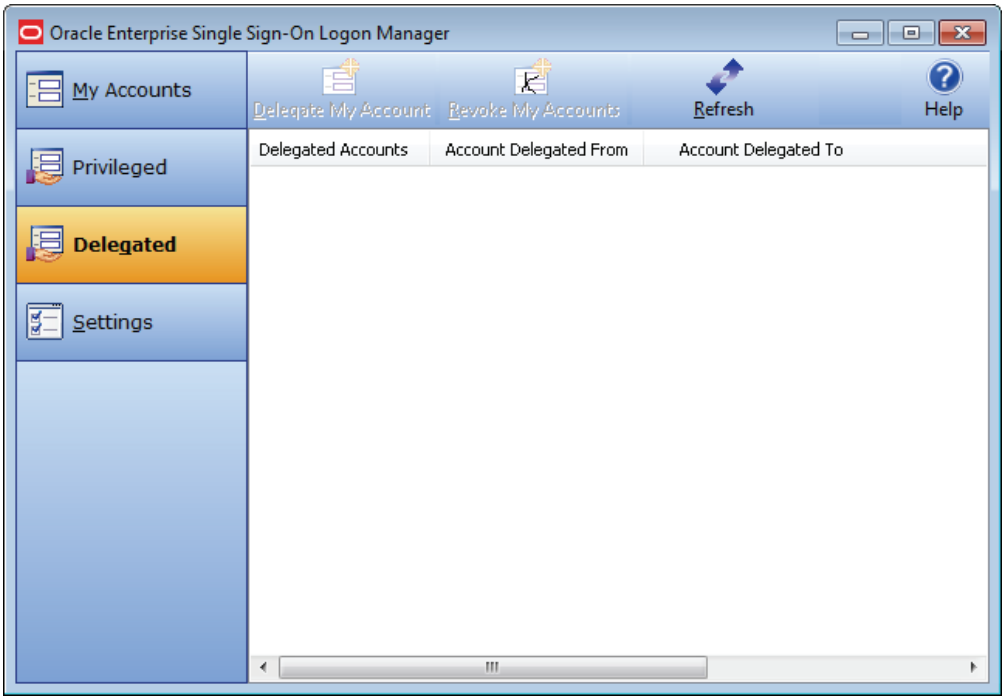
If you are experiencing logon loops, contact your administrator about enabling the grace period feature.

2.4.11 Delegating Your Account Credentials to Another User

Delegating account credentials provide a means for one user to give another user temporary access to his application credentials. Situations where this typically happens would be if you are going to be out of the office for vacation, or you have recruited a colleague to help you meet a tight deadline. In instances such as these, you would need someone other than yourself to be able to access your applications and data on your behalf. Your administrator can configure applications so that you have the ability to assign and receive access to another user's accounts within Logon Manager, using the Delegated Credentials feature.

2.4.11.1 Delegated Credentials in Logon Manager

When your configuration includes the ability to delegate and receive credentials, you will see a Delegated option in the left pane of Logon Manager.



The Delegated settings allow you to view and manage incoming and outgoing delegated accounts. If an account has been delegated to you, the Account Delegated

From column lists the delegator. If you have delegated an account to another user, the Account Delegated To column lists the delegatee.

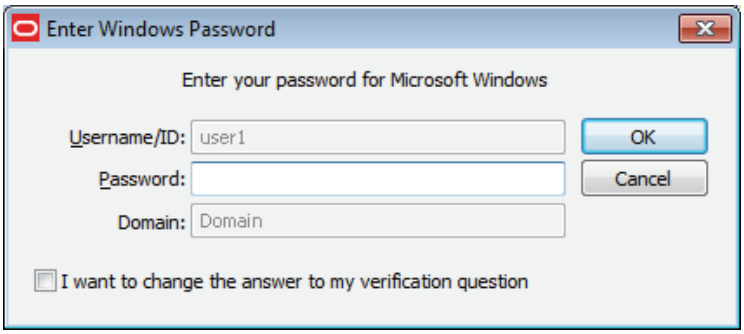
Use the icons across the top of the Delegated Accounts menu to delegate and revoke credentials.

Icon	Label	Purpose
	Delegate My Account	Initiates the account delegation process. You will be prompted to designate another user to receive your account credentials and specify the conditions for the account access. After you delegate an account, it appears in the Delegated Accounts column.
	Revoke My Account	Allows you to discontinue another user's access to your accounts. This icon is only enabled if the selected account was delegated.
	Refresh	Synchronizes delegated account changes with the repository. Synchronization occurs automatically when the delegator initiates or revokes a delegation.

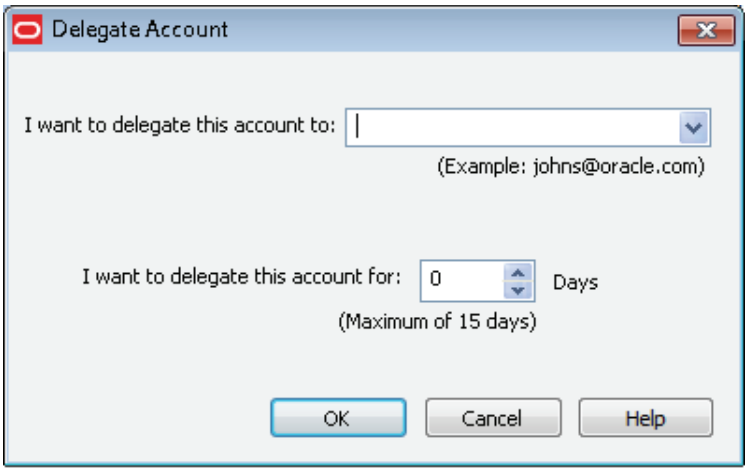
2.4.11.2 Delegating an Account to Another User

To delegate an account:

1. In the Delegated view of Logon Manager, select the account that you want to delegate.
2. Click the **Delegate My Account** icon.
3. Enter your password at the prompt.

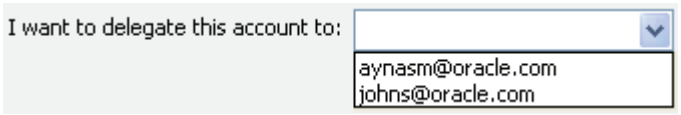


4. In the dialog that appears, specify the delegatee and configure a delegation policy.

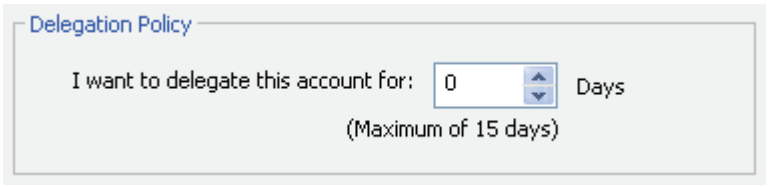


- To specify the delegatee:
  - Enter the delegatee's username (typically the user's email address).

    or
  - Select a user from the user history dropdown list (a list of users to whom you have delegated credentials in the past).

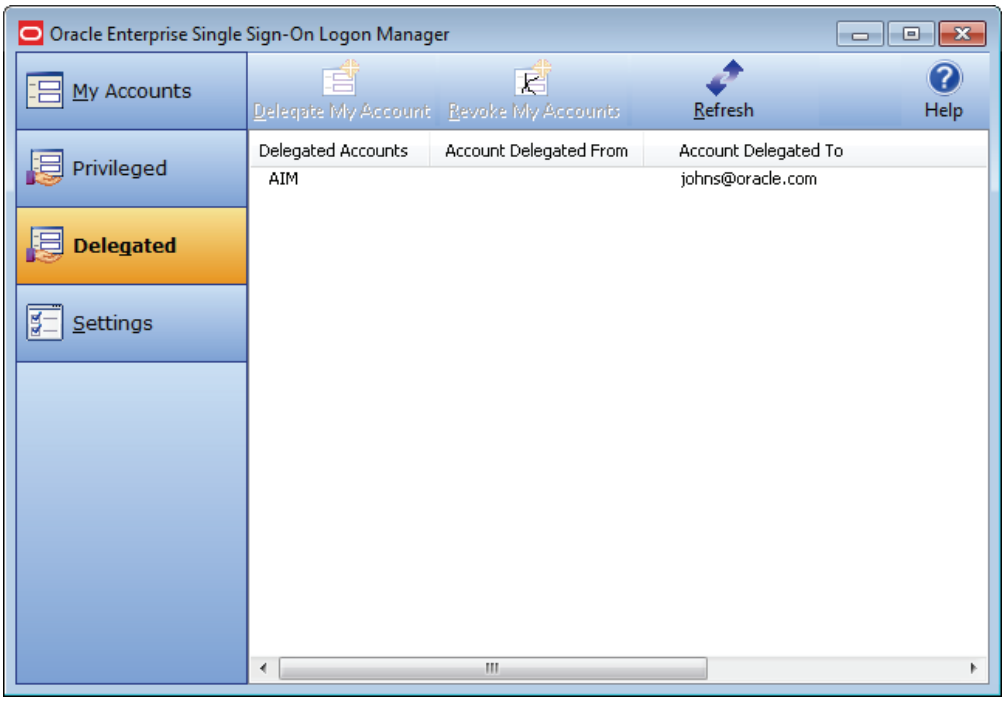


- To configure the policy, set the number of days that the delegatee can use this account. The maximum number of days appearing below this setting reflects what the administrator has set in the template policy.



5. Click **OK**.

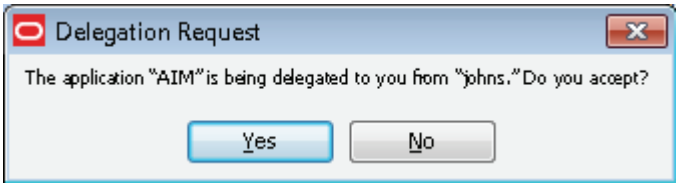
   The account is delegated and the server receives an instruction to delegate the credential. After you complete the delegation process, the account appears on the Delegated tab in your Delegated Accounts list.



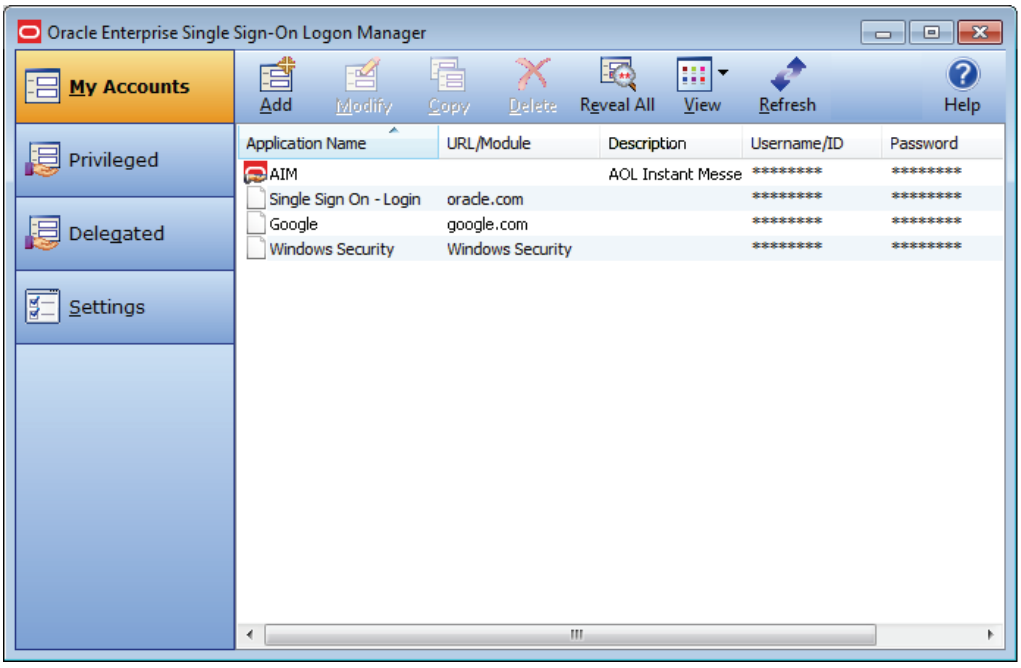
2.4.11.3 Receiving a Delegated Account from Another User

When another user delegates an account to you, you will be prompted to enter your Windows password.

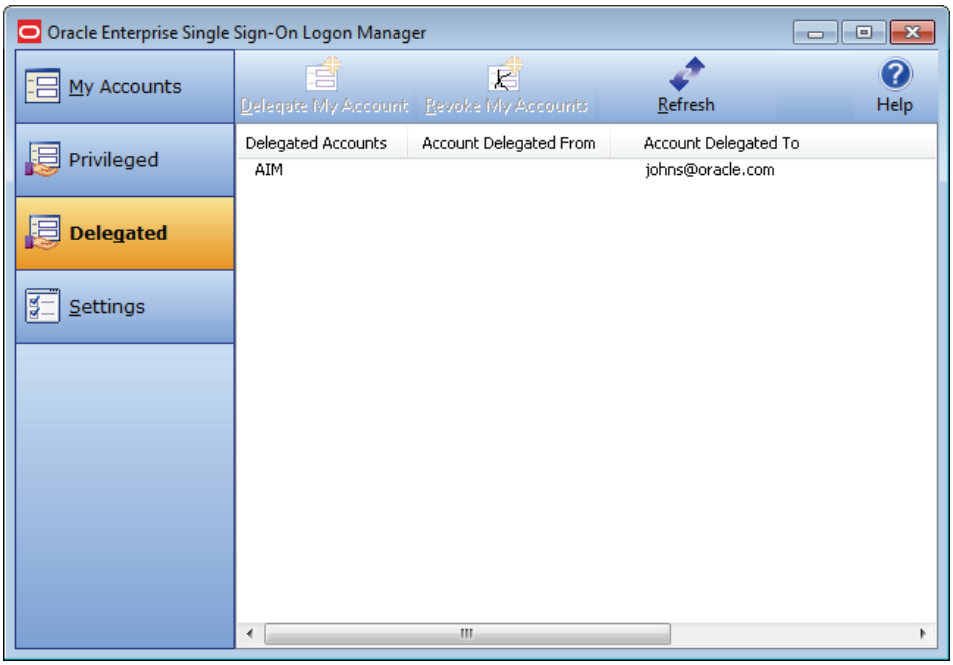
After you authenticate, a prompt appears, asking you whether you accept the delegation.



When you confirm your acceptance, the delegated account appears in the My Accounts tab of Logon Manager, with a special icon indicating that it is delegated to you.

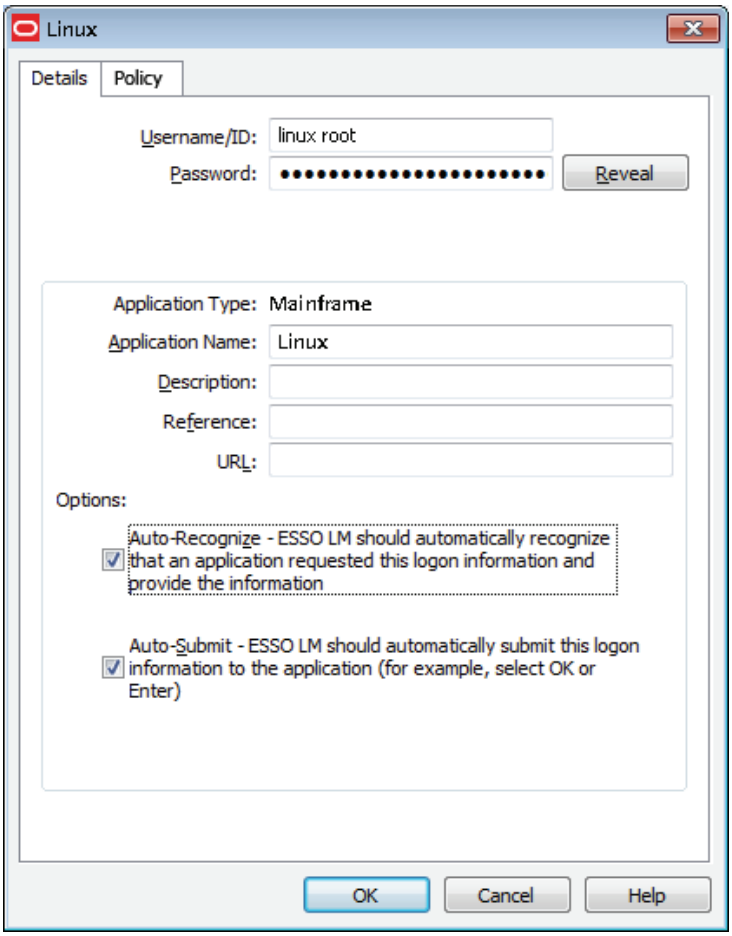


The account also appears in the Delegated Accounts column of the Delegated tab, with the name of the user who has delegated the account to you.

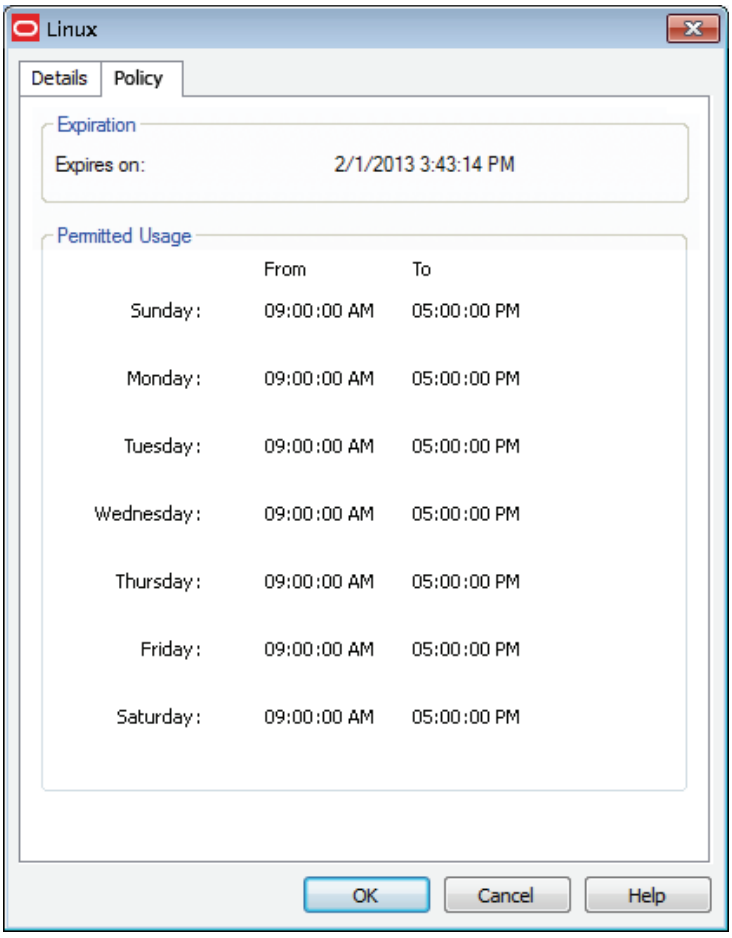


2.4.11.4 Viewing Delegated Account Properties

To view the properties of an account that has been delegated to you, select the account in Logon Manager, and select the **Modify** icon. The account's Properties window appears. The Details tabs lists general information about the account that you typically see in this dialog. Additionally, there is a Policy tab for a delegated account.



Select the **Policy** tab to view the delegation policy's properties: the date and time that the delegation expires, and the days and hours during which you can use the account.



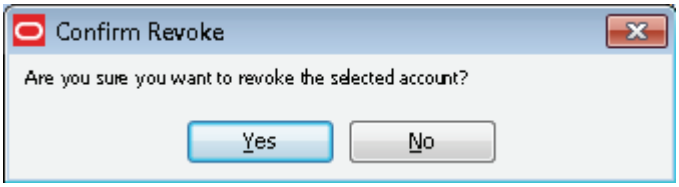
2.4.11.5 Updating Delegated Credentials

You can change the policy of a delegated account by repeating the original delegation process. In order to apply a policy update to an existing delegatee, you must revoke the account and redelegate it.

2.4.11.6 Revoking Delegated Credentials

To revoke credentials prior to the expiration date and time set in the policy:

1. On the Delegated tab, select the account whose credential you want to revoke.
2. Click the **Revoke My Account** icon.
3. Enter your password in the authentication dialog.
4. When prompted with the Confirm Revoke dialog, click **Yes**.



The delegatee's name no longer appears next to that account in the Delegated tab.

If you are the delegatee, when the delegator revokes the account, you will receive a prompt to authenticate. After you enter your credentials, the account no longer appears in your list of delegated accounts.

2.4.12 Working with Privileged Accounts

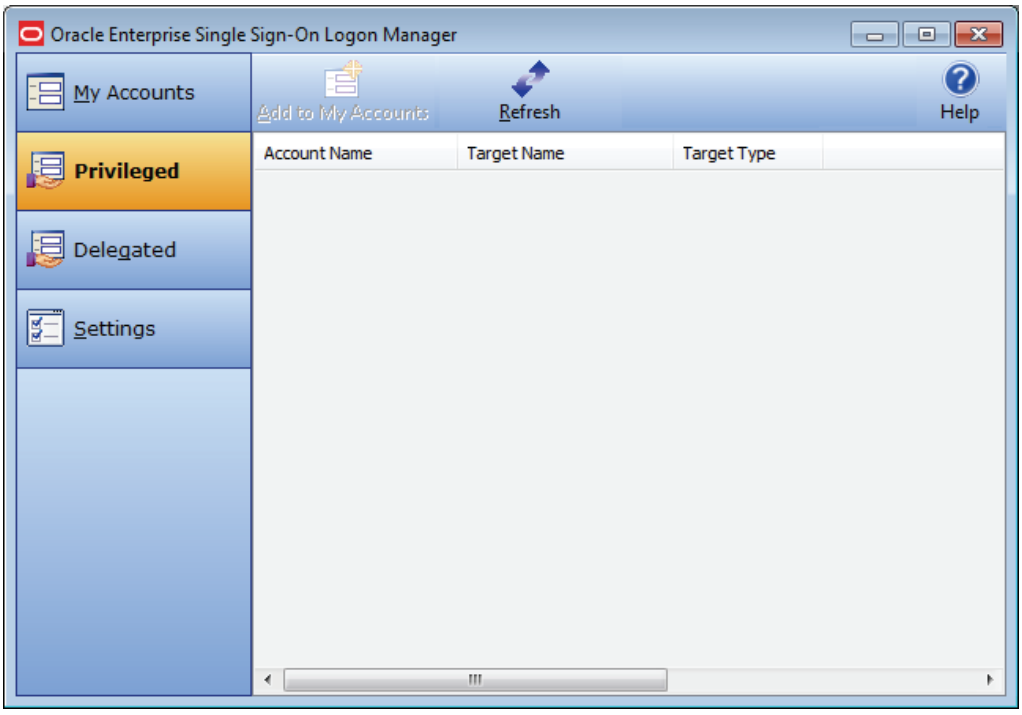
Privileged accounts apply to users responsible for key Information Technology resources, such as servers and databases. When you have been assigned the use of a privileged account, that account appears in the **Privileged** tab of Logon Manager.

In order for you to use a privileged account, an administrator of the account must have authorized your access to the account, the account must be available for checkout, and the checkout must be within the timeframe during which you are authorized to do so.

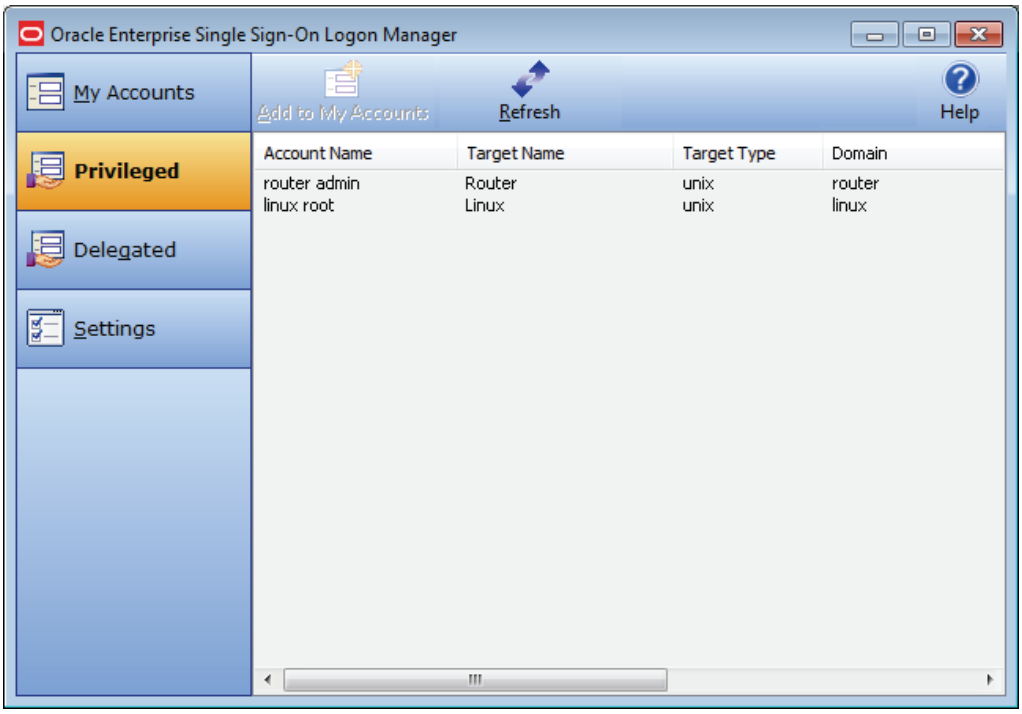
2.4.12.1 Displaying and Using Privileged Accounts

To display your privileged accounts:

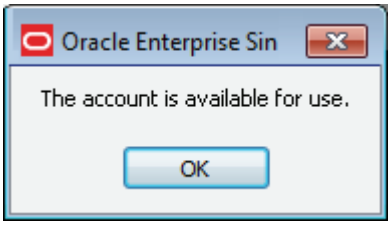
1. Open Logon Manager and select the **Privileged** tab.



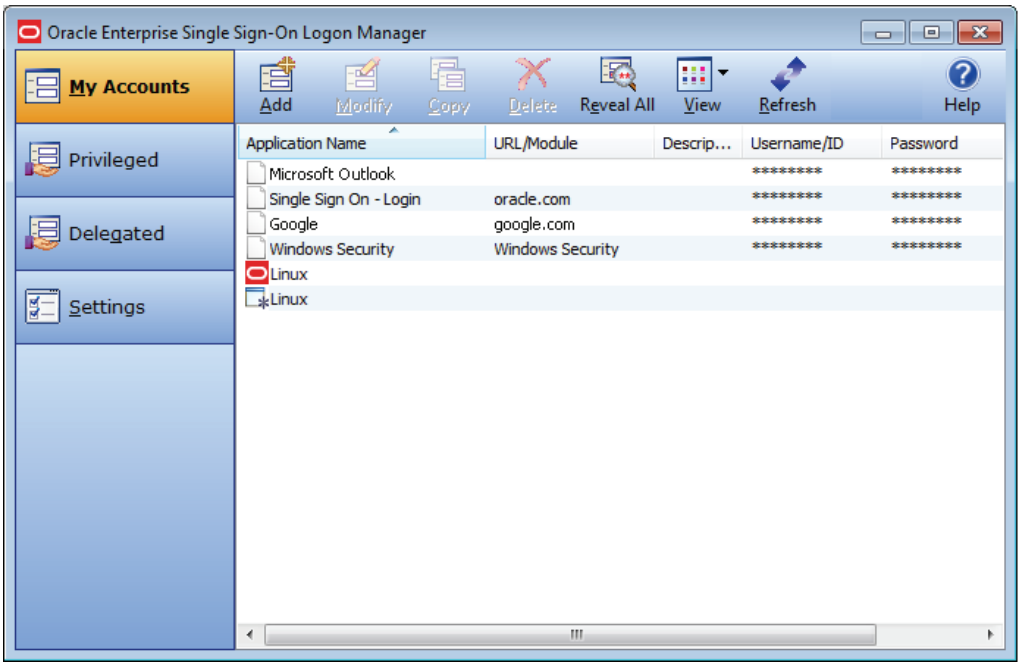
2. Click **Refresh** and fill in the fields in the **Authentication** dialog that appears. When the screen refreshes, you will see a list of all available privileged accounts assigned to you.



3. From the list, select the privileged account you want to work with, and click **Add to My Accounts**. You will be prompted to reauthenticate. After a moment, a popup message informs you that the account is available for use.



It now appears in the **My Accounts** window with a special icon indicating its status.



Note: If you have previously checked out this account and the checkout is still in effect, you will receive a message that the account is already checked out when you attempt to check it out again.

4. Proceed to log on to the account. Depending on how your administrator has configured the account, you might be required to provide your Windows password before Logon Manager authenticates you.

After you have checked out the account and for the duration of your permission to access it, you can work with it as you would any other account in Logon Manager.

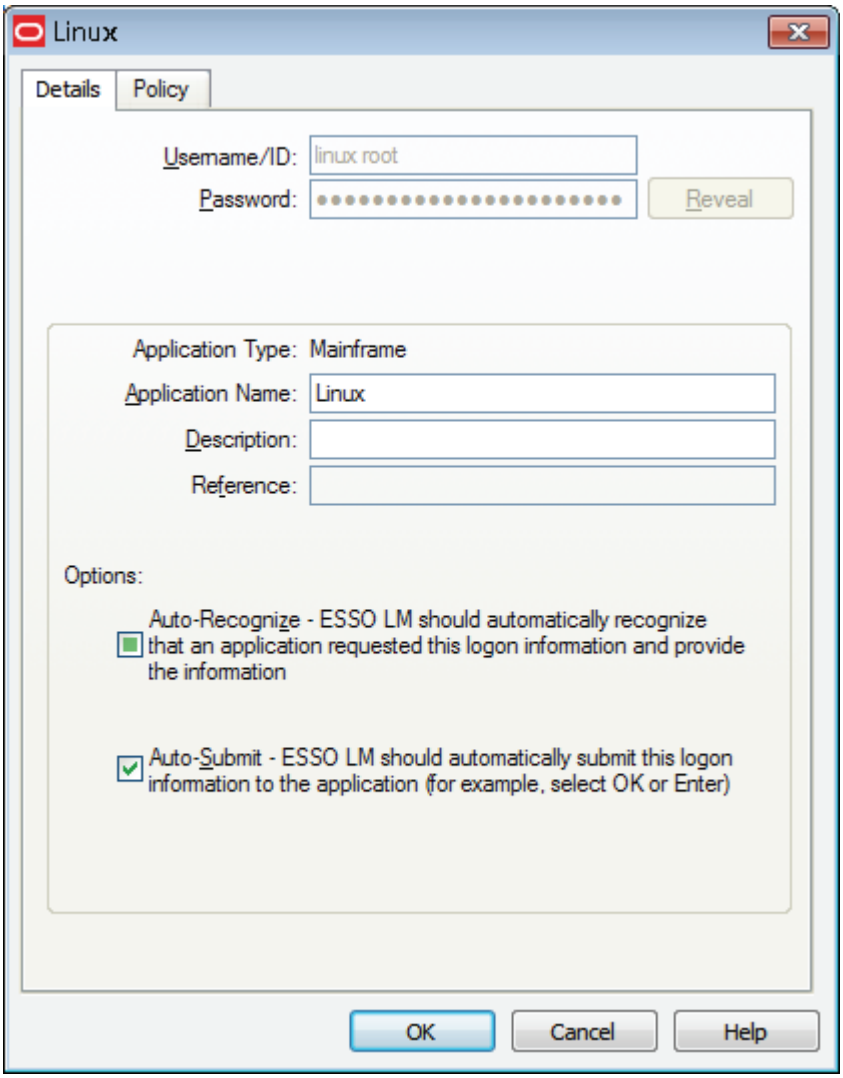
2.4.12.2 If an Account Is Unavailable

If you attempt to check out an account that is unavailable for any reason, you will receive a popup message informing you of the reason why you cannot check out the account. The account might not be available for one of the following reasons:

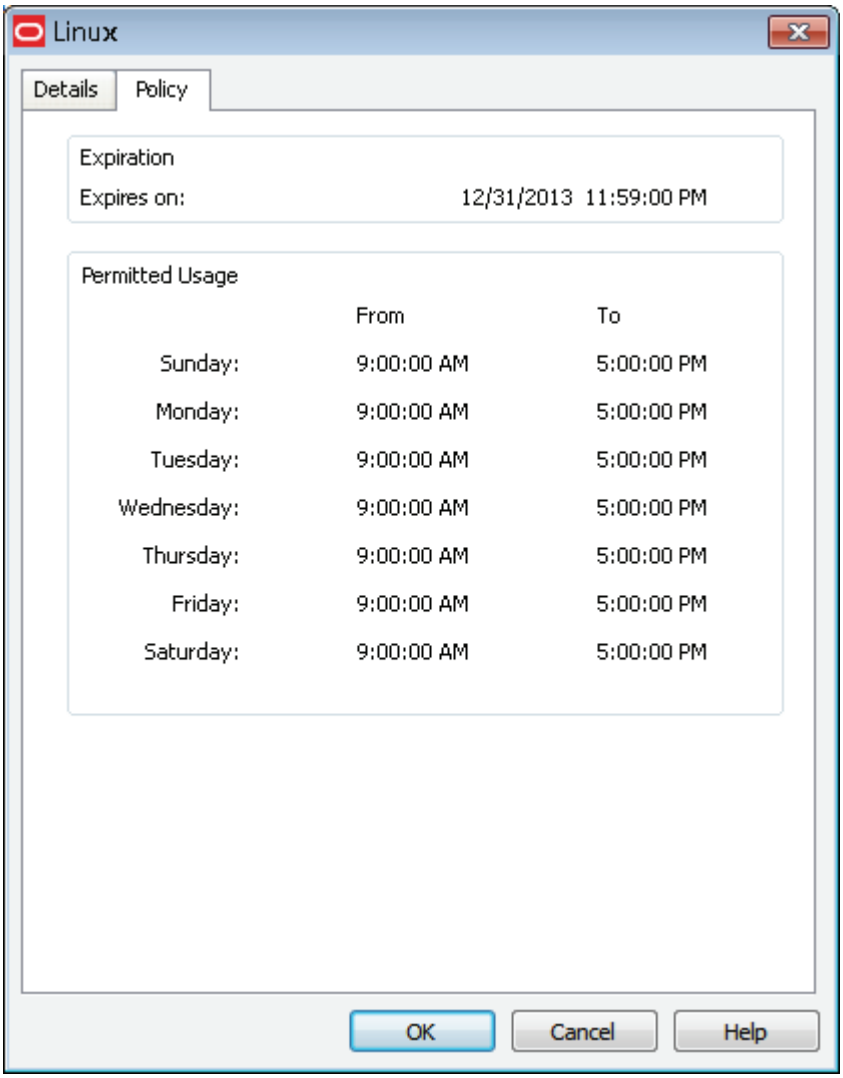
- Your attempt occurs outside of the policy's schedule. Review the account's properties to verify that you are working within the permitted schedule.
- The Provisioning Gateway server might be unavailable. Contact your administrator for help.
- An unspecified system error has occurred. Contact your administrator for help.

2.4.12.3 Viewing Privileged Account Properties

To view the properties of a privileged account, select the account in Logon Manager, and select the **Modify** icon. The account's **Properties** window appears. The **Details** tabs lists general information about the account that you typically see in this dialog. Additionally, there is a **Policy** tab for a provisioned account.



Select the **Policy** tab to view the privileged account's policy properties: the date and time that the account expires, and the days and hours during which you can use the account.



2.4.12.4 Checking In a Privileged Account

Privileged accounts can be checked in manually in Logon Manager, due to expiration as per the account policy settings, or outside of Logon Manager, by you or the policy administrator.

To check in a privileged account in Logon Manager:

1. Click the **My Accounts** tab in Logon Manager.
2. Select the privileged account you want to check in.
3. Click the **Delete** icon, and confirm the deletion when prompted.

2.5 Settings

The Settings panel in the Logon Manager lets you control Logon Manager configuration options.

Note: Throughout the settings tabs, the Apply and Cancel buttons are unavailable until you make a change. After a change is made, you can implement the changes by clicking **Apply**, or discard the changes by clicking **Cancel**.

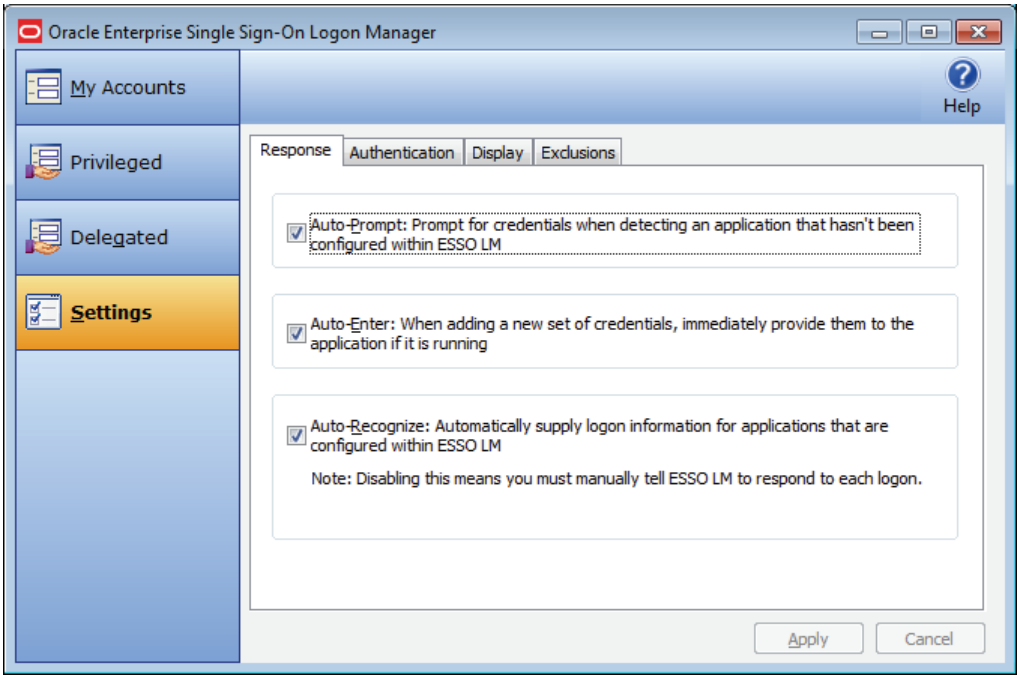
Changes made on the settings tabs take effect after you click **Apply**.

To view or modify Logon Manager settings:

1. Open Logon Manager.
2. Click the **Settings** panel.
3. The following tabs are available:
   - Response
   - Authentication
   - Display
   - Exclusions

2.5.1 Response Tab Settings

The Response tab lets you control Logon Manager account features.



Note: Your administrator may enable, disable or override any of the settings described below.

2.5.1.1 Auto-Prompt

The Auto-Prompt setting specifies whether Logon Manager should prompt for credentials when it detects a credential request from an application that does not have an account set up in Logon Manager.

See Setting Up Accounts Using Auto-Prompt for more information.

2.5.1.2 Auto-Enter

The Auto-Enter setting specifies whether Logon Manager should attempt to provide credentials to an application immediately after you create the account.

When this feature is enabled, Logon Manager immediately logs on to an application or Web site once you have set up an account for that application or Web site.

2.5.1.3 Auto-Recognize

The Auto-Recognize setting specifies whether Logon Manager should automatically provide credentials when an application requests them.

When this feature is enabled, Logon Manager recognizes applications and Web sites and logs you on automatically.

When this feature is not enabled, you must manually request Logon Manager to respond to the logon request. You can do this from the system tray icon menu. Select **Log On Using Logon Manager**.

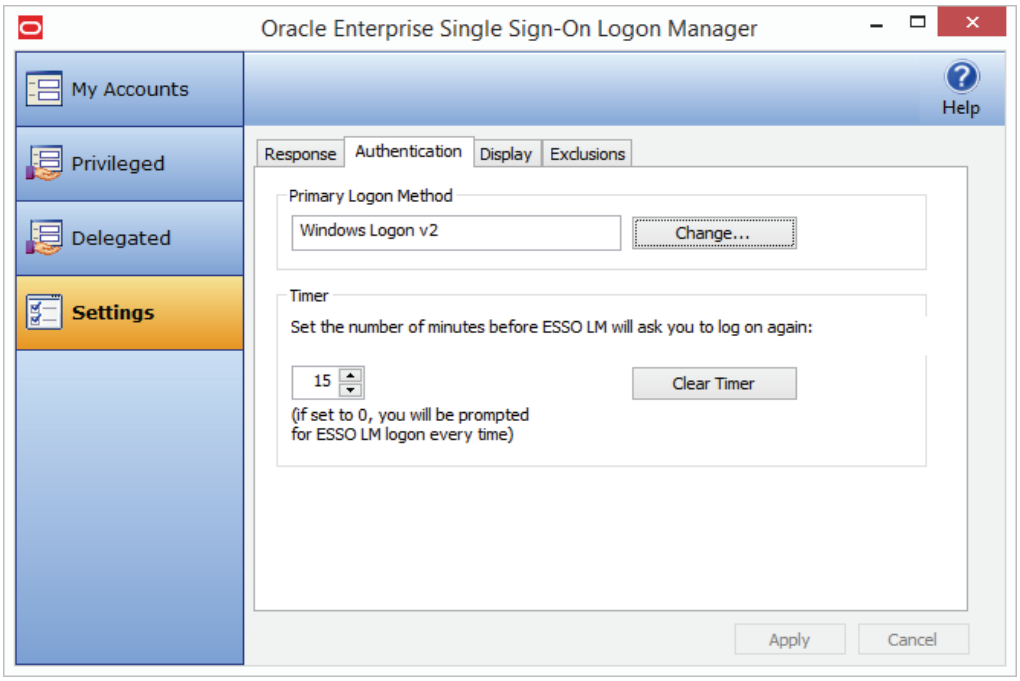
2.5.1.4 Viewing or Modifying Response Settings

1. Open Logon Manager.
2. On the Settings panel, click the **Response** tab.
3. When you have completed your changes, do one of the following:
   - Click **Apply** to confirm your changes (without closing Logon Manager), then select another settings tab.

     or
   - Click **Cancel** to discard your changes.

2.5.2 Authentication Tab Settings

The Authentication tab lets you control Logon Manager authentication features.



Note: Your administrator may enable, disable or override any of the settings described below.

2.5.2.1 Primary Logon Method

You can authenticate to Logon Manager through various logon methods. The Primary Logon Method is the authentication method you select to use. You can have multiple installed authenticators but can only have one Primary Logon Method.

This setting gives you the ability to choose which logon method will be the primary authentication mechanism.

To change your logon method, click **Change**. The Primary Logon Setup Wizard displays.

See Changing Your Primary Logon Method for more information.

2.5.2.2 Timer

Logon Manager can prompt you to authenticate at a specified time interval. You can determine the length of time before authenticating again.

Use the up and down arrows to enter a time limit (between 0 and 999 minutes); after this interval, Logon Manager asks for your password before performing any credential-related task.

If the timer setting is set to zero, Logon Manager asks for your password before every credential-related task.

The Clear Timer button forces you to enter your password upon your next credential-related task, without waiting for the expiration time.

2.5.2.3 Viewing or Modifying Authentication Settings

1. Open Logon Manager.

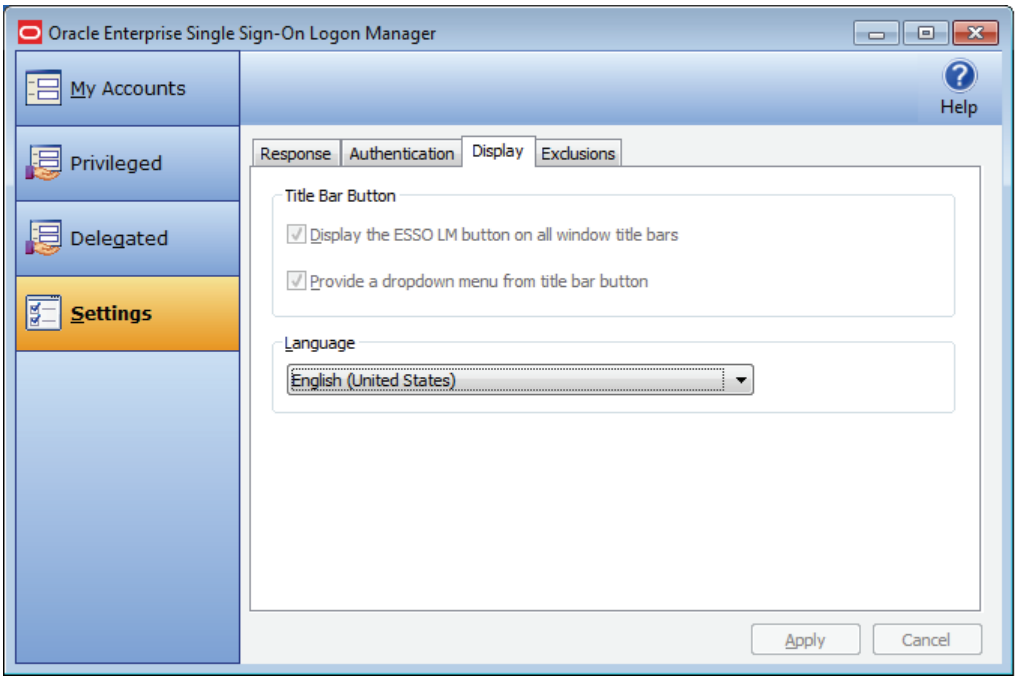
2. On the Settings panel, click the **Authentication** tab.
3. When you have completed your changes, do one of the following:
   - Click **Apply** to confirm your changes (without closing Logon Manager), then select another settings tab.

     or

   - Click **Cancel** to discard your changes.

2.5.3 Display Tab Settings

The Display tab of the Settings panel lets you control Logon Manager display options.



Note: Your administrator may enable, disable or override any of the settings described below.

2.5.3.1 Title Bar Button and Dropdown Menu

When checked, the Title Bar Button setting activates a Logon Manager icon in the upper-right corner of all window title bars.

When double-clicked, this button tells Logon Manager to attempt to log on to the application (same functionality as the Log On Using option in the System Tray Icon menu).

You also have the option to display a dropdown menu when you click the Logon Manager Title Bar Button.

These two settings can be enabled via the checkboxes labeled *Display the Logon Manager button on all window title bars*, and *Provide a dropdown menu from title bar button*.

2.5.3.2 Language

Logon Manager can run in many different languages, depending on which version you are running, and which language packs are installed.

You can view the languages that are available in the Language dropdown.

Choose the desired language for Logon Manager. All Logon Manager dialogs and help screens will display in the selected language.

2.5.3.3 Viewing or Modifying Display Settings

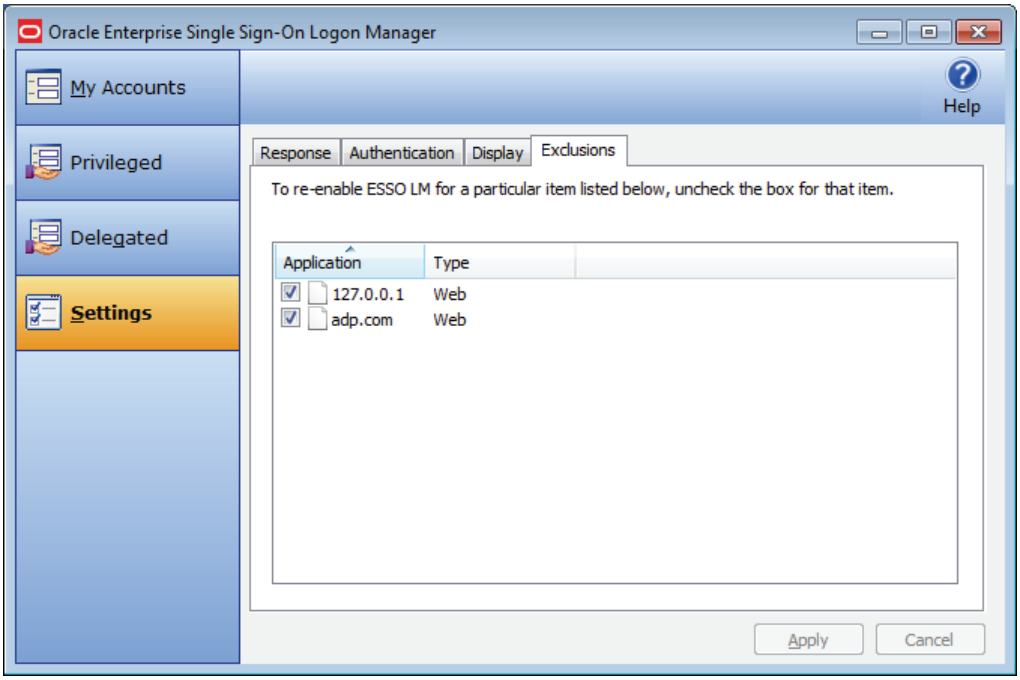
1. Open Logon Manager.
2. On the Settings panel, click the **Display** tab.
3. When you have completed your changes, do one of the following:
   - Click **Apply** to confirm your changes (without closing Logon Manager), then select another settings tab.

     or

   - Click **Cancel** to discard your changes.

2.5.4 Exclusions Tab Settings

The Exclusions tab lets you review and restore Auto-Prompt capability for application logons that you have previously told Logon Manager to ignore.



Note: Your administrator may enable, disable, or override any of the settings described below.

When you launch a password-protected application for which you do not have a Logon Manager account, Logon Manager recognizes it. If your administrator has configured your system to use automatic credential capture, Logon Manager captures your credentials as you enter them. If automatic credential capture is disabled, Logon Manager asks you if you want to create a new account. You have the following options:

- Enter credentials for the account and click **Save**.

- Choose to dismiss the logon dialog for now, and click **Cancel**.
- Permanently dismiss the logon dialog and click **Disable**. This selection adds the application to the Exclusions list.

If at a later time you decide to add an account for an application that you have previously excluded, you can remove the application from the Exclusions list by clearing its checkbox, thereby allowing Logon Manager to prompt you to create an account the next time you launch the application.

See Setting Up Accounts Using Auto-Prompt and Automatic Credential Capture for more information about these features.

2.5.4.1 Restoring Auto-Prompt for an Excluded Application

1. Open Logon Manager.
2. On the Settings panel, click the **Exclusions** tab.
3. This panel contains the list of applications that Logon Manager is currently set to ignore.
4. Click to clear the check boxes of the applications for which you want Auto-Prompt restored, then click **Apply**, or click **Cancel** to discard your changes.

   When you refresh the window, the items you deselected are no longer in the Exclusion list. The next time you launch the password-protected application that you cleared, Logon Manager asks you if you want to create an account.

2.6 Managing Passwords

This section describes how to manage and change passwords within Logon Manager and target applications.

Most applications allow you to change your password at any time while others require you to change passwords periodically, such as every 30 days. You can use Logon Manager to apply and keep track of these changes.

2.6.1 Changing Your Application Password

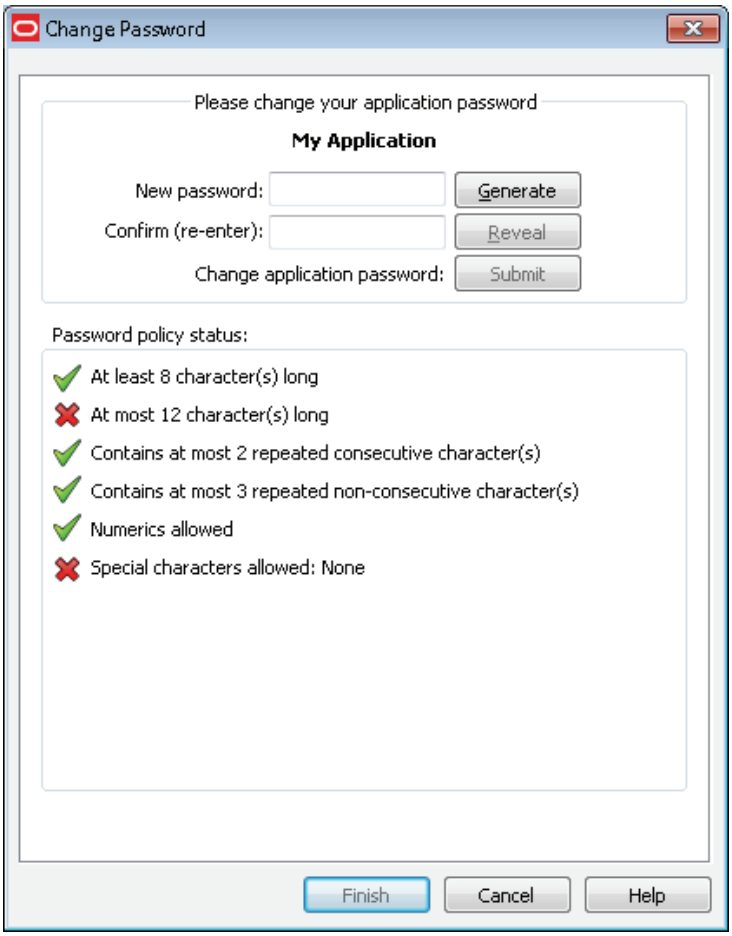
Logon Manager's automated password change functionality increases security by eliminating the potential for poor password selection and poor password management. It also increases usability by saving you the trouble of creating, changing, and remembering passwords.

Logon Manager detects when an application requests a password change. Depending on your configuration, Logon Manager either:

- Automatically generates a new password that conforms to a password policy (the rules that govern what a valid password can be) that your administrator sets.
- Presents the Change Password dialog, which provides you with the option to automatically generate a password or choose your new password.

You may change your password manually or you may be requested to change your password in response to a system-generated prompt. In both scenarios, the following steps apply (with one exception, as explained in step 1).

1. When an application requests a password change, Logon Manager prompts with the Change Password dialog (unless the administrator has configured Logon Manager to perform the change automatically).



Note: If the application displays its logon and password change fields in the same window, the Action Chooser prompts you to choose whether you want to log on or change your password when you launch the application. Logon Manager displays the appropriate screen based on your choice.

2. To change the password, do one of the following:
   - Manually enter a password by typing in and confirming the password.

Note: As you enter the new password, the Password policy status changes. Your new password must comply with each of these rules in order to be valid. As you type your password, the rules it complies with are automatically checked. When all of the rules are checked, your password is valid. The Submit button becomes active after all password policies have been met.

The "Special Characters Allowed" policy indicates the specific special characters that are allowed to be used in a password. If any special characters are not allowed, this policy states: "Special characters allowed: None."

- Click the **Generate** button to have Logon Manager automatically generate the password.
- To view the password, click **Reveal**.
- Click **Submit**.
- If the application accepts the password change, a message appears indicating that the password has been accepted. Click **OK** and Logon Manager saves the password.

  If the application rejects the password, a message appears advising you of such. You can either try a different password and resubmit, or click the **Cancel** button.

Note: If the password has met the password policy set up by the administrator, but has been rejected by the application, contact your system administrator.

2.7 Using Kiosk Manager

Depending on your work environment, your Agent configuration might include Kiosk Manager. Kiosk Manager delivers a secure, easy to use, and easy to administer solution that addresses the needs of traditional single sign-on in a kiosk environment. The Kiosk Manager has a client-side Agent that suspends or closes inactive sessions and shuts down all applications seamlessly.

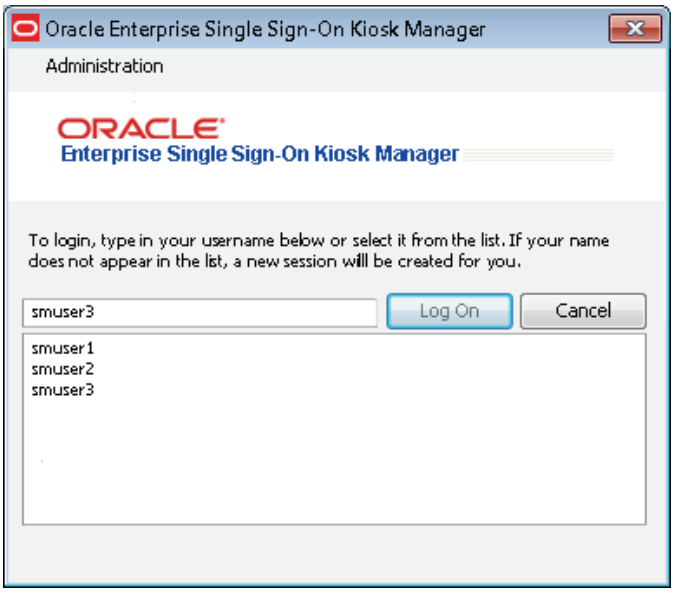
Only an administrator can close Kiosk Manager.

Note: In order for you to log on to your own session, your administrator must set up a synchronization for you. If this is your first time using Logon Manager, when you log onto Kiosk Manager, the Logon Manager Setup Wizard (FTU) appears. Follow the prompts (click **Help** if you need assistance). Select the appropriate authentication method for the Primary Logon Method.

2.7.1 Desktop Manager

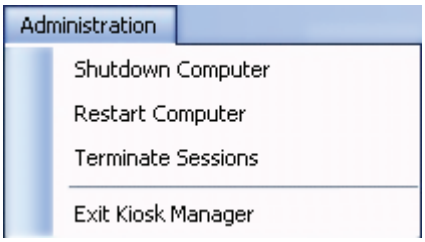
The Desktop Manager is a logon dialog that manages Kiosk Manager sessions. End users can start and unlock sessions, and administrators can terminate sessions, shut down, restart, and exit Kiosk Manager.

The Desktop Manager contains the following information and choices:



2.7.1.1 Administration Menu

Click the **Administration** menu on the top of the Desktop Manager. These menu options might or might not be available, depending on your system configuration.



Command	Function
Shutdown Computer	This option shuts down the kiosk. A confirmation window may appear asking if you are sure you want to shut down this computer. An Authenticate as Administrator dialog may appear prompting you to enter administrative credentials before performing this action.
Restart Computer	This option restarts the kiosk. A confirmation window may appear asking if you are sure you want to restart this computer. An Authenticate as Administrator dialog may appear prompting you to enter administrative credentials before performing this action.
Terminate Sessions	This option allows administrators to terminate open sessions. The Terminate Sessions Authentication dialog appears prompting the administrator to enter credentials before performing this action.
Exit Kiosk Manager	This option allows administrators to exit Kiosk Manager. The Authenticate as Administrator dialog appears prompting you to enter administrative credentials before performing this action.
Reset Password	Depending on your system's configuration, this option may appear. This option initiates the Password Reset Web application, which allows you to reset your password. See Reset Password below.

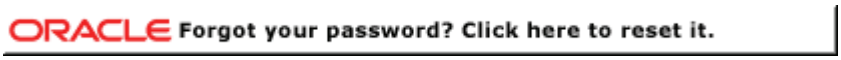
2.7.1.2 Session Logon

The Desktop Manager provides a list that displays all open sessions. If your name does not appear in the list, enter your name to start a new session. After a session is initiated, the Connect to Server dialog appears, prompting you for your password. Enter your password and click **OK**.

Session Option	Function
Log On text field	If your name does not appear in the Open Sessions list, enter your user name in this field and click Log On. A new session will be created for you. This field is editable.
Log On button	Click this button after entering a user name in the field. Double-clicking a user name from the Open Sessions list automatically initiates this function.
Cancel button	This button is available to terminate a logon in process. This button is enabled after a logon has been initiated.
Open Sessions list	The Open Sessions list contains names of all users that have open sessions on this workstation. Clicking once in the list moves the username to the logon field. Clicking twice attempts to open the session.

2.7.1.3 Resetting a Password

Depending on your system's configuration, a password reset banner might appear at the top of the Desktop Manager.

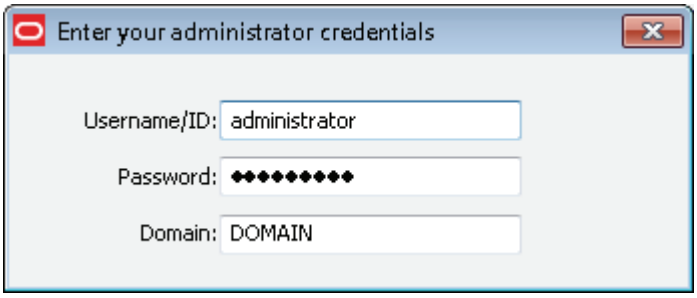


Clicking this banner launches the Password Reset Web interface. Enter your User Name, click **OK** and follow the prompts to reset your password.

2.7.1.4 Terminating Sessions

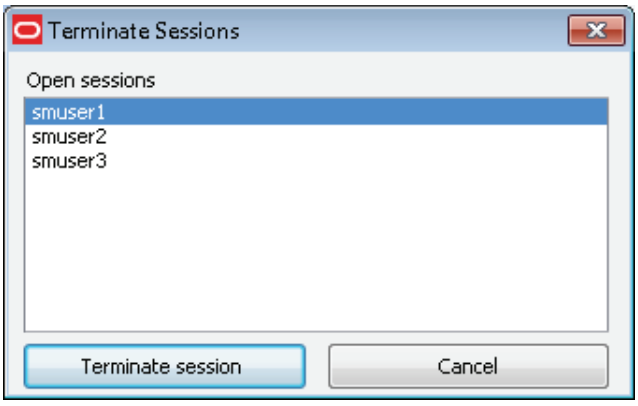
To terminate a session:

1. From the Desktop Manager Administration menu, click **Terminate Sessions**.
2. In the Authenticate as Administrator dialog, enter administrative credentials.



3. Enter your Username/ID, Password, and Domain. Click **OK**.

   The Terminate Sessions dialog prompts you to select a session to terminate.



4. Select a session from the Open Sessions list box and click **Terminate session**. You can select only one session at a time. The session will be removed from the Open sessions list.
5. Click **Cancel** to close this dialog.

2.7.2 Session Owner Window

The Session owner window might display in the upper right corner of your desktop during a session, depending on your system's configuration.

You can view the session owner or lock your session from this window.

2.7.3 Locking and Unlocking Sessions

Do one of the following to lock a session:

- Click the **Lock Session** button on the Desktop Status window.
- Select the Kiosk Manager tray icon menu and click **Lock Session**.
- When configured with smart card, proximity card, or other presence-sensing authenticator, remove the card. Kiosk Manager automatically locks a session if the strong authenticator is no longer present (either removed from the reader or is out of range).
- Allow the screen saver to launch. Kiosk Manager locks the session when the kiosk screen saver would normally start.
- Shut down Logon Manager.
- Perform any activity that would normally lock the desktop. This will cause Kiosk Manager to lock the session.
- Click **Ctrl + Alt + Delete**.

It is important to note that if a user locks a session or leaves the kiosk while an application has a dialog open, (such as the "Save As" dialog) and Kiosk Manager is unable to dismiss that dialog, the application may be terminated. It is strongly recommended that users save data before locking a session or leaving the kiosk.

Do one of the following to unlock a session:

- When configured with smart card, proximity card, or other presence-sensing authenticator, Kiosk Manager automatically initiates a session when a strong authenticator is detected (either inserted into reader or is in range).
- The current session can be unlocked from the Desktop Manager by selecting your name and re-entering your credentials.

3

Deploying Single Sign-On Client Software Using Anywhere

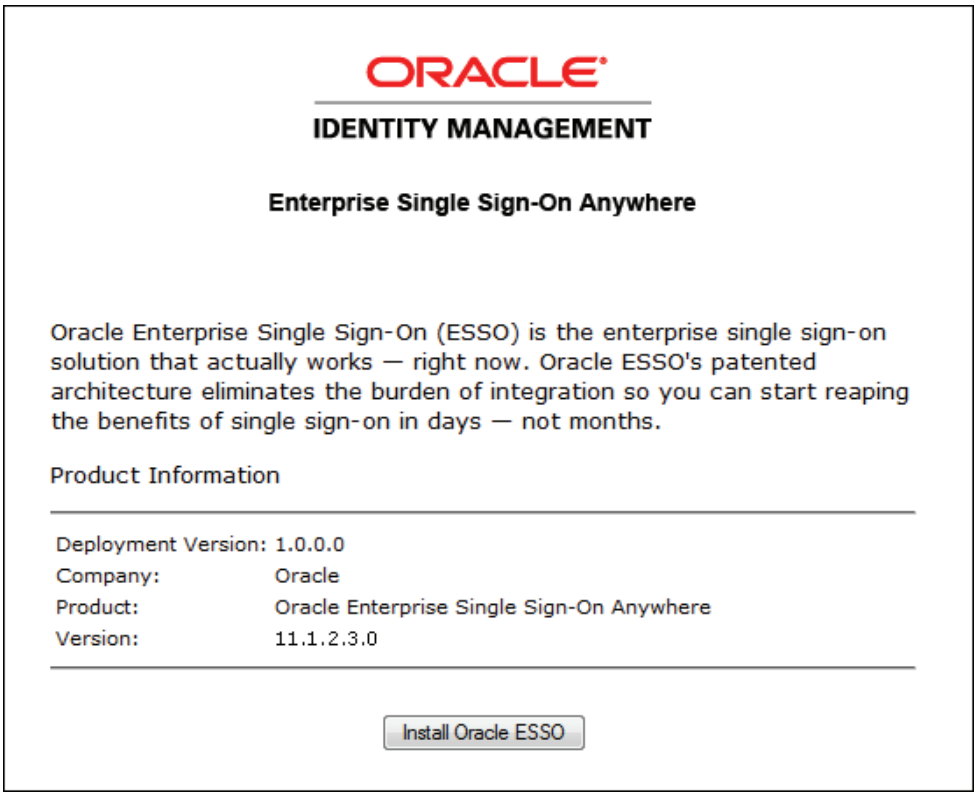
Anywhere provides a simple mechanism for you to deploy a Logon Manager configuration on your own workstation, without the assistance of your administrator. You will receive notification that the Anywhere deployment package is available for download. Simply click the link to the deployment package, download it, and follow the familiar Windows installation wizard process. The package has been pre-configured exactly as you need it.

Updates and rollbacks are equally simple. Whenever your administrator makes any changes to your configuration, you will receive another notification. Follow the same process as for your original installation.

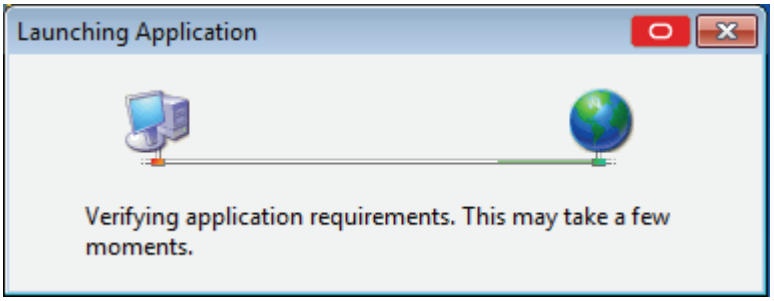
You can be certain that your configuration is always correct and ready to run, because your administrator has pre-configured and tested it before you receive it.

3.1 Setting Up Anywhere

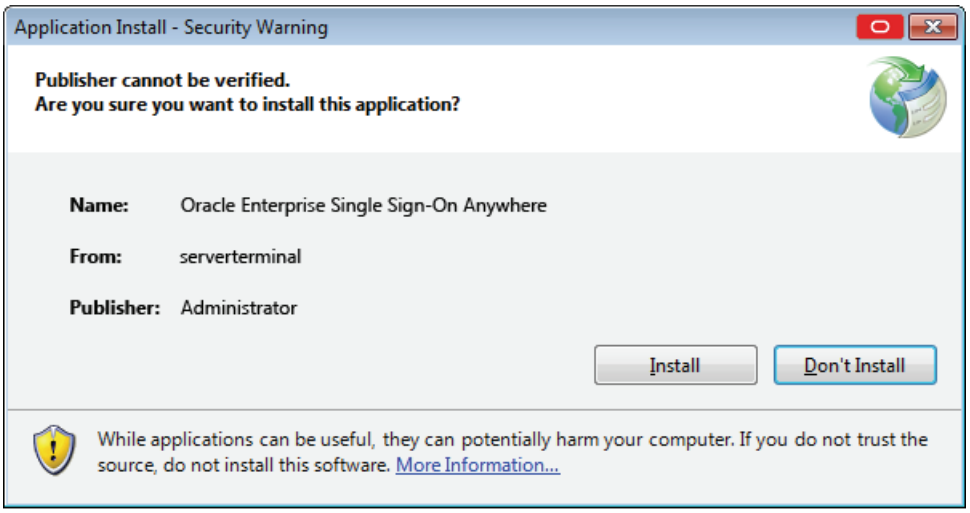
Prior to installing Anywhere on your local workstation, you should have received any authentication hardware that you will need, if applicable. When you launch the installer, all the software and settings that you need to run Logon Manager, and Provisioning Gateway will automatically be installed with one click. Your administrator will notify you where to locate the Anywhere installer, and you will be directed to the Anywhere landing page, which will look similar to the following:



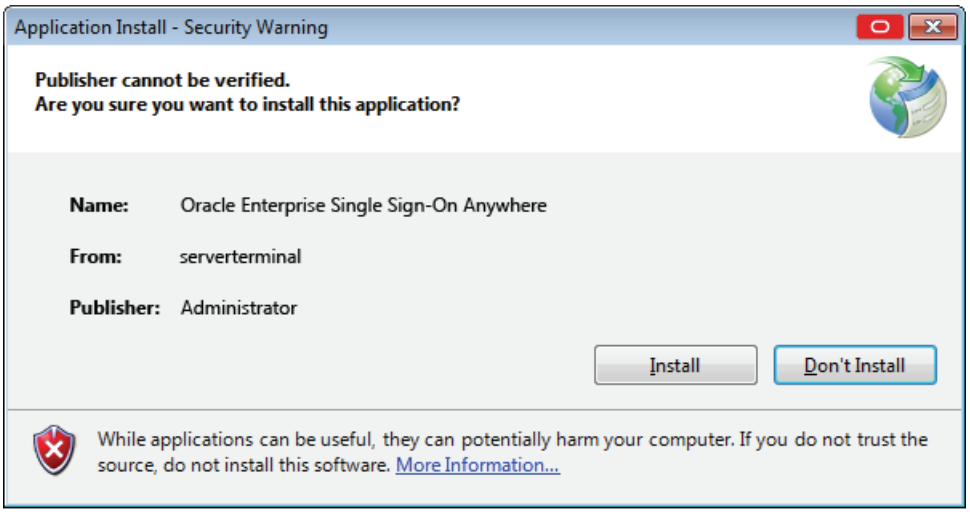
1. Click on the **Install Oracle** button to launch the installation package. Anywhere scans your workstation to verify that all prerequisites are present.



After Anywhere ascertains the presence of all prerequisites on your workstation, Anywhere may ask you to verify that the installation certificate is valid. There are two possibilities:

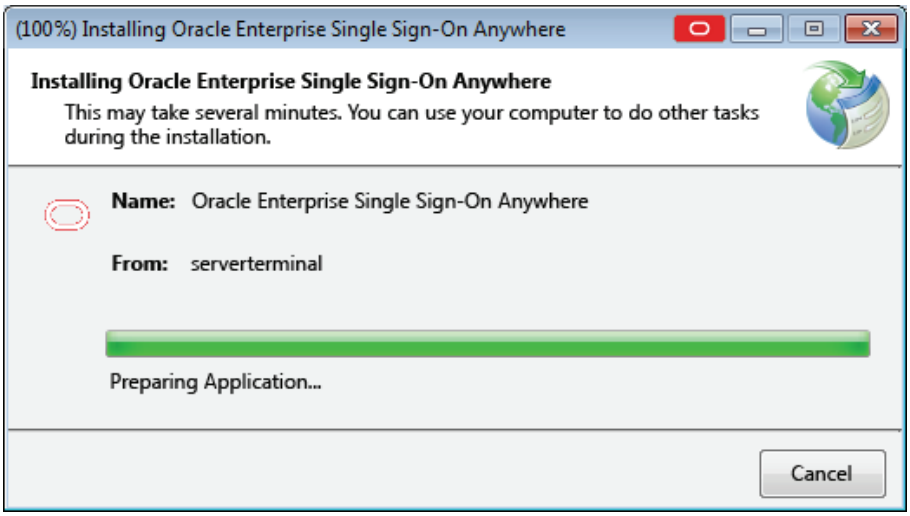


The certificate is valid. Click Install to proceed.



The certificate publisher is unknown. Check with your administrator before proceeding.

2. After you have verified the authenticity of the certificate, click **Install** to begin installation.

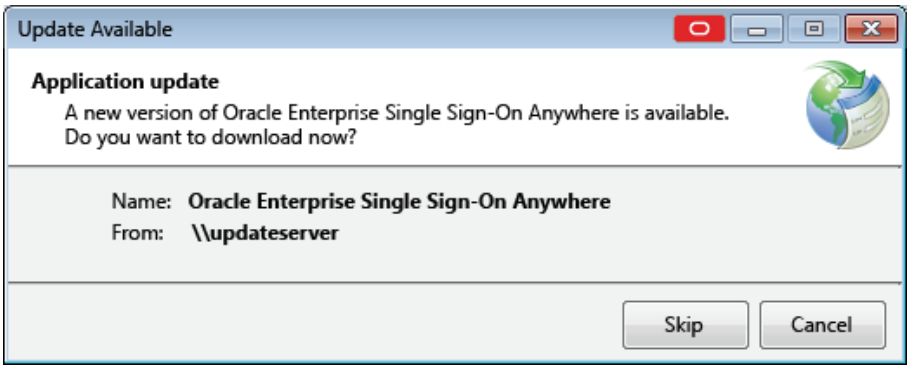


Anywhere completes the installation. If you have not previously gone through the First Time Use (FTU) wizard, you will be prompted to do so after installation completes. If you have already supplied credentials to the system, your credentials are available immediately. You can begin using Logon Manager immediately.

3.2 Updating Anywhere

At various times you will receive notification that an update is available for Anywhere. The frequency at which this occurs, and whether installing the update is mandatory, are determined by your administrator.

When an update is available, the following screen displays:



If your administrator has given you the option, you can choose to click **Skip** and not install the update. If you do not have the option or want to install the update, click **OK**.

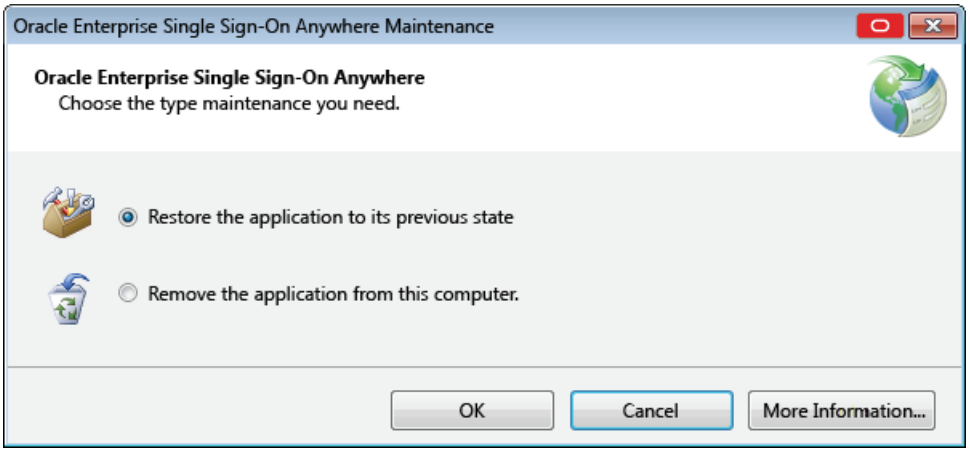
3.3 Rolling Back Anywhere

If your administrator decides to roll back your version of Anywhere to an earlier version, you will receive a notification.

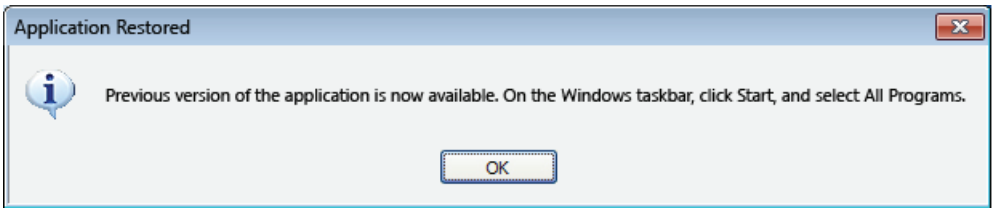
To perform a rollback:

1. Open the Control Panel settings and select **Programs and Features**.
2. Select **Anywhere** from the program list, and click **Change/Remove**.

3. Select **Restore** the application to its previous state. Then click **OK**. Anywhere installs the rollback.



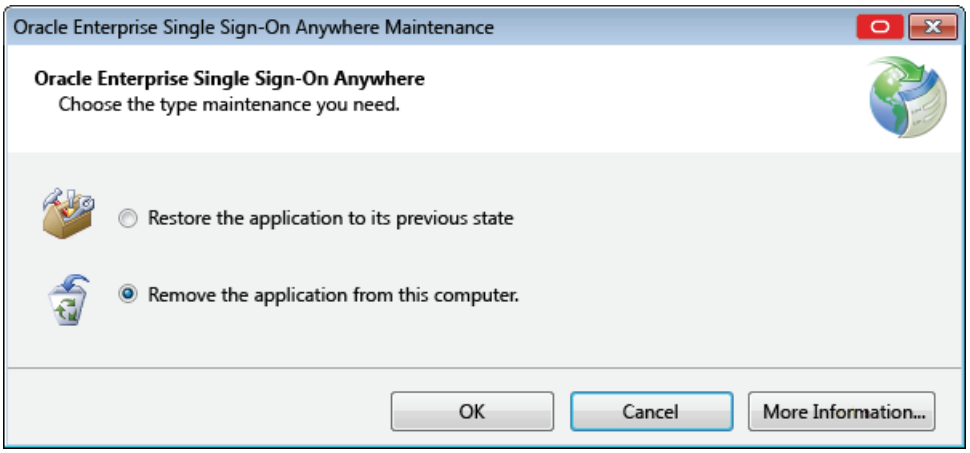
4. When the Application Restored message displays, click **OK**.



3.4 Uninstalling Anywhere

To uninstall Anywhere:

1. Open the Control Panel settings and select **Programs and Features**.
2. Select **Anywhere** from the program list, and click **Uninstall**.
3. Click the **OK** button.



4

Resetting Your Password Using Password Reset

Password Reset lets you access your Windows user account when you lose or forget your password. There is no need to call your help desk or technical support, and no waiting for an administrator to reset your password. Password Reset is specially designed for the purpose of allowing you to reset your Windows password, without contacting your administrator, if you lose or forget it.

All you have to do is pass a quick pop-quiz that verifies your identity, and you can reset your password yourself. And you will pass, because you will have created the quiz answers during the Enrollment Interview.

After you complete your Enrollment Interview, you can take the Reset Quiz any time you lose or forget your password. If your quiz answers match the answers you provided in the Enrollment Interview, you can create a new Windows password and log on.

Password Reset is simple, quick, and secure, and it frees up your organization's technical support for other priorities. Best of all, the couple of minutes that the Enrollment Interview takes will more than make up for the time and effort if you lose your Windows password.

4.1 A Word About Passwords

If you do forget your password, at the very least, it indicates that you picked a good one—that is, one that no one else could have guessed.

The best passwords are the ones that are the hardest to remember, because they're composed of random letters and numbers. Moreover, good network security calls for changing passwords every few weeks. As fast and easy as the Password Reset Reset Quiz is, it is still faster to use a password to access your network. Here are some tips for creating and managing your password:

- A meaningless string of characters is best. Mix capital and lower-case letters and use numbers.
- Avoid using the names of relatives, friends, or pets.
- Avoid any meaningful words at all—in any language. If your password is in the dictionary, someone can guess it.
- Do not share your password with others.
- Do not write or post your password—especially on "sticky-notes" near your workstation.

One trick for creating a memorable (and meaningless) password quickly is to take the first letters of a familiar phrase or quote. In this way, "Self trust is the first secret of success" (Emerson) becomes "stitfsos."

4.2 About Enrollment

Enrollment in Password Reset consists of answering a series of questions that your administrator has configured with point values for correct and incorrect answers. You must answer enough questions so that if you ever need to reset your password, you can accumulate enough points to pass the reset quiz.

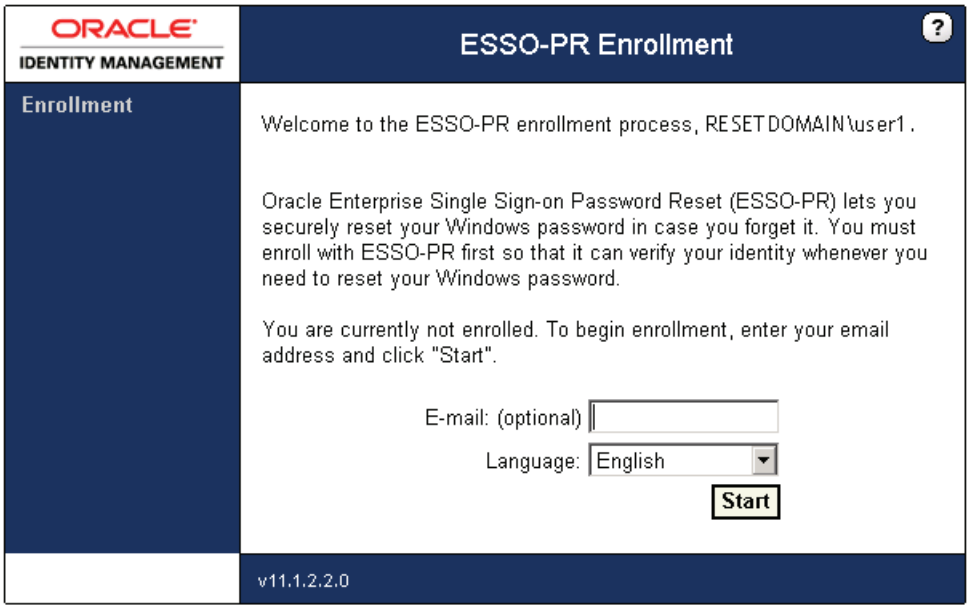
There are no wrong answers during enrollment, but the answers that you supply here must match your answers if you ever have to take the Reset Quiz, so it is important that you select answers that you will remember easily. During enrollment, Password Reset continues to present questions until you have supplied enough answers to achieve the point threshold to qualify for resetting your password. Your administrator might require answers to some questions, and make other answers optional. It is to your advantage to answer as many questions as you can-even the optional ones-because it will increase your chances of passing the reset quiz if you forget any of the answers you supplied during enrollment.

The questions are weighted based on how likely it is that you, or someone else, will know the answer. Certain questions can be immediate disqualifiers. For example, during the Reset Quiz, getting your eye color right will not score you a lot of points, but getting it wrong would certainly indicate that the person taking the quiz is not you, and result in an immediate failure. Contrastingly, certain questions will not have a great point value either way. Many people besides you are likely to know your pets' or children's names, or the type of car you drive, so these types of questions will help you progress towards achieving your point threshold, but will not be weighted heavily.

4.2.1 The Enrollment Interview

Before you can use Password Reset when you really need it-to create a new Windows password-you need to provide the right answers to the questions in the Reset Quiz. That is the purpose of the Enrollment Interview.

To begin enrollment, in your browser, enter the URL provided by your administrator to access the Enrollment Interview. At the enrollment screen, enter your Email address (if required), select the language in which to enroll, and click **Start**.



The questions in the Enrollment Interview will be used to create the Reset Quiz you will take if you ever need to log on without your password, and the answers you provide will be the ones used to verify that it is really you when you take the Reset Quiz.

Note: Reset questions will be displayed in the same language as the one in which you enrolled.

There are two types of questions in the Enrollment Interview:

- **Required Questions.**·If required questions are set up, you must answer these questions to complete enrollment.
- **Optional Questions.** If optional questions are available, you can answer or skip any of them. You may be required to complete a certain number of them in order to complete the enrollment interview.

Note: it is important that you keep your answers to the questions as brief and as memorable as possible.

4.2.1.1 Required Questions

You must provide an answer to each of the required questions. These questions will be used to create the Reset Quiz. Enter the briefest, simplest answers you can, because:

- You will need to remember them.
- You will need to enter your answers in the Reset Quiz exactly as you enter them here.

Be careful of how you use upper-case or lower-case characters, and be especially careful of spelling and spaces. Avoid punctuation if possible. Note and follow any format instructions or examples that the question provides.

When you have typed your answer in the text box, click **Next**.

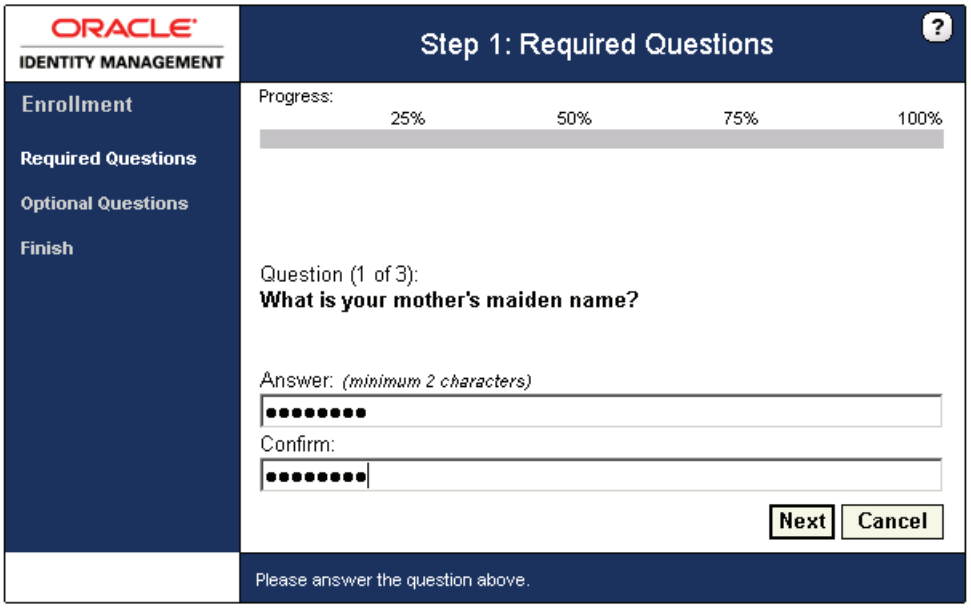
4.2.1.2 Optional Questions

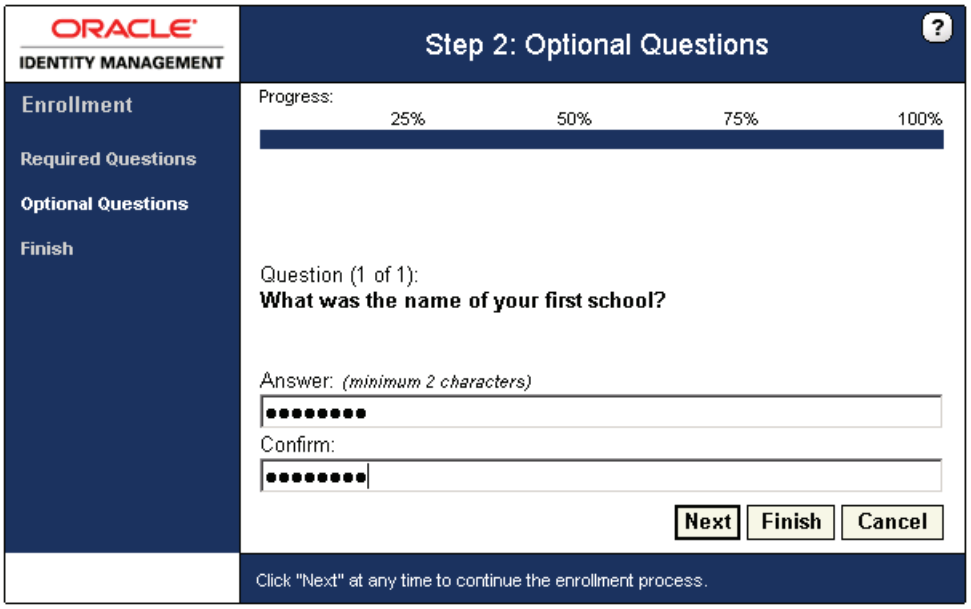
You have the option to answer these questions or skip them. Remember that the more questions you choose to answer, the more secure the quiz will be.

4.2.1.3 The Progress Bar

The progress bar seen during the enrollment interview indicates your progress (in percentage) in satisfying the enrollment level threshold. You must answer questions until the progress bar reaches 100%.

Depending on how your administrator set up the interview, the progress bar might leap from one percentage to another, as all questions might not be weighted evenly. The percentage does not indicate the number of questions you must answer to complete the interview.



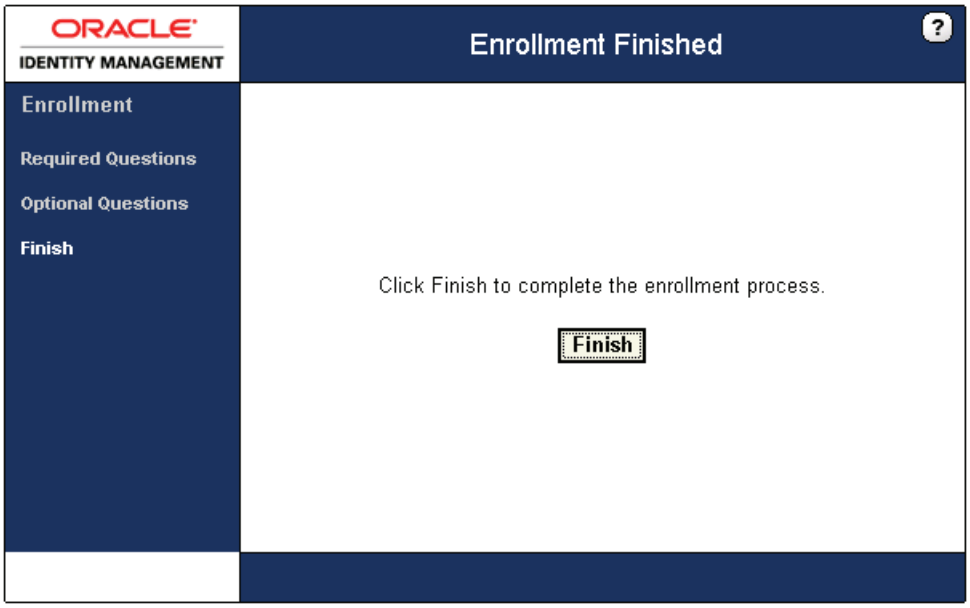


After you answer each question, click **Next** to proceed with the interview. If at any time you decide not to answer any more optional questions, or when you have answered all the questions presented, click **Finish**.

4.2.1.4 Completing the Enrollment Process

If you reach the end of the question set without enough points to meet the enrollment level threshold, Password Reset displays a message stating that you have not reached the minimum enrollment threshold and you need to answer more questions: "You have not answered enough questions to satisfy the enrollment requirement. Please answer more questions until the progress bar reaches 100%."

Password Reset will then begin the optional question set, prompting you to answer questions you previously skipped. You must answer questions until the progress bar reaches 100%.



At the final screen of the interview, click **Finish**.

4.2.2 About the Reset Quiz

If you lose or forget your password, you'll need to reset it; that is, erase the old password you have forgotten and supply a new one. The Reset Quiz is how Password Reset verifies your identity when you need to reset your password.

The Reset Quiz is like having a bank officer verify your identity over the telephone by asking for a piece of information that only you would be likely to know; your mother's maiden name is a common example. You might be asked for several such items from different sources-your place of birth, your current address, and so on-that only you would be likely to know. Password Reset uses the same idea-not just one question, but a group of questions that confirm your identity.

If you need to reset your password, click the **Password Reset** button on the Windows logon dialog. At the Password Reset reset logon dialog, enter your username to begin the Reset Quiz.

Password Reset displays one of the questions from your Enrollment Interview. Type the answer to the question exactly as you did in the Enrollment Interview, and click **Answer**. Repeat this process until the New Password dialog appears.

The Reset Quiz might not use all of the questions from your interview. How many questions the quiz asks depends on how your administrator has set it up. Questions can have different point values, and it is your overall score that Password Reset uses to authorize a password reset.

Note: Depending on how your administrator configured Password Reset, after passing the Reset Quiz, you might have the option to choose whether to reset your password or unlock your account.

Reset questions are displayed in the language in which you enrolled.

4.2.3 Taking the Reset Quiz to Reset Your Password

You can use the Reset Quiz to reset your password at your own workstation from the Windows logon, or, you can use Internet Explorer to take the Reset Quiz on any other workstation that is already logged on.

During the Reset Quiz, Password Reset presents the same questions that you answered during the Enrollment Interview. Enter your answers exactly as you did in the interview. Spaces and punctuation must match, although capitalization can vary.

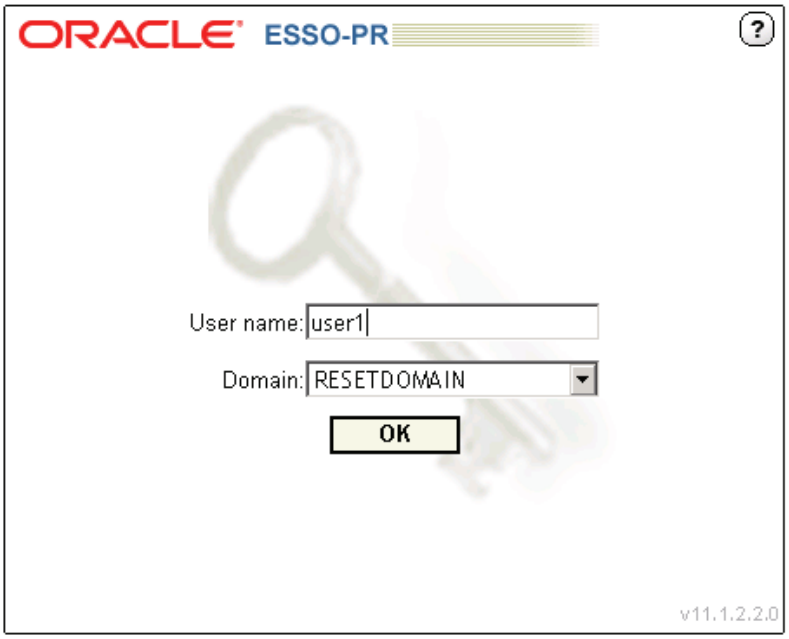
4.2.3.1 Starting the Reset Quiz at the Windows Logon (On Your Own Workstation)

1. Click the **Password Reset** button in the upper-right corner of the window. Password Reset displays a logon prompt that asks for your username.
2. Type your username and click **OK**. Password Reset begins the Reset Quiz.

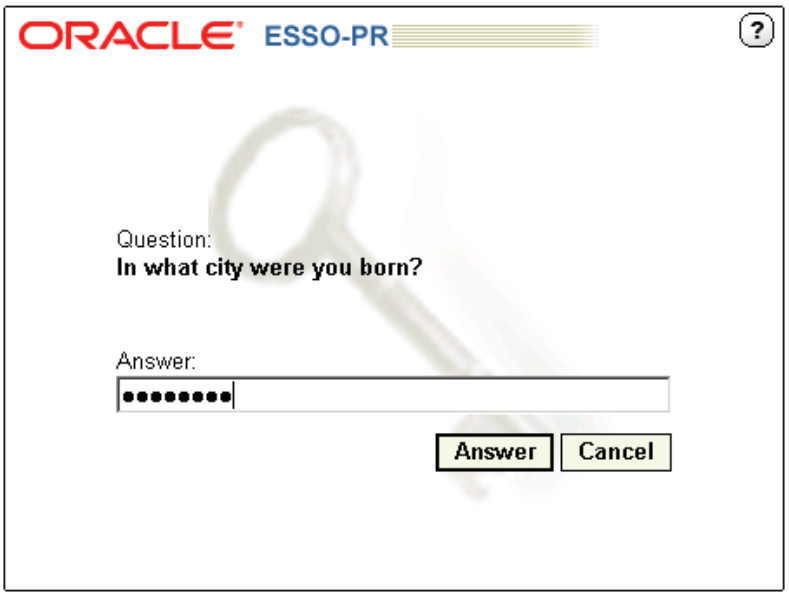
4.2.3.2 Starting the Reset Quiz from a Logged-On Workstation

Note: You will need the Web address of the Password Reset Reset Quiz start page to use this method. This address might be available as a link on your organization's intranet or it could be in the Internet Explorer Favorites list.

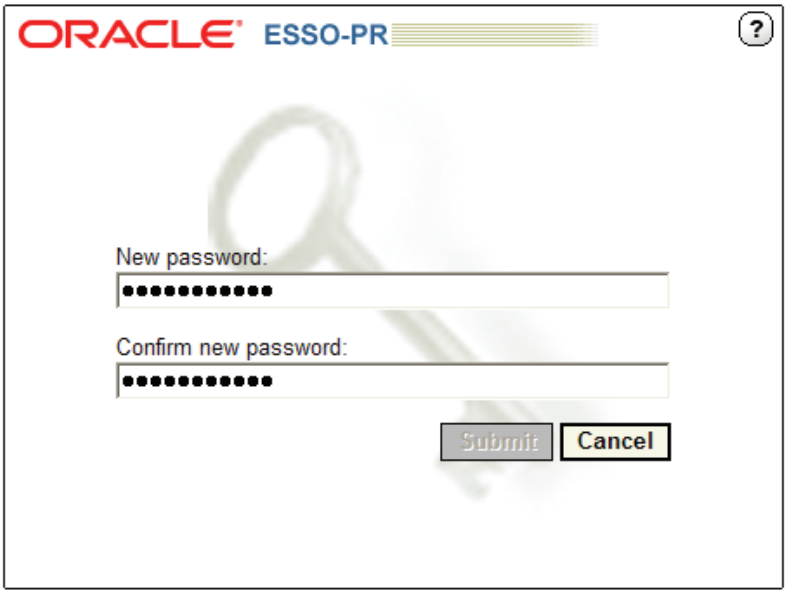
1. Open Internet Explorer and point the browser to the Password Reset Reset Quiz start page. Password Reset displays a logon prompt that asks for your username.



2. Enter your username and click **OK**. Password Reset begins the Reset Quiz.



3. Enter your answers when the questions are presented to you. When you answer enough questions correctly to reach your threshold score, the Reset Password screen displays.



4. Enter a new password and confirm it. Then click the **Submit** button. Your password is reset.

4.2.3.3 After You Pass the Reset Quiz

Depending on how your administrator configured Password Reset, after passing the Reset Quiz, you may have the option to choose whether to reset your password or unlock your account:

- If you choose to reset your password, you will be taken to the Reset Password page.
- If you choose to unlock your account, the Password Reset Change Password Service will unlock your account and you will be presented with a Finish page.

4.2.3.4 If You Fail the Reset Quiz

- Try again. Password Reset selects and displays quiz questions in random order. You might very well be asked different questions on your next try.
- Enter your answers carefully. Your quiz answers must exactly match the ones you entered during your Enrollment Interview. How you use upper-case and lower-case letters does not matter, but spelling, spacing, and punctuation do.
- If you are using a workstation other than your usual one, make certain that you have provided the correct-that is, your own-username and ID. Otherwise, you might be taking the quiz against another user's answers.

If all else fails, call your administrator to reset your password. If you do take this last resort, you should also re-take the Enrollment Interview to revise your answers to be simpler or easier to remember.

4.2.3.5 Temporary Passwords

Your administrator might also have configured Password Reset to provide you with a temporary password after you pass the Reset Quiz. In this case, Password Reset will give you a temporary password, which you use to log on to Windows. You can then change your temporary Windows password to a permanent one using the Windows Change Password feature.

5

Using Universal Authentication Manager for Strong Authentication

The Oracle Enterprise Single Sign-On Universal Authentication Manager system enables you to replace the use of native password logon to Microsoft Windows and Active Directory networks with stronger and easier to use authentication methods, while further enhancing security by providing two-factor authentication in the form of a PIN paired with an enrolled logon method.

Universal Authentication Manager allows you to rapidly and securely enroll credentials that will be used to identify and authenticate you to the system. Out of the box, Universal Authentication Manager offers four built-in and configurable authentication methods: smart cards, passive proximity cards, biometric fingerprint, and a challenge questions quiz. Native Windows passwords are also supported.

5.1 Getting Started Using Universal Authentication Manager

Universal Authentication Manager offers an intuitive interface that allows you to easily enroll credentials for your logon methods. There are two panels from which you can perform all actions for your logon methods:

- Logon Methods
- Settings

5.1.1 Fingerprints

Universal Authentication Manager enables you to enroll and use third party standalone and embedded fingerprint scanners as an authentication mechanism to Universal Authentication Manager.

Depending on your environment, your administrator may configure Universal Authentication Manager to require that a PIN be entered when logging on with a fingerprint; in such cases, you will be prompted to select a PIN when enrolling your fingerprints with Universal Authentication Manager. If the PIN requirement is not being enforced by your administrator, you may still choose to assign a PIN to your fingerprint enrollment for heightened security.

Note: This logon method requires the BIO-key 1.12 BSP to be installed. If this is not installed, you will get an error message. Versions earlier than 1.10 are not supported. Contact your system administrator for assistance.

The following actions are available:

- Enrolling a Fingerprint at Windows Logon
- Enrolling a Fingerprint When Launching Universal Authentication Manager
- Changing Your Universal Authentication Manager PIN
- Fingerprint Settings

5.1.2 Proximity Cards

A passive proximity card or token is an identity object (such as a workplace ID badge) containing a circuit that a card-reading device can detect and decipher. When you place a proximity card close to a card reader, the reader detects the token's presence and recognizes identifying information that is associated with you.

Universal Authentication Manager also gives you the option (depending on your system configuration) to require a PIN during logon for more secure two-factor authentication.

The following actions are available:

- Enrolling a Proximity Card at Windows Logon
- Enrolling a Proximity Card when Launching Universal Authentication Manager
- Enrolling a Proximity Card Manually
- Changing Your Universal Authentication Manager PIN
- Proximity Card Settings

5.1.3 Smart Cards

A smart card is a credit card-sized token containing a chip or embedded circuits that can store and process data securely. Information stored on a smart card can also be used for identification and authentication. Universal Authentication Manager enables you to enroll and use smart cards for logon and authentication without writing any data on the smart card chip.

For heightened security, Universal Authentication Manager requires that a PIN be assigned to each enrolled Smart Card and that you enter that PIN when logging on with the corresponding card. Universal Authentication Manager supports a card's built-in PIN and can also generate and assign a virtual PIN.

The following actions are available:

- Enrolling a Smart Card at Windows Logon
- Enrolling a Smart Card when Launching Universal Authentication Manager
- Changing Your Universal Authentication Manager PIN
- Enrolling a Smart Card Manually
- Smart Card Settings

Note: When using a smart card, the card's own PIN cannot be changed. Only a Universal Authentication Manager PIN associated with the smart card can be changed. For more information, see Configuring Universal Authentication Manager.

5.1.4 Challenge Questions

Challenge Questions is a question-and-answer quiz that requires you to correctly answer enough questions (which you have selected and provided answers for when you first enrolled this method) to satisfy the weight requirement for successful logon set by the administrator.

- Enrolling Challenge Questions at Windows Logon
- Enrolling Challenge Questions when Launching Universal Authentication Manager
- Enrolling Challenge Questions Manually
- Challenge Questions Settings

5.2 Configuring Universal Authentication Manager

The Settings panel displays configurable policy settings for each logon method. The following settings are available, depending on how your instance of Universal Authentication Manager is configured by your administrator:

- Display Settings
- Fingerprint Settings
- Proximity Card Settings
- Smart Card Settings
- Challenge Questions Settings
- Windows Password Settings
- Availability of Settings in Enterprise Mode

5.2.1 Display Settings

On the **Display** tab, you may be able to view or configure the following setting:

User Language	Selects the language in which the Universal Authentication Manager interface is displayed. The default value is the language of the operating system. **Note:** This menu only shows languages for which the corresponding Universal Authentication Manager language packs have been installed. If you don't see the desired language in the list, contact your administrator.

5.2.2 Fingerprint Settings

On the **Fingerprint** tab, you may be able to view or configure the following settings:

Logon Method Enabled	Controls if an installed authenticator is enabled or disabled. This policy setting enhances security by controlling the specific logon methods you are allowed to use. Options are **Yes** (default setting) and **No**. **Note:** The **Logon Method Enabled** setting is only displayed if Universal Authentication Manager has been configured into local client mode. In enterprise mode, this setting is not displayed.

Number of Fingers	Specifies the number of finger samples you are required to enroll. This policy requires you to enroll exactly the specified number of finger samples during enrollment. Default is 1. Maximum is 10.
PIN Required	Specifies whether you must submit a PIN in order to be authenticated. Options are **Yes** (default setting) or **No**.
PIN Minimum Length	The minimum allowed length for the PIN. Possible values are 4-16 characters (default setting is 4 characters).
PIN Allowed Characters	Restricts the character type(s) you can use in your PIN. Options are **numeric only**, **alphanumeric only**, or **any characters** (default setting).

5.2.3 Proximity Card Settings

On the **Proximity Card** tab, you may be able to view or configure the following settings:

Logon Method Enabled	Controls if an installed authenticator is enabled or disabled. This policy setting enhances security by controlling the specific logon methods you are allowed to use. Options are **Yes** (default setting) and **No**. **Note:** The **Logon Method Enabled** setting is only displayed if you are working in local mode. In enterprise mode, this setting is not displayed.
Removal Action	Controls how Universal Authentication Manager behaves when you "tap out" your proximity card (tap your card against the reader a second time during a session). Options are: ■ No Action. ■ Lock workstation (locks the workstation; you must re-authenticate to return to your session). ■ Force Logoff (automatically logs you off the workstation).
PIN Required	Specifies whether you must submit a PIN for your card in order to be authenticated. Options are **Yes** (default setting) or **No**.
PIN Minimum Length	The minimum allowed length for the proximity card PIN. Possible values are 4-16 characters (default setting is 4 characters).
PIN Allowed Characters	Restricts the character type(s) you can use in your proximity card PIN. Options are **numeric only**, **alphanumeric only**, or **any characters** (default setting).

5.2.4 Smart Card Settings

On the Smart Card tab, you may be able to view or configure the following settings:

Logon Method Enabled	Controls if an installed authenticator is enabled or disabled. This policy setting enhances security by controlling the specific logon methods you are allowed to use. Options are **Yes** (default setting) and **No**. **Note:** The **Logon Method Enabled** setting is only displayed if you are working in local mode. In enterprise mode, this setting is not displayed.

Removal Action	Controls how Universal Authentication Manager behaves when you remove your smart card. Options are: ■ No Action ■ Lock workstation (locks the workstation; you must re-authenticate to return to your session) ■ Force Logoff (automatically logs you off the workstation)
PIN Type	Specifies whether to use the card's internal preconfigured PIN or create and store a PIN within Universal Authentication Manager's secure data store. Options are **Smart Card PIN** (default setting) or **ESSO-UAM PIN**.
PIN Minimum Length	(ESSO-UAM PIN type only) The minimum allowed length for the smart card PIN. Possible values are 4-16 characters (default setting is 4 characters).
PIN Allowed Characters	(ESSO-UAM PIN type only) Restricts the character type(s) you can use in your smart card PIN. Options are **numeric only**, **alphanumeric only**, and **any characters** (default setting).

5.2.5 Challenge Questions Settings

On the Challenge Questions tab, you may be able to view or configure the following settings:

Logon Method Enabled	Controls if an installed authenticator is enabled or disabled. This policy setting enhances security by controlling the specific logon methods you are allowed to use. Options are **Yes** (default setting) and **No**. **Note:** The **Logon Method Enabled** setting is only displayed if you are working in local mode. In enterprise mode, this setting is not displayed.

5.2.6 Windows Password Settings

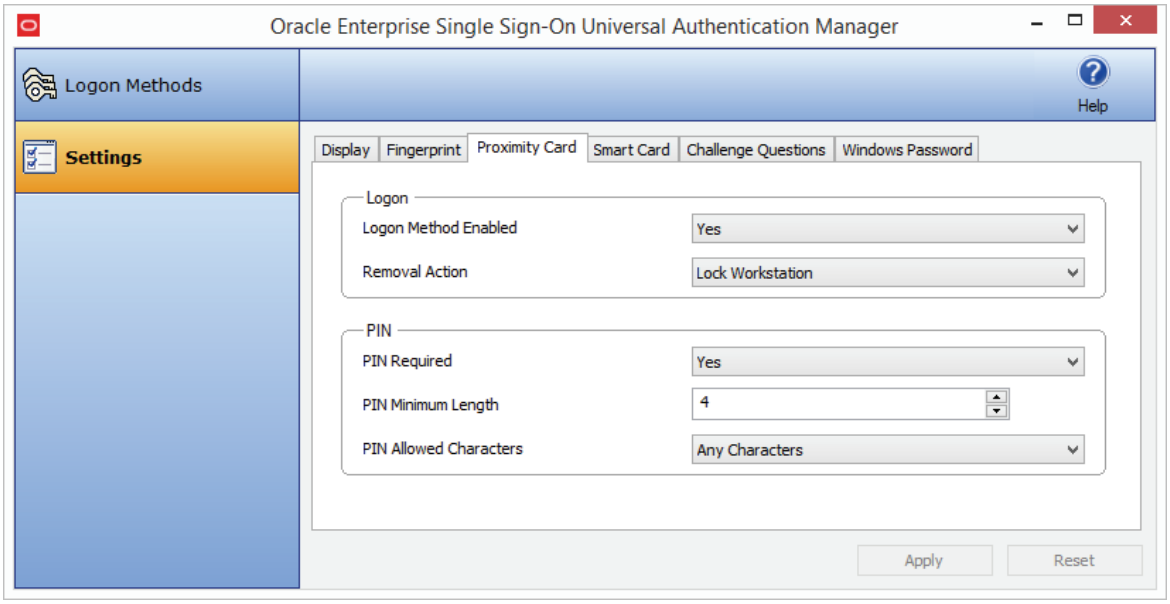
On the Windows Password tab, you may be able to view or configure the following settings:

Logon Method Enabled	Controls if an installed authenticator is enabled or disabled. This policy setting enhances security by controlling the specific logon methods you are allowed to use. Options are **Yes** (default setting) and **No**. **Note:** The **Logon Method Enabled** setting is only displayed if you are working in local mode. In enterprise mode, this setting is not displayed.

5.2.7 Availability of Settings in Enterprise Mode

If Universal Authentication Manager has been deployed in enterprise mode, your administrator may choose to enforce certain settings that will be disabled in your workspace; that is, your administrator will configure those settings and you will not be able to configure them.

For example, your administrator may choose to specify and enforce that when a smart card is removed, you are automatically logged off the workstation (using the **Force Logoff** setting). In this scenario, the **Force Logoff** setting will be visible to you, but it will be disabled; you will not be able to change it.



For more information, see Selecting the Client Mode.

5.2.8 Selecting the Client Mode

When you install Universal Authentication Manager, the InstallShield Wizard asks you to choose the client mode you wish to use.

5.2.8.1 Enterprise Client Mode

If you choose the enterprise client mode, you will be accessing a network and a database that stores settings for your account. In this mode, the administrator configures Universal Authentication Manager for you and you may not be able to modify some of the settings. To update your account with changes made by your administrator, click **Refresh**.

5.2.8.2 Local Client Mode

If you choose the local client mode, Universal Authentication Manager will not connect to a network in order to retrieve your settings; instead, Universal Authentication Manager stores and manages your settings on your local workstation. You can configure all of the settings that are visible to you in this mode.

To configure settings, click the **Settings** tab in the left panel of the screen. A tab is displayed for each Universal Authentication Manager logon method installed on the workstation. Click a tab to display and configure settings for that logon method. To apply your configuration, click **Apply** at the bottom of the screen. To cancel your changes and return settings to their previous state, click **Reset**.

For more information, see Configuring Universal Authentication Manager.

5.3 Integrating with Logon Manager

Universal Authentication Manager can operate as a stand-alone application and also integrate seamlessly with Logon Manager. Depending on how your administrator has configured Universal Authentication Manager, one of the following scenarios applies:

- If your administrator has installed and enabled one or more of the individual Universal Authentication Manager authenticators during a Universal Authentication Manager custom installation, those authenticators will appear as separate logon methods in the list of Logon Manager logon methods.

  In this scenario, if you have not already enrolled with the primary logon method chosen by your administrator, you will be prompted to enroll with the method chosen by the administrator when you log on for the first time.

- If your administrator has chosen to install the multi-method Universal Authentication Manager authenticator instead, and has enabled at least one logon method through that authenticator, you will see a single "Universal Authentication Manager" entry in the list of Logon Manager logon methods.

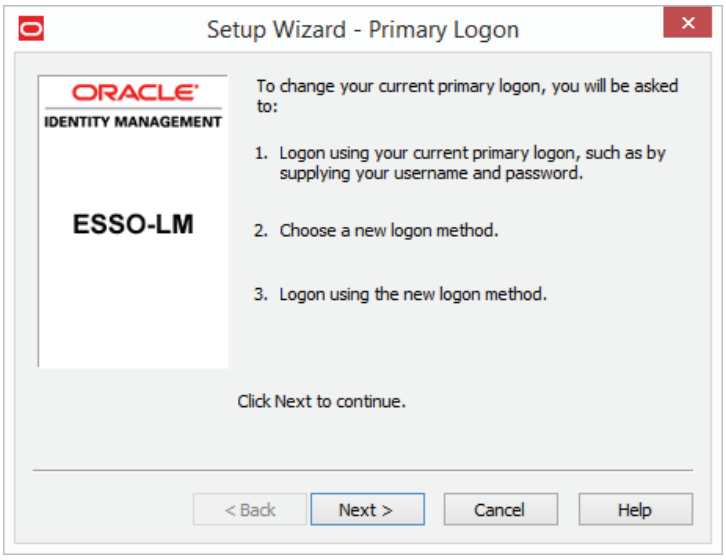
  In this scenario, if you have not already enrolled any logon methods with Universal Authentication Manager, you will need to enroll with the enabled logon methods from within Universal Authentication Manager before they can be used to authenticate to Logon Manager. Until then, you will be prompted to authenticate with your Windows password.

Note: Universal Authentication Manager authenticators must be installed before you can configure a Universal Authentication Manager logon method as the primary logon method for Logon Manager. For details on installing the necessary integration components, see the *Oracle Enterprise Single Sign-On Suite Installation Guide*.

5.3.1 Configuring Universal Authentication Manager as the Primary Logon Method with the First-Time Use Wizard

If you are new to Logon Manager and Universal Authentication Manager, you can configure a Universal Authentication Manager logon method as your primary Logon Manager logon method with the Logon Manager First-Time Use wizard. The First-Time Use wizard gives you the option to select a Universal Authentication Manager logon method (or any other Logon Manager logon methods that are installed) as your primary logon method. To use the first-time use wizard to set a Universal Authentication Manager logon method as your primary logon method:

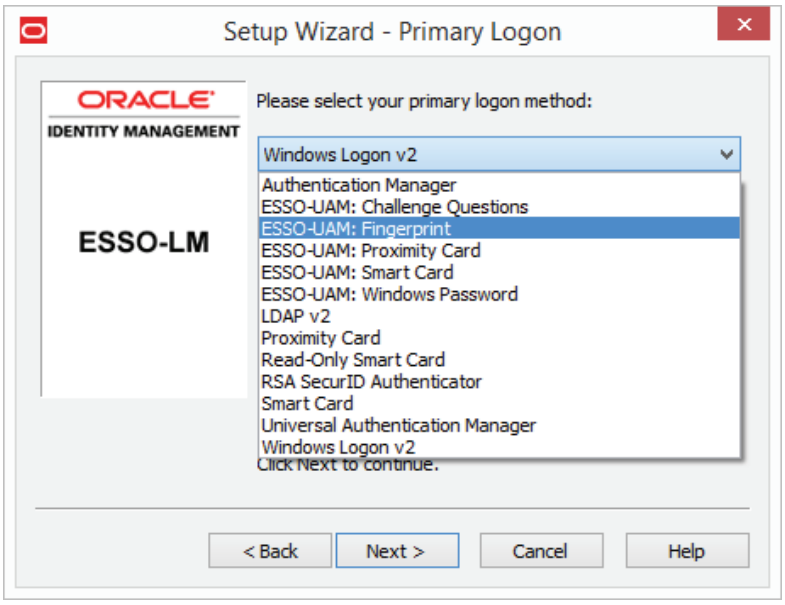
1. Click **Start** > **Programs** > **Oracle** > **Logon Manager** > **Logon Manager**. The First-Time Use wizard opens. Click **Next** on the first screen of the wizard.



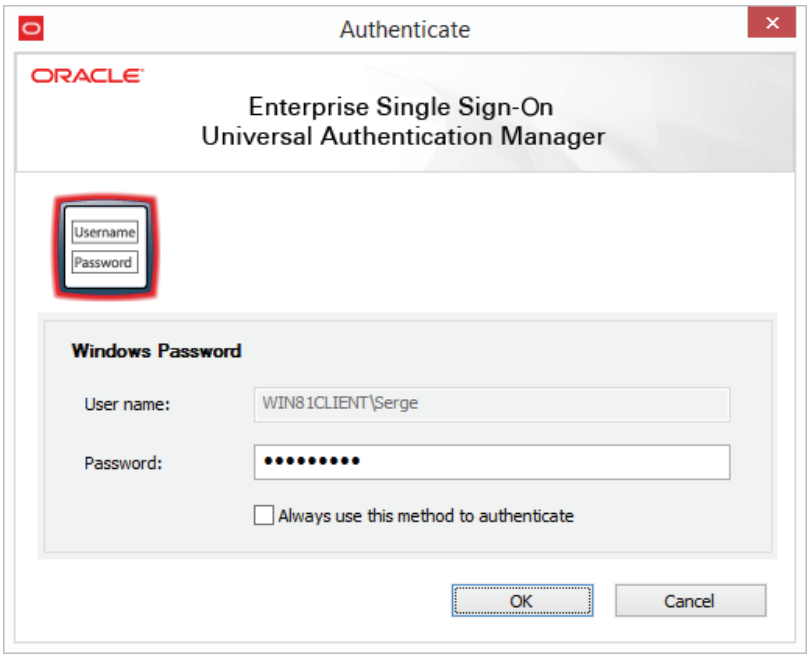
2. If prompted, authenticate to Logon Manager and click **OK**, then click **Next**.
3. Select the desired Universal Authentication Manager logon method from the list of available primary logon methods, then click **Next**. If a method does not appear in the list, your administrator has chosen not to enable it.

   If you select one of the individual Universal Authentication Manager logon methods (shown as E**SSO-UAM:** *logon method name* in the drop-down list), only that single method will be available for authentication to Logon Manager; if you have not yet enrolled with that method, you will be prompted to enroll the first time Logon Manager requests authentication.

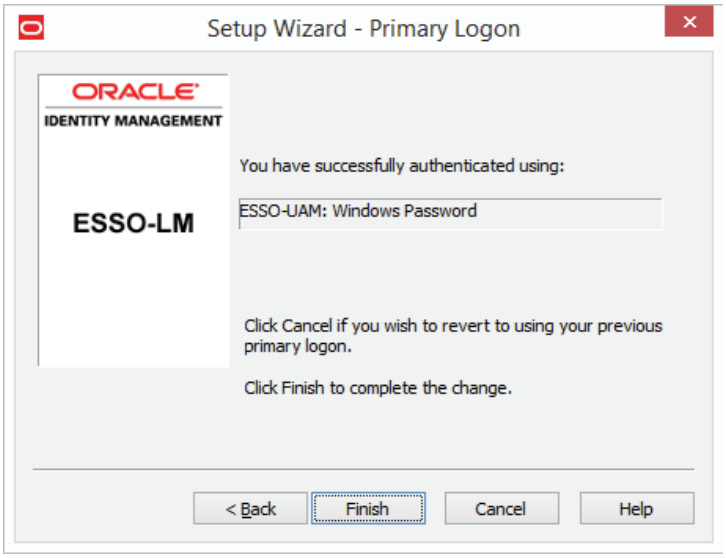
   If you select **Universal Authentication Manager** (the multi-method Universal Authentication Manager authenticator), you will be able to use any Universal Authentication Manager logon method with which you have previously enrolled. If you have not yet enrolled any logon methods with Universal Authentication Manager, you will be prompted to authenticate with your Windows password.



4. Authenticate with the logon method you used to log on to Windows (a Windows password or other logon method).



5. Logon Manager displays a message informing you that it is ready for use. The Universal Authentication Manager logon method you selected is now configured as your primary logon method for Logon Manager. Click **Finish** to complete the wizard.

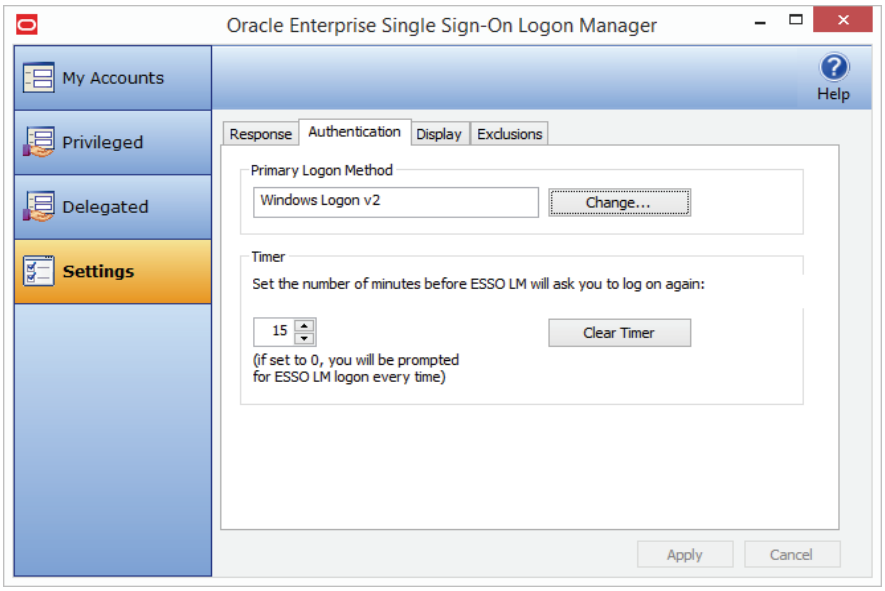


5.3.2 Configuring a Universal Authentication Manager Logon Method as the Primary Logon Method Using Logon Manager

To configure a Universal Authentication Manager logon method as the primary logon method for Logon Manager:

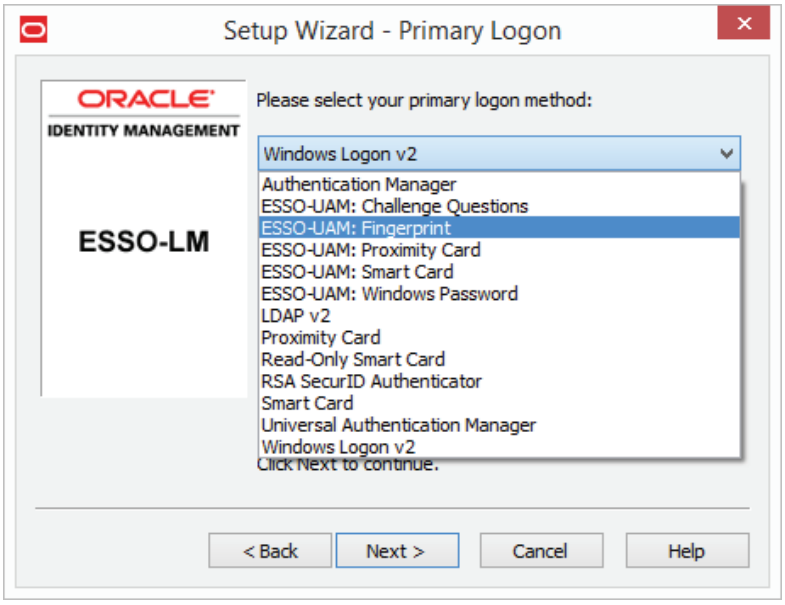
1. Click **Start** > **Programs** > **Oracle** > **Logon Manager** > **Logon Manager**. The Logon Manager icon appears in the system tray. Launch Logon Manager.

2. Select **Settings**, then click the **Authentication** tab.



3. In the Primary Logon Method section, click **Change…**. The Primary Logon Setup Wizard opens. Click **Next** to proceed.
4. Enter your Windows password or authenticate to your currently enrolled logon method when prompted.
5. From the list of available primary logon methods, select the desired Universal Authentication Manager logon method. (For an explanation of the available logon methods, and the difference between the individual logon methods vs. the multi-method **Universal Authentication Manager** option, see Integrating with Logon Manager.)

   Click **Next**.



6. The Universal Authentication Manager authentication dialog is displayed; enter your Windows password or authenticate with another enrolled logon method.

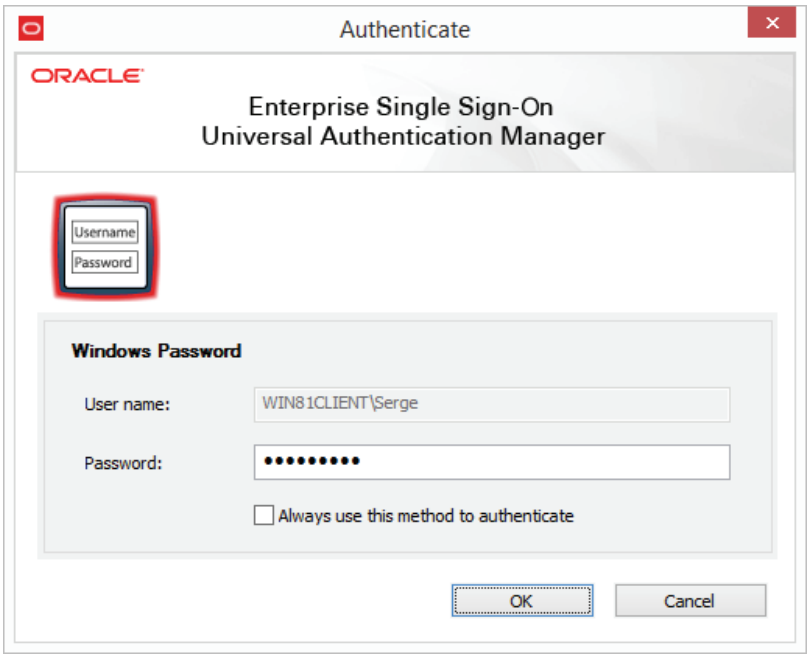
5.3.3 Authenticating With Universal Authentication Manager When Prompted by Logon Manager

Several Logon Manager events will trigger Universal Authentication Manager to prompt you for authentication. When this occurs, the standard Universal Authentication Manager authentication process begins. You can choose to authenticate with any logon methods that are enabled for your account. For details on Logon Manager events that will trigger Universal Authentication Manager to prompt you for authentication, see the Logon Manager User Guide.

Note: If you have not yet enrolled any logon methods in Universal Authentication Manager and Logon Manager prompts you for authentication, one of the following scenarios applies:

- If your administrator has configured Logon Manager to use an individual Universal Authentication Manager logon method authenticator (shown as **ESSO-UAM:** *logon method name* in the Primary Logon Method drop-down list in Logon Manager) as its primary logon method, you will be prompted to enroll with that method the first time Logon Manager prompts you to authenticate. In such case, you cannot skip enrollment; you must enroll or you will not be able to use Logon Manager.
- If your administrator has chosen to use the multi-method Universal Authentication Manager authenticator (shown as **Universal Authentication Manager** in the **Primary Logon Method** drop-down list in Logon Manager), you will be prompted to authenticate with your Windows password.

When authentication is required, you are prompted by the Universal Authentication Manager authentication screen. This screen may vary depending upon the logon methods you have enrolled and will reflect the logon method you last used to authenticate to Universal Authentication Manager. For example, if you last authenticated to Universal Authentication Manager with your Windows password, the screen will appear as follows:



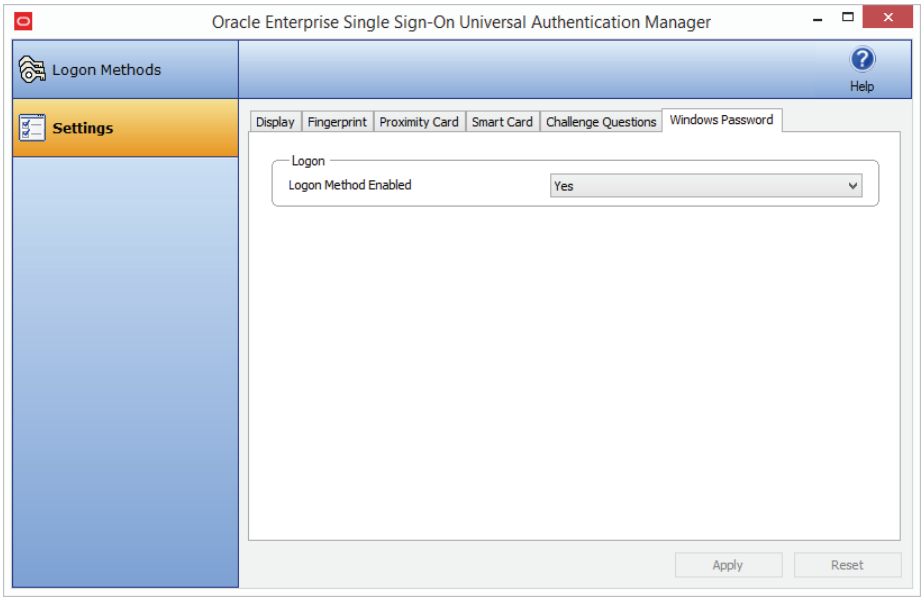
Enter your Windows password or use another enrolled logon method to continue with authentication. After you have authenticated, you can continue working with Logon Manager.

5.4 Logon Method Enabled

The Logon Method Enabled policy allows administrators or users to disable an installed Universal Authentication Manager authenticator.

This policy applies to all authenticators individually and each authenticator will have its own value.

- In enterprise mode, the Logon Method Enabled policy setting is an Administrative policy only. This means that the policy will never appear in the Universal Authentication Manager settings.
- In the local client mode, the Logon Method Enabled policy setting is an end-user policy setting. You can manage the policy setting right from the Settings tab in the Universal Authentication Manager :



5.4.1 Windows Password Exception

Universal Authentication Manager automatically enables Windows Password authentication if no other logon methods are enrolled.

This is a "built-in" behavior that requires no configuration. For example, if you've disabled Windows Password via the Logon Method Enabled policy, a password will be allowed for logon, re-authentication and unlock, if you are not enrolled in at least one other method.

Note: If you are enrolled in one or more other methods, but those methods (and password) are all disabled, you will be locked out. The Administrator will have to correct this by re-configuring the Logon Method Enabled policy in the Universal Authentication Manager Administrative Console.

5.4.1.1 Logon Method Enabled Rules

If the Logon Method Enabled is configured to **No** for a logon method:

- The logon method is displayed in the Universal Authentication Manager Logon Methods tab with a status of DISABLED. The only action you are allowed to perform is a Delete, as long as you are enrolled using the logon method. No other enrollment actions (Enroll or Modify) are available.
- In enterprise mode, the logon method appears in the Universal Authentication Manager Settings tab. All policy settings are disabled, and the Logon Method Enabled policy setting is not displayed.
- In local mode, the logon method appears in the Universal Authentication Manager Settings tab. The Logon Method Enabled policy setting is enabled, and all other policy settings are disabled.
- You are not allowed to log onto or enroll on the workstation using that logon method. If you attempt to log on with a disabled logon method, you will receive an error message.

- You are not allowed to re-authenticate using the logon method and will not see the logon method as an authentication option. A password authentication is enabled for Logon, Unlock, and Re-authentication, if you are not enrolled in any other method.

5.4.2 Configuring Universal Authentication Manager to Lock a Workstation

Note: Locking a workstation using Universal Authentication Manager is only supported with proximity cards and smart cards.

From the Settings page, you can configure Universal Authentication Manager to lock your workstation when you remove a token, for example, when you remove a smart card or "tap out" a proximity card (that is, when you tap the proximity card on the card reader long enough for it to be detected). If you set the Removal Action setting to "Lock Workstation" (which is the default setting), the workstation will lock when you perform a removal action.

A change to the Removal Action will not take effect until the subsequent removal. For example, if you log on to Windows with a token, launch Universal Authentication Manager, and change the removal action for that token from Lock Workstation to Force Logoff, your workstation will still lock when you remove the token; the Force Logoff action will occur the following time you remove the token.

Note: The removal action will only be activated for the same token you used to log on to the workstation. For example, if you log on using your Windows password but try to lock the workstation by "tapping out" with a proximity card, the workstation will not lock.

The removal action will not be triggered if the Universal Authentication Manager Client Application or the re-authentication dialog is open.

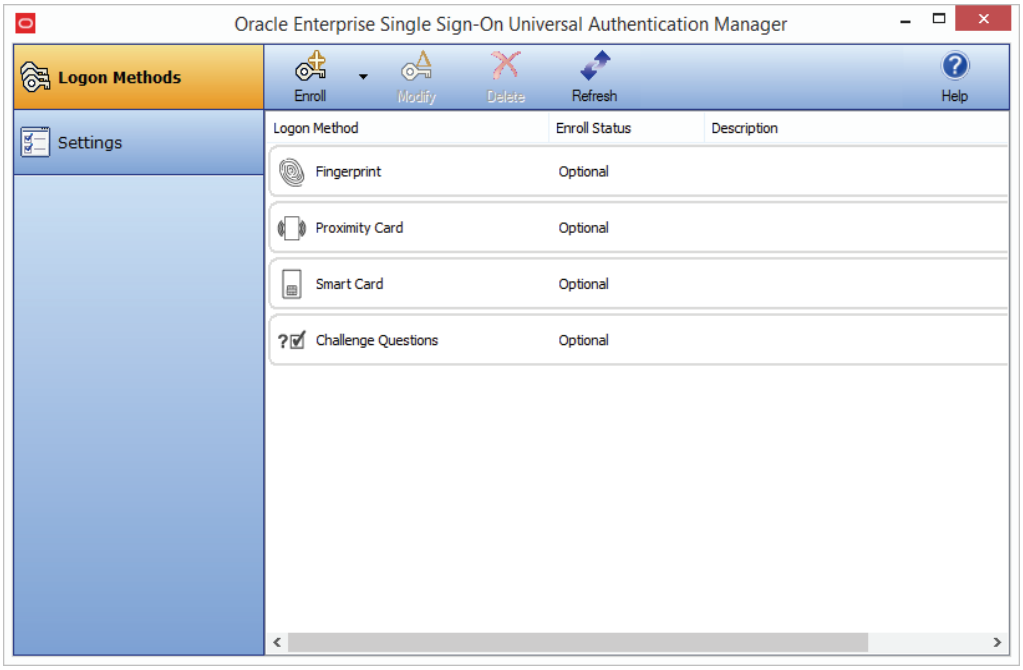
For more information about Removal Action and other settings, see Settings.

5.5 Using Universal Authentication Manager

To start Universal Authentication Manager:

1. Click **Start**, then **Programs**.
2. Point to **Oracle**, then **Universal Authentication Manager**.
3. Click **Universal Authentication Manager.**

Universal Authentication Manager opens.



The Logon Methods panel displays the installed logon methods (authenticators) available to you, and allows you to enroll a logon method, as well as modify and delete existing enrollments. For faster access, the **Enroll**, **Modify**, and **Delete** controls are also available in a context menu accessible by right-clicking the desired logon method in the list. From this panel you can also do the following:

- Managing Enrolled Credentials.
- Changing Your Universal Authentication Manager PIN associated with a fingerprint, smart card, or proximity card.
- Refreshing your account to synchronize changes made by your administrator.
- Accessing the help system.

Your administrator has made available one or more of the following logon methods:

- Fingerprints
- Proximity Cards
- Smart Cards
- Challenge Questions

The controls on this panel are:

Icon	Label	Purpose
	**Enroll**	Enrolls a new credential. When you click **Enroll**, a drop-down list of available logon methods appears; from this menu, select the logon method you wish to use.
	**Modify**	Modifies the selected enrollment. For some enrollment methods, you can modify properties of your credential. For example, if you are authenticating with a proximity card that has an associated PIN code, click **Modify** to change your PIN.

Icon	Label	Purpose
	**Delete**	Deletes an enrolled credential. If you do not have permission to delete the enrolled credential, you will receive an error message stating so.
	**Refresh**	Synchronizes with the Universal Authentication Manager repository and updates any policy settings that were changed by your administrator (in Enterprise client mode).

5.5.1 Shortcut Keys

You can accomplish tasks and access features in Universal Authentication Manager more quickly using the following keyboard shortcuts:

- To view logon methods: (Alt + L).
- To view settings: (Alt + S).
- To enroll credentials: (Alt + E).
- To modify credentials: (Alt + M).
- To delete credentials: (Alt + D).
- To refresh policies or settings: (F5).
- To view help: (F1).

5.5.2 Enrolling Credentials

Credentials can be enrolled manually, or you may be prompted to enroll credentials during Windows logon, or upon launching the Universal Authentication Manager Client Application. Your administrator may also set a grace period for required enrollment.

Click one of the links below to see instructions for enrolling your selected logon method:

- To enroll a Fingerprint, see:
  - Enrolling a Fingerprint at Windows Logon
  - Enrolling a Fingerprint When Launching Universal Authentication Manager
  - Enrolling a Fingerprint Manually
- To enroll a Proximity Card, see:
  - Enrolling a Proximity Card at Windows Logon
  - Enrolling a Proximity Card when Launching Universal Authentication Manager
  - Enrolling a Proximity Card Manually
- To enroll a Smart Card, see:
  - Enrolling a Smart Card at Windows Logon
  - Enrolling a Smart Card when Launching Universal Authentication Manager
  - Enrolling a Smart Card Manually
- To enroll Challenge Questions, see:

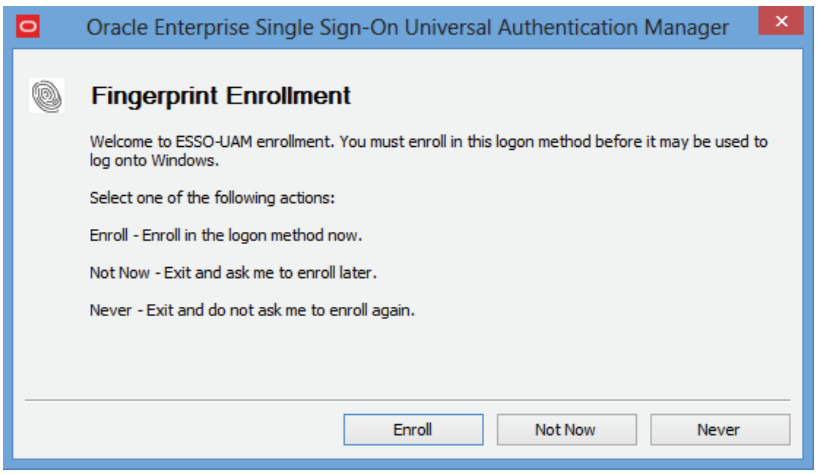
- Enrolling Challenge Questions at Windows Logon
- Enrolling Challenge Questions when Launching Universal Authentication Manager
- Enrolling Challenge Questions Manually

5.5.2.1 Ways to Enroll

Enrollment can occur in one of the following ways:

- Prompted Enrollment
- Prompted with a Grace Period
- Manual Enrollment

5.5.2.1.1 Prompted Enrollment After Universal Authentication Manager is installed and you restart your machine, you will be prompted (by default) to enroll in one or more logon methods when you log on to Windows.



If multiple logon methods are installed, you will be consecutively prompted to enroll each logon method. You may choose one of the following options when prompted (depending on your configuration):

- **Enroll.** Enroll in the logon method now.
- **Not Now.** Skip this enrollment and ask me to enroll later.
- **Never.** Exit and do not ask me to enroll again.

5.5.2.1.2 Grace Period Your administrator may have set an enrollment grace period which allows you to defer a required enrollment for a configured number of days. If a grace period is set, the automatic enrollment screen informs you that your administrator requires you to eventually enroll this logon method before you can log on to Windows.

- The **Never** option is not available.
- If you click **Not Now**, a message appears stating how many days remain within the grace period.

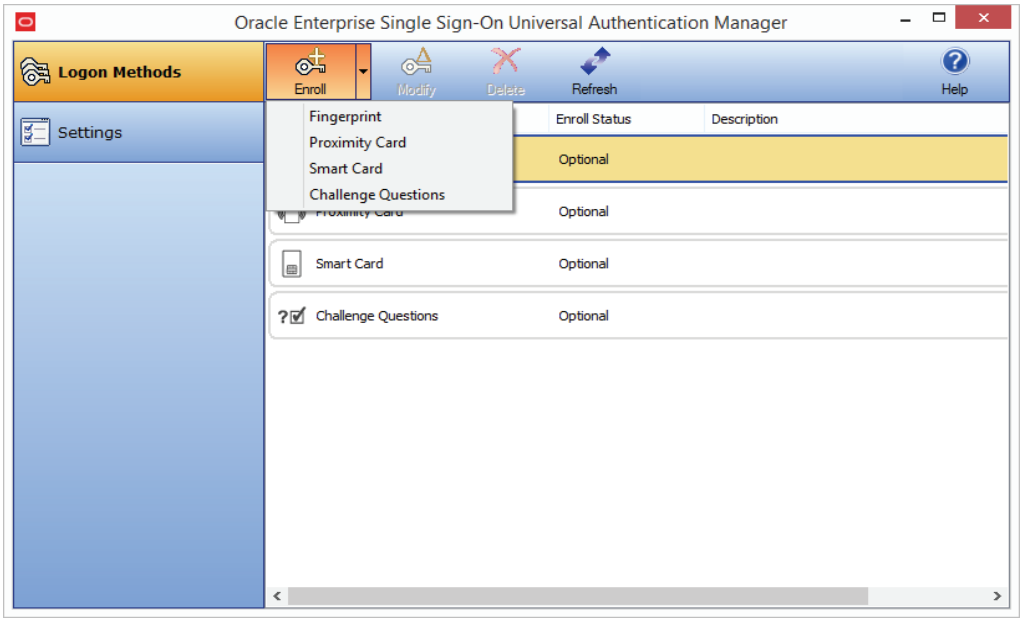
You must enroll this logon method within the configured number of days. Once the Grace Period has ended, you will be required to enroll in this logon method before logging on to Windows.

5.5.2.1.3 Manual Enrollment If prompted enrollment is configured to optional or required with a grace period, you will be prompted to enroll when you launch the Universal Authentication Manager.

If you choose not to enroll a logon method when you log on to Windows, you can launch Universal Authentication Manager and manually enroll a logon method using one of the following enrollment procedures:

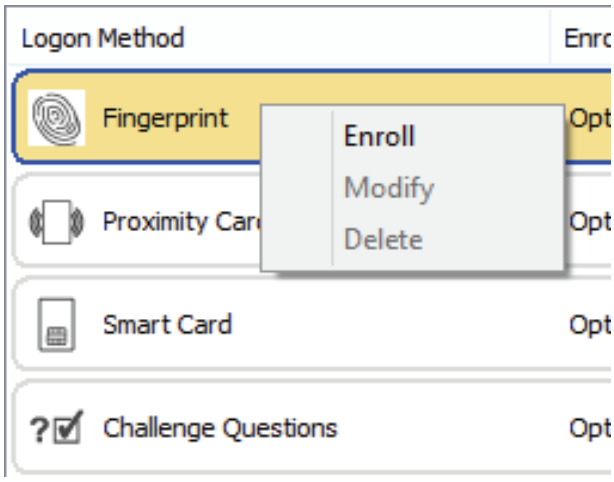
- Click the **Enroll** button and choose a logon method from the drop-down list that appears.

  Enter your Windows password (or authenticate with a previously enrolled logon method) when prompted. You are instructed to follow enrollment steps based on the type of authenticator you are using. For example, if you are enrolling a smart card as an authenticator, you are prompted after entering your Windows password to insert the smart card into the card reader and enter the PIN. A confirmation message then informs you that your card is enrolled.



- Right-click a displayed logon method and select **Enroll**.

  Enter your Windows password when prompted (or authenticate with a previously enrolled logon method) and follow the enrollment steps that appear. (Enrollment steps will vary depending on the type of authenticator you are using.)

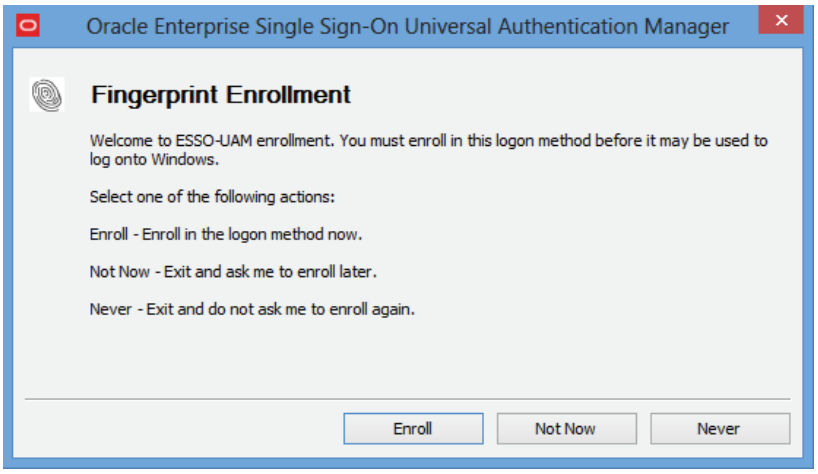


- Double-click on a logon method that is not yet enrolled. Enter your Windows password when prompted (or authenticate with a previously enrolled logon method) and follow the enrollment steps that appear. (Enrollment steps will vary depending on the type of authenticator you are using.)

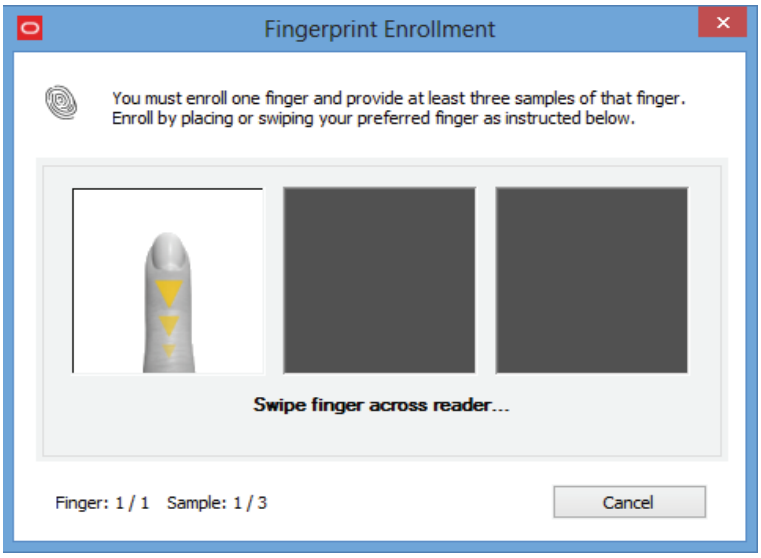
5.5.3 Enrolling a Fingerprint at Windows Logon

When you log on to your workstation, you are automatically prompted to enroll installed logon methods. If one of those methods is Fingerprint, you will be prompted to enroll it.

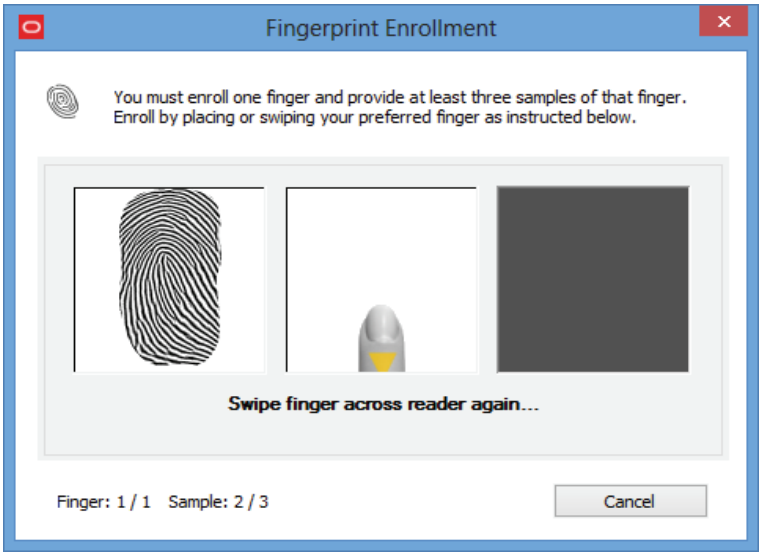
1. Click **Enroll** to enroll a fingerprint.



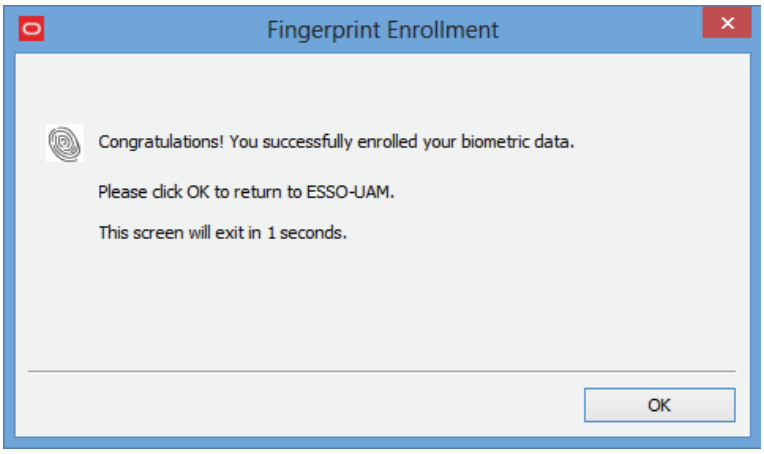
2. If your system is configured to require a PIN with the fingerprint, enter and confirm a PIN.
3. Enroll at least one fingerprint sample. The number of fingerprint samples is configured by your administrator. Enroll by placing or swiping your preferred finger.



4. Swipe your finger on the reader again and repeat as many times as requested.



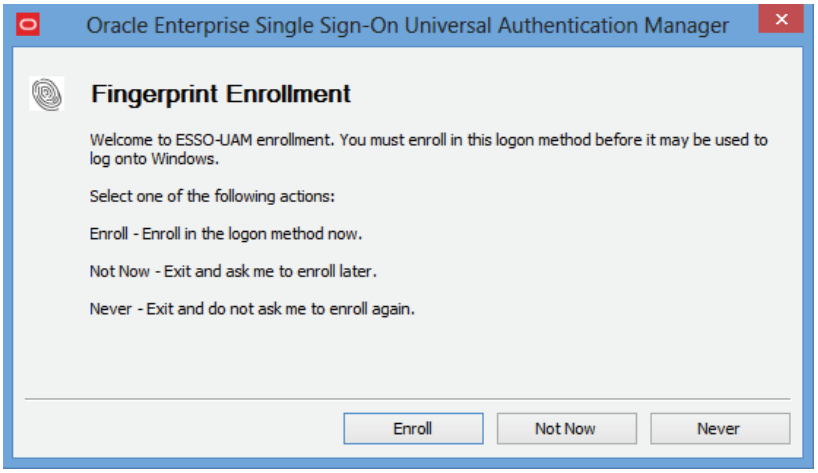
5. After all fingerprint samples have been enrolled, a message informs you that the data is processing. Wait until it completes.
6. When enrollment is complete, a message confirms that your biometric data is enrolled. Click **OK** to exit and resume log on to Windows. If other Universal Authentication Manager logon methods are installed, you may be prompted to enroll in additional methods.



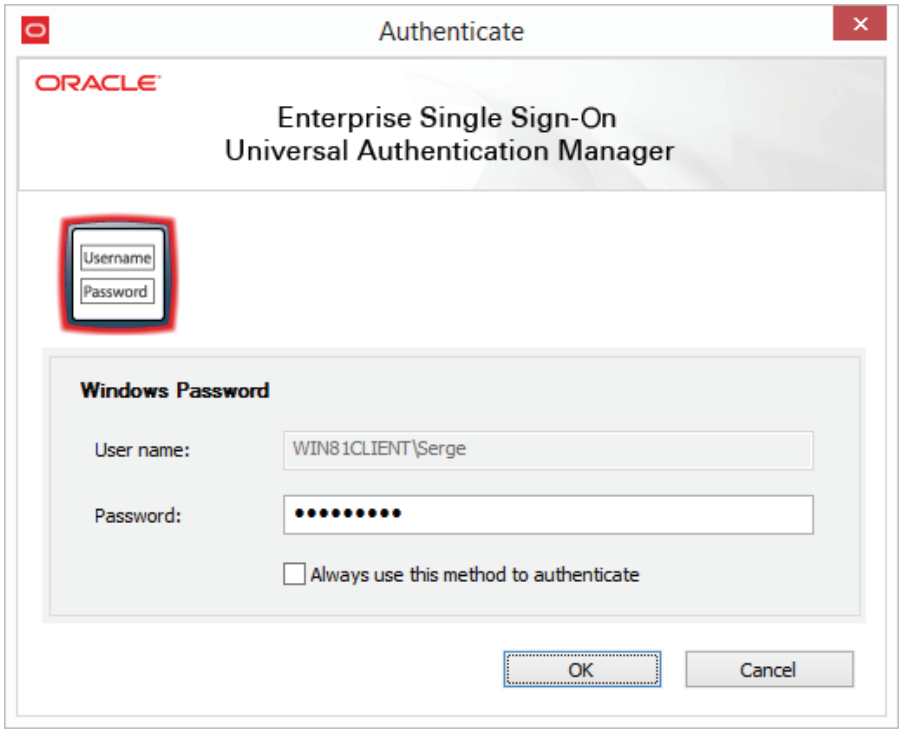
5.5.4 Enrolling a Fingerprint When Launching Universal Authentication Manager

When you launch Universal Authentication Manager, you are automatically prompted to enroll installed logon methods (if they are not already enrolled). If one of those methods is a fingerprint, you will be prompted to enroll it.

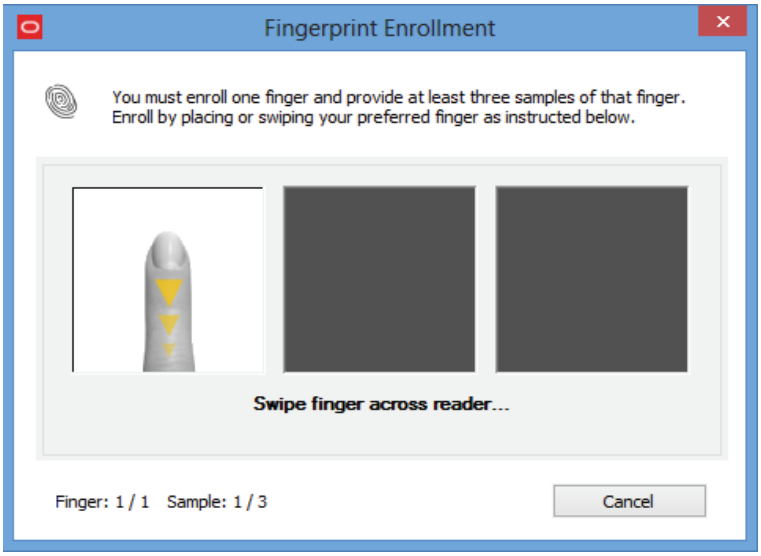
1. Click **Enroll** to enroll a fingerprint.



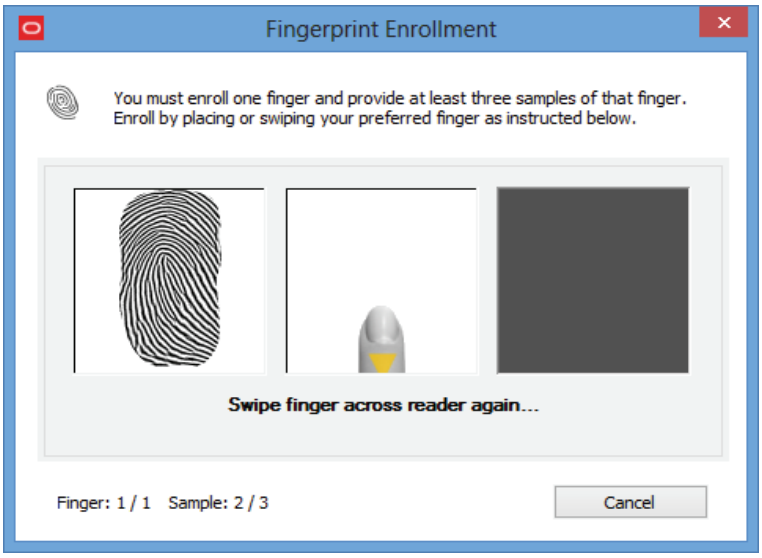
2. Authenticate using a previously enrolled logon method or your Windows password.



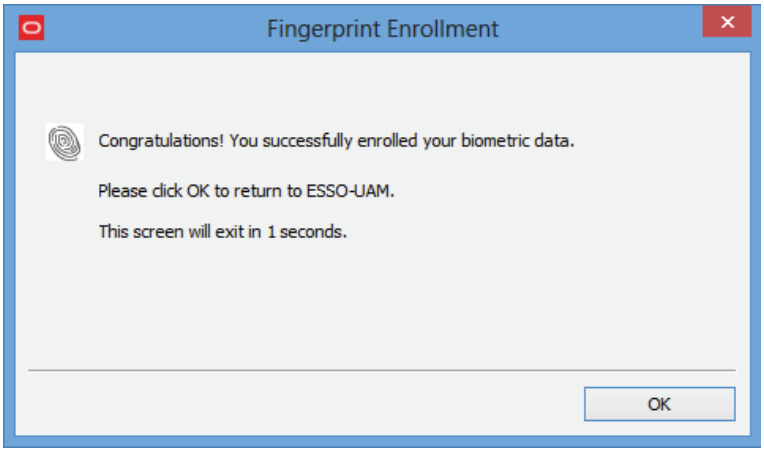
3. If your system is configured to require a PIN with the fingerprint, provide a PIN when prompted.
4. Enroll at least one fingerprint sample. The number of fingerprint samples is configured by your administrator. Enroll by placing or swiping your preferred finger.



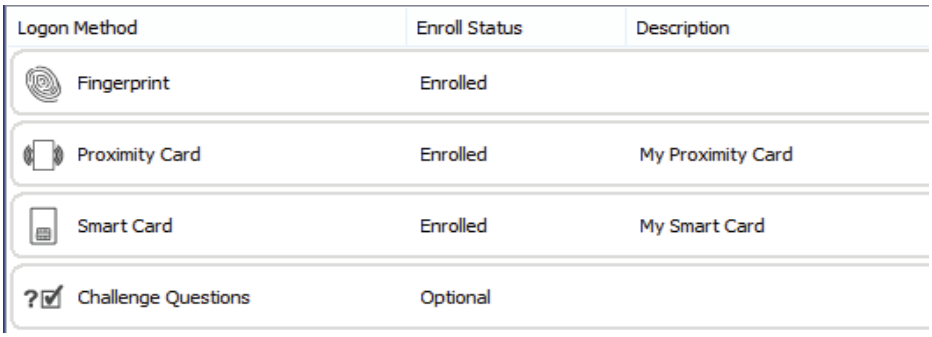
5. Swipe your finger on the reader again and repeat as many times as requested.



6. After all fingerprint samples have been enrolled, a message informs you that the data is processing. Wait until it completes.
7. When enrollment is complete, a message confirms that your biometric data is enrolled. Click **OK** to return to Universal Authentication Manager.



8. The Enroll Status column shows a status of **Enrolled**.



5.5.5 Enrolling a Fingerprint Manually

To enroll a fingerprint manually:

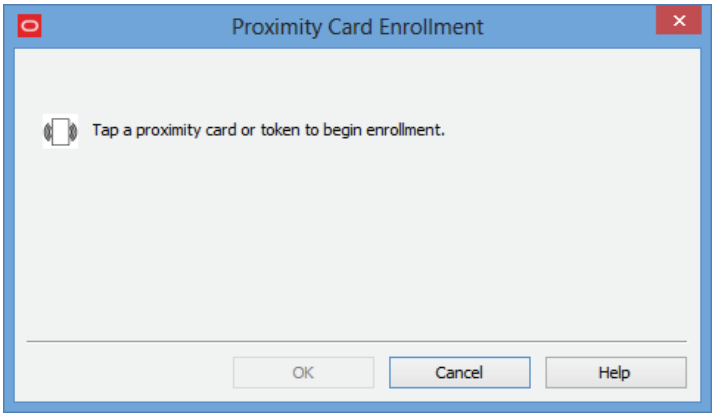
1. Launch Universal Authentication Manager.
2. Click **Enroll** in the Logon Methods toolbar and select **Fingerprint** from the drop-down list; or right-click in the highlighted Fingerprint row and select **Enroll**; or double click in the Fingerprint row.
3. Authenticate with a previously enrolled logon method or your Windows password.
4. Follow the steps to enroll your fingerprints (see detailed instructions in the previous section).
5. A message confirms that you have successfully enrolled your fingerprints.
6. The Enroll Status column shows a status of **Enrolled**.

5.5.6 Enrolling a Proximity Card at Windows Logon

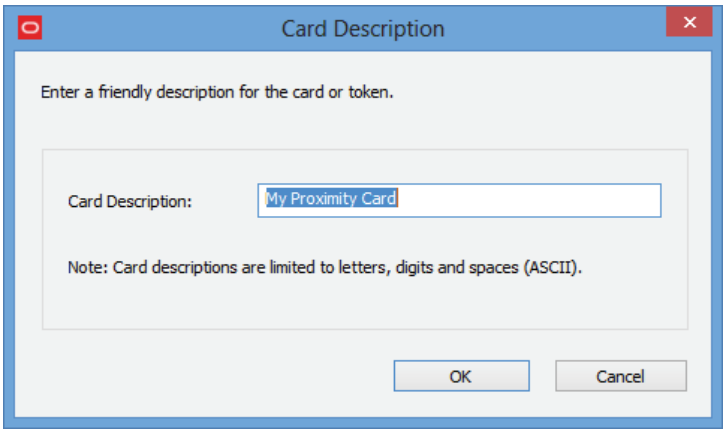
When you log on to your workstation, you are automatically prompted to enroll installed logon methods. If one of those methods is a proximity card, you will be prompted to enroll it.

1. Click **Enroll** to enroll a proximity card.

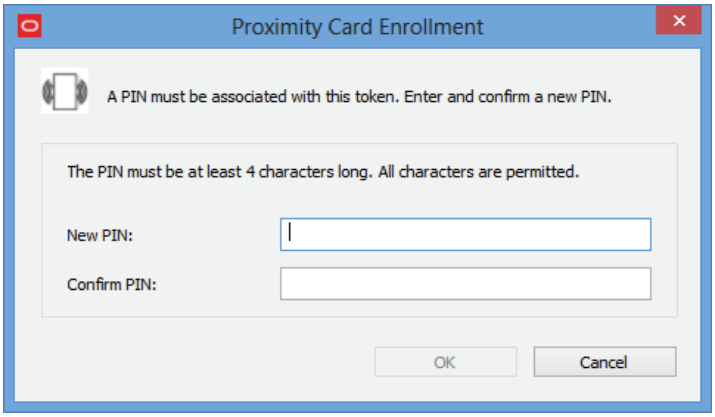
2. Hold your card near the reader until Universal Authentication Manager detects it.



3. Enter a meaningful description for the proximity card and click **OK**.



4. If your system is configured to require a PIN with a proximity card, enter and confirm a PIN, then click **OK**.

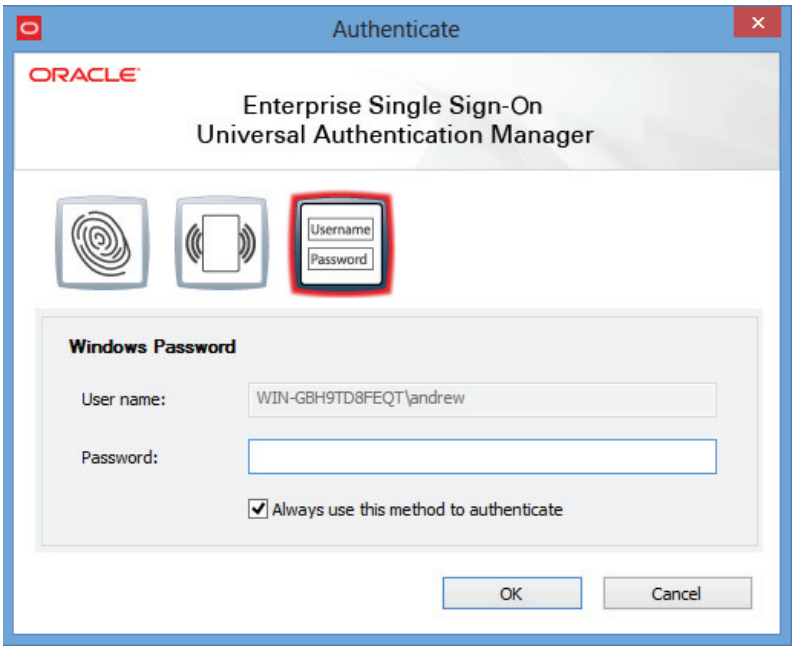


5. When enrollment is complete, a message confirms that your card is enrolled. Click **OK** to exit and resume logon to Windows. If other logon methods are installed, you may be prompted to enroll in additional methods.

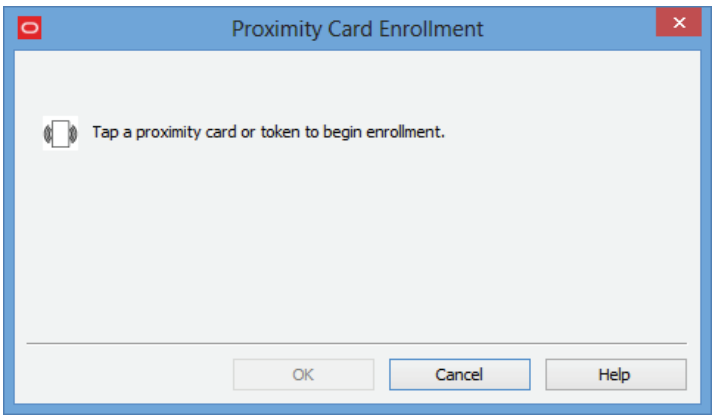
5.5.7 Enrolling a Proximity Card when Launching Universal Authentication Manager

When you launch Universal Authentication Manager, you are automatically prompted to enroll installed logon methods. If one of those methods is a proximity card, you will be prompted to enroll it.

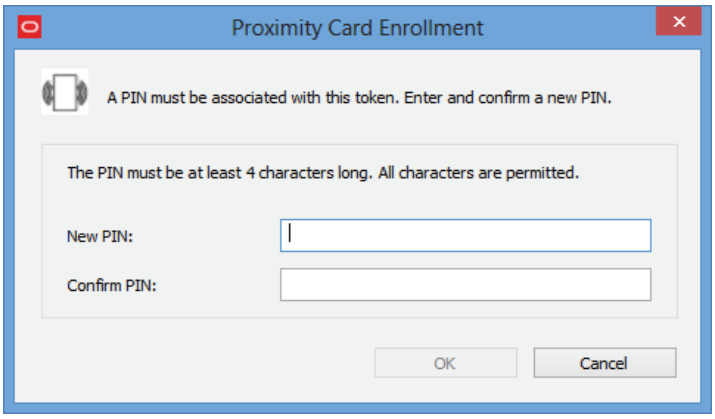
1. Click **Enroll** to enroll a proximity card. You are prompted to authenticate to continue. You can authenticate through any of the available authentication methods.



2. Hold your card near the reader until Universal Authentication Manager detects it.

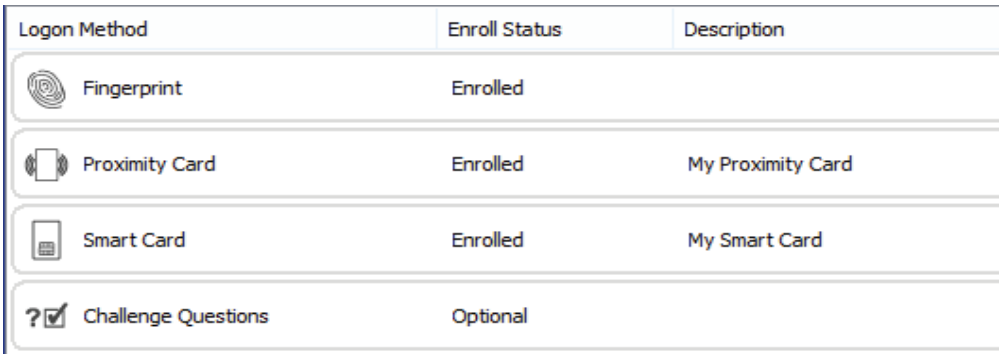


3. If your system is configured to require a PIN with a proximity card, enter and confirm a PIN, then click **OK**.



4. A message confirms that you have successfully enrolled your card. Click **OK** to return to Universal Authentication Manager.

5. The Enroll Status column shows a status of **Enrolled**.



5.5.8 Enrolling a Proximity Card Manually

To enroll a proximity card manually:

1. Launch Universal Authentication Manager.
2. Click **Enroll** in the Logon Methods toolbar and select **Proximity Card** from the drop-down list; or right-click in the highlighted proximity card row and select **Enroll**; or double click in the proximity card row.

3. Authenticate with a previously enrolled logon method or your Windows password.
4. Hold your card near the reader until Universal Authentication Manager detects it.
5. If your system is configured to require a PIN with a proximity card, enter and confirm a PIN. (see detailed instructions in the previous section).
6. A message confirms that you have successfully enrolled your card. Click **OK** to return to Universal Authentication Manager.
7. The Enroll Status column shows a status of **Enrolled**.

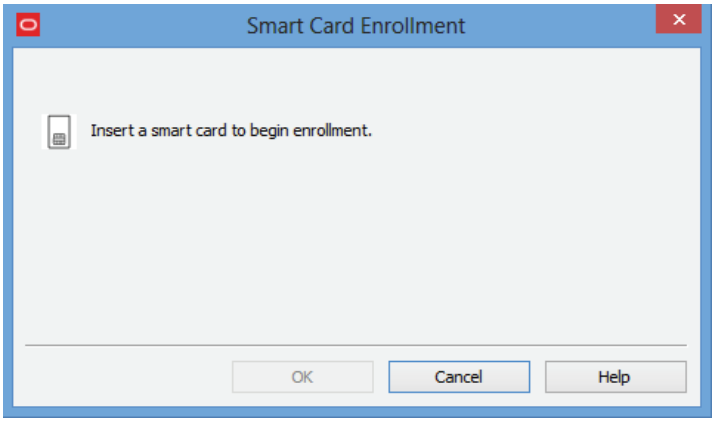
Note: It is best not to leave a proximity card resting on the card reader after using it to log on to, log off from, or lock a workstation. If you leave a proximity card on the reader, you may need to tap the card on the reader twice in order to log on to or unlock the workstation.

5.5.9 Enrolling a Smart Card at Windows Logon

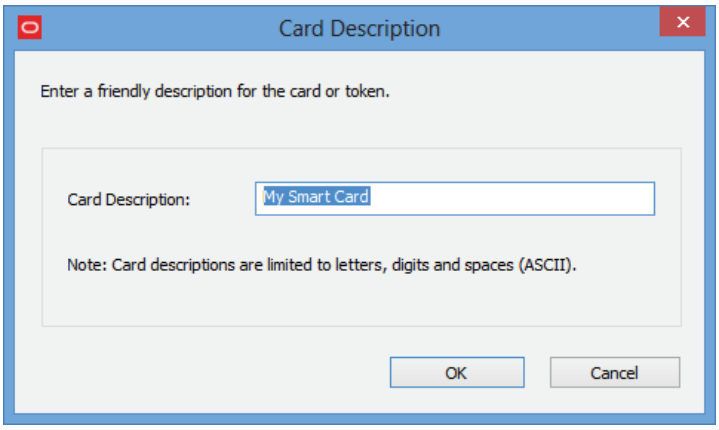
When you log on to your workstation, you are automatically prompted to enroll installed logon methods. If one of those methods is a smart card, you will be prompted to enroll it.

1. Click **Enroll** to enroll a smart card.

2. Insert your card into the reader.

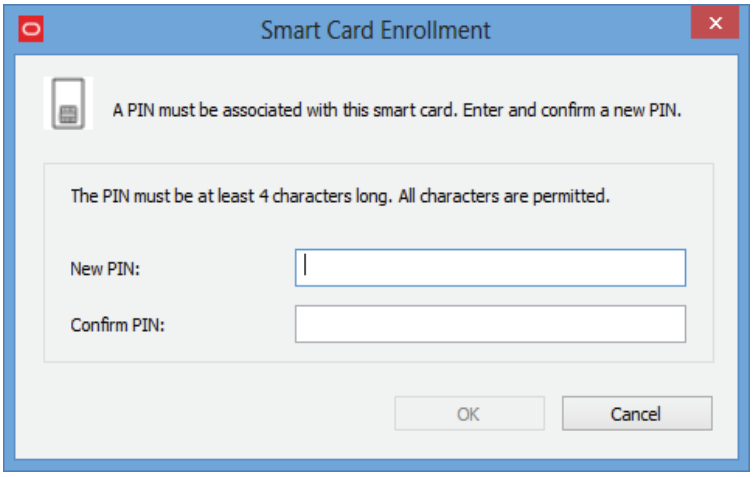


3. Enter a meaningful description for your smart card, then click **OK**.



4. Do one of the following:

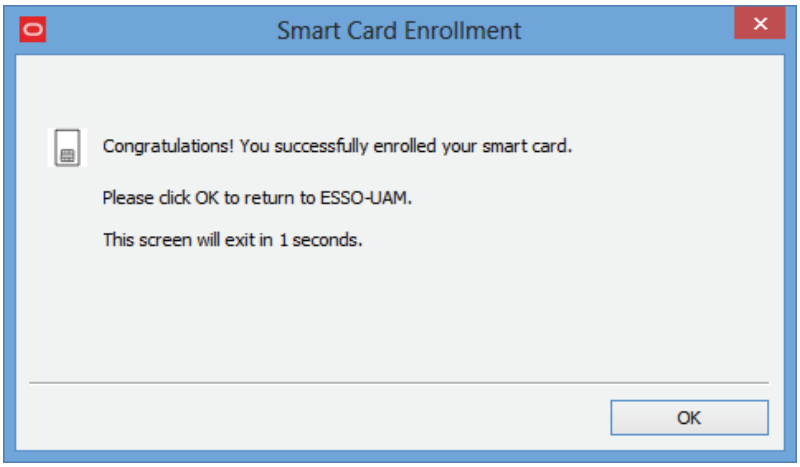
   - If the smart card logon method is configured to use the card's own PIN, enter the PIN and click **OK**.



   - If the smart card logon method is configured to use the Universal Authentication Manager PIN, enter and confirm a PIN of your choice, then click **OK**.

   For more information, see Smart Card Settings.

5. A message informs you that your card is being enrolled. When enrollment is complete, a message confirms that your card is enrolled. Click **OK** to exit and resume logon to Windows. If other Universal Authentication Manager logon methods are installed, you may be prompted to enroll in additional methods.

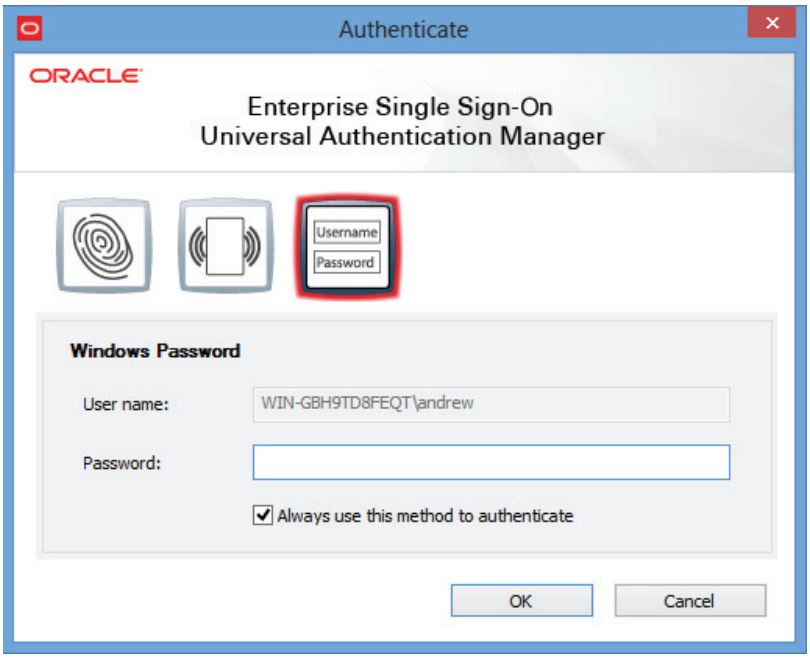


5.5.10 Enrolling a Smart Card when Launching Universal Authentication Manager

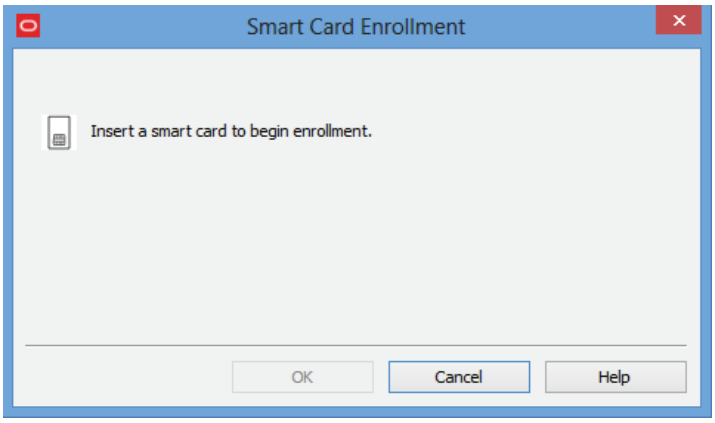
When you launch Universal Authentication Manager, you are automatically prompted to enroll installed logon methods (if they are not already enrolled). If one of those methods is a smart card, you will be prompted to enroll it.

1. Click **Enroll** to enroll a smart card.

2. Authenticate using a previously enrolled logon method or your Windows password.

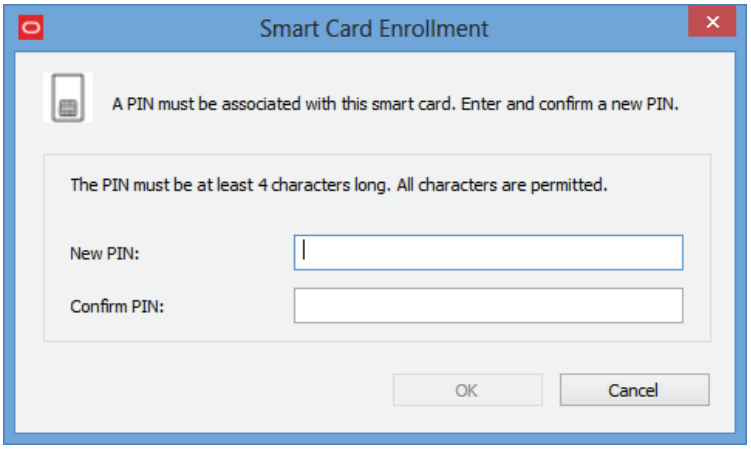


3. Insert your card into the reader.



4. Do one of the following:

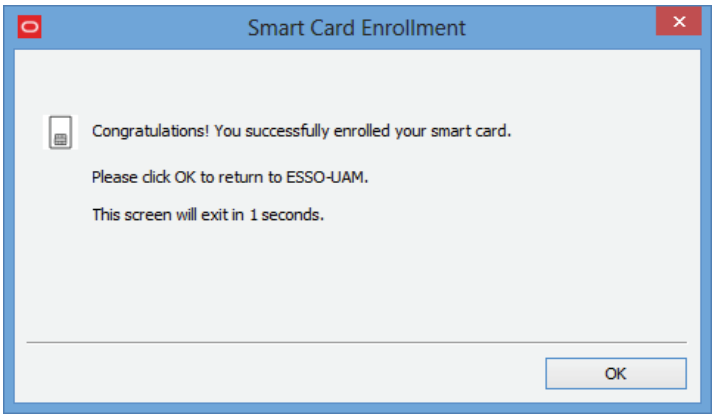
   - If the smart card logon method is configured to use the card's own PIN, enter the PIN and click **OK**.



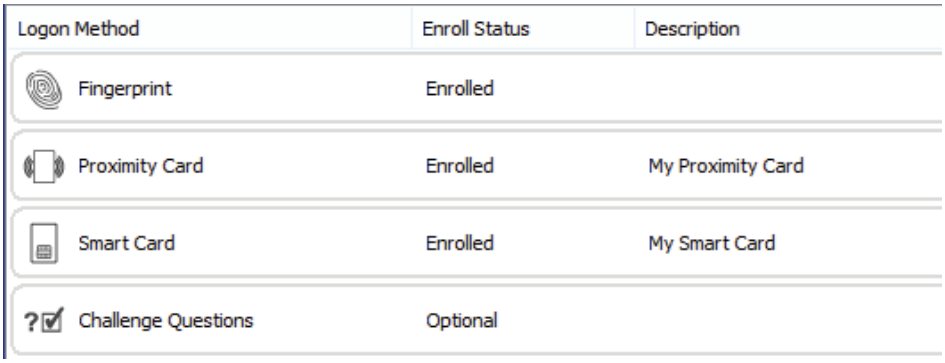
- If the smart card logon method is configured to use the Universal Authentication Manager PIN, enter and confirm a PIN of your choice, then click **OK**.

  For more information, see Smart Card Settings.

5. A message informs you that your card is being enrolled. When enrollment is complete, a message confirms that your card is enrolled. Click **OK** to return to Universal Authentication Manager.



6. The Enroll Status column shows a status of **Enrolled**.



5.5.11 Enrolling a Smart Card Manually

To enroll a smart card manually:

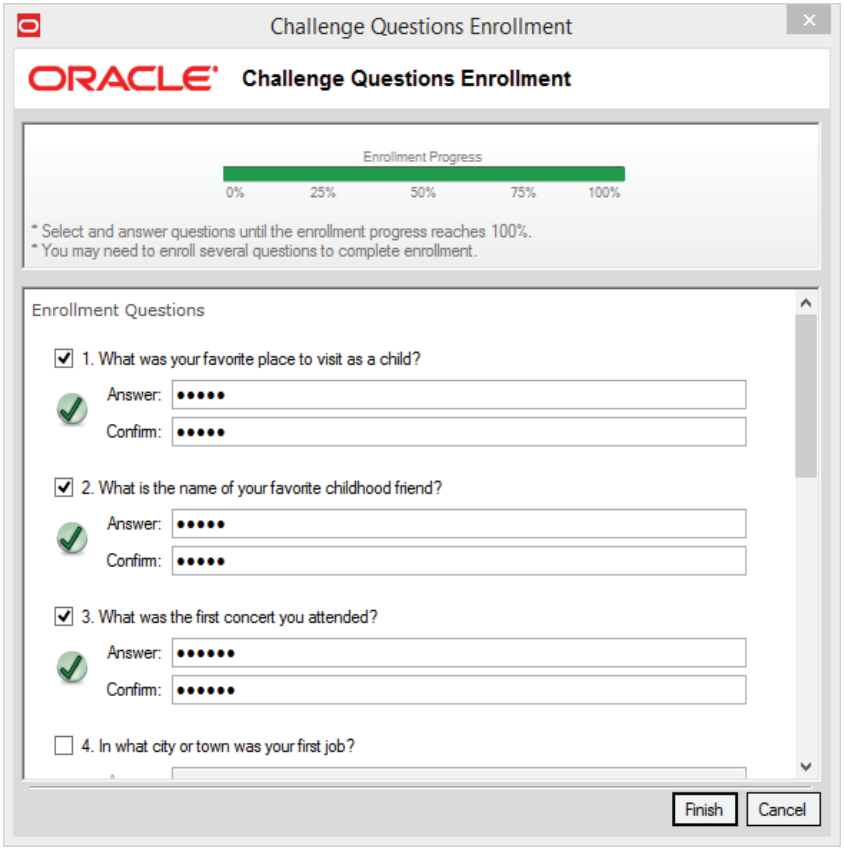
1. Launch Universal Authentication Manager.
2. Insert the card in the card reader.
3. Click **Enroll** in the Logon Methods toolbar and select **Smart Card** from the drop-down list; or right-click in the highlighted smart card row and select **Enroll**; or double click in the smart card row.
4. Authenticate with a previously enrolled method or your Windows password.
5. Enter the PIN associated with the card (see detailed instructions in the previous section).
6. Click **OK** to return to Universal Authentication Manager. A message confirms that you have successfully enrolled your card.
7. The Enroll Status column shows a status of **Enrolled**.

5.5.12 Enrolling Challenge Questions at Windows Logon

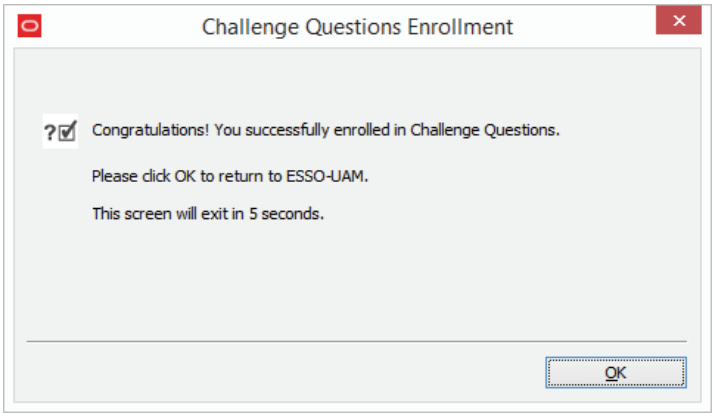
When you log on to your workstation, you are automatically prompted to enroll installed logon methods. If one of those methods is a challenge questions quiz, you will be prompted to enroll it.

1. Click **Enroll** to begin the enrollment process.

2. Select the challenge questions you want to enroll, then enter and confirm your answers.If your entries do not match, the mismatch is indicated in red; re-enter each incorrect answer and its confirmation to correct the mismatch. When you have selected and answered enough questions to satisfy the weight requirements configured by the administrator, the progress bar at the top of the window will show 100%. At this point you can select additional questions to fall back on in case you forget the answers to your main questions. When you have selected and answered all of the desired questions, click **Finish**.



3. When enrollment is complete, a message confirms that the Challenge Questions method is now enrolled. Click **OK** to dismiss the dialog.

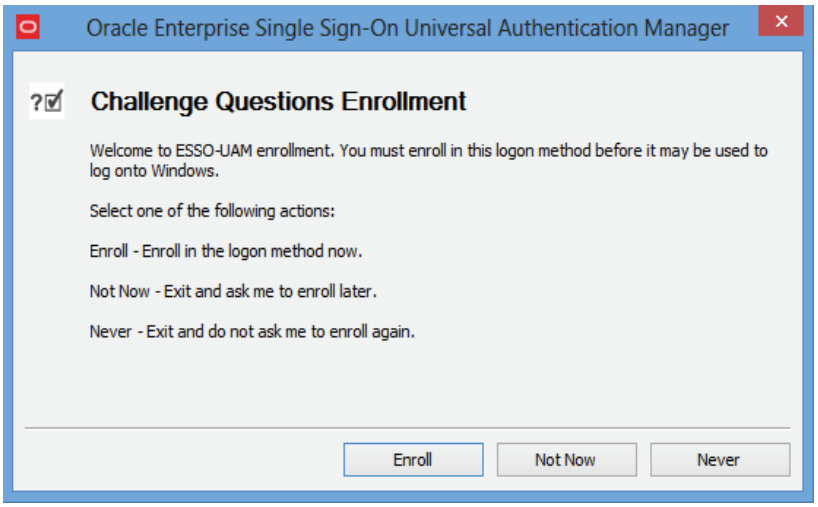


4. If other Universal Authentication Manager logon methods are installed, you may be prompted to enroll in additional methods.

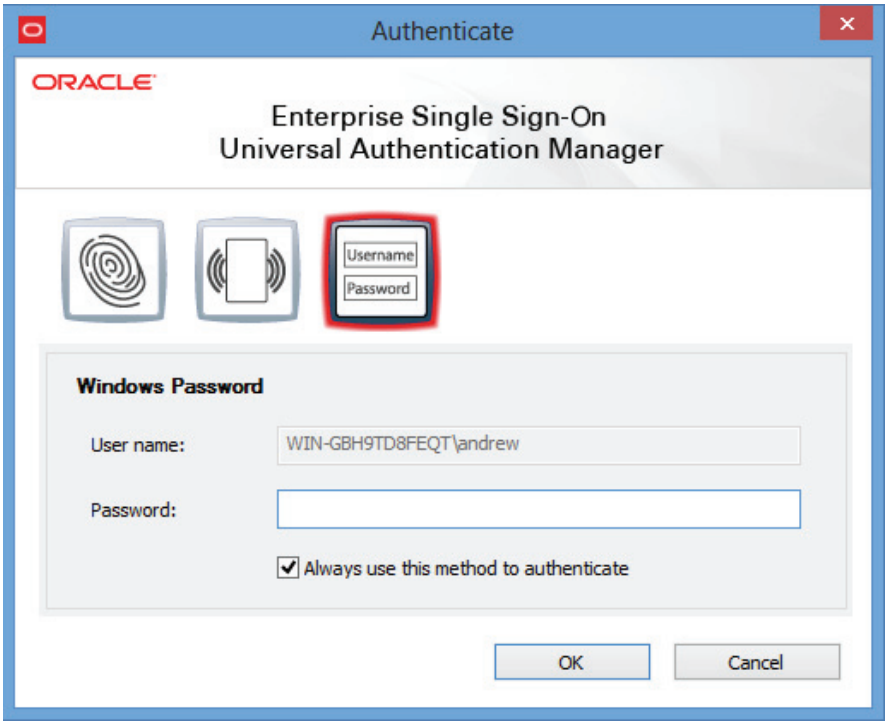
5.5.13 Enrolling Challenge Questions when Launching Universal Authentication Manager

When you launch Universal Authentication Manager, you are automatically prompted to enroll installed logon methods (if they are not already enrolled). If one of those methods is the challenge questions quiz, you will be prompted to enroll it.

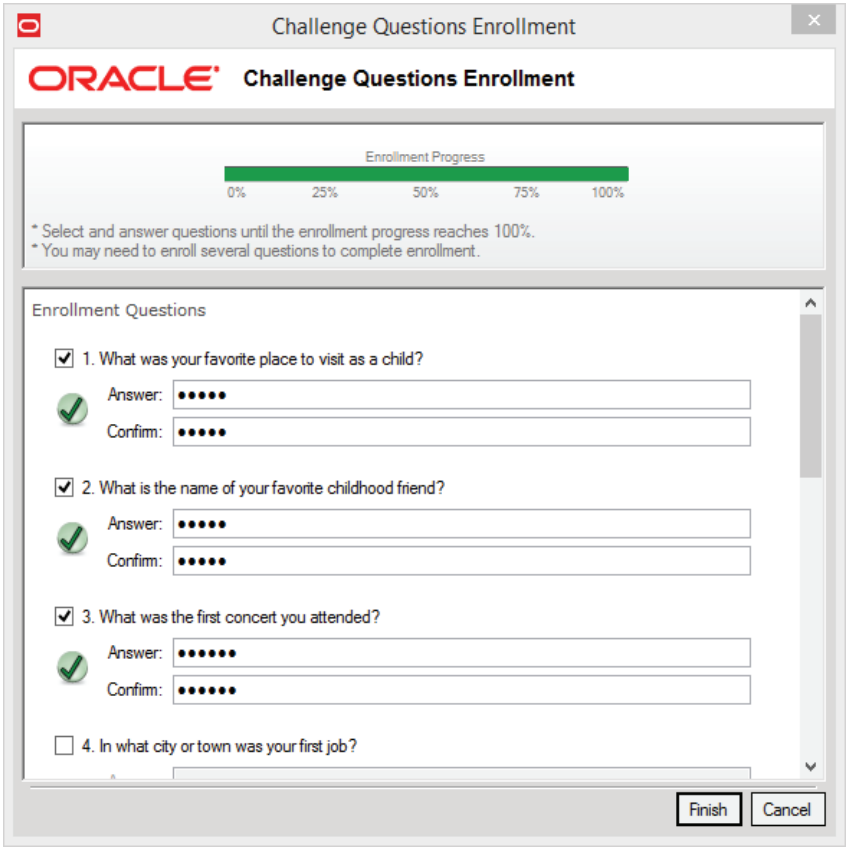
1. Click **Enroll** to begin the enrollment process.



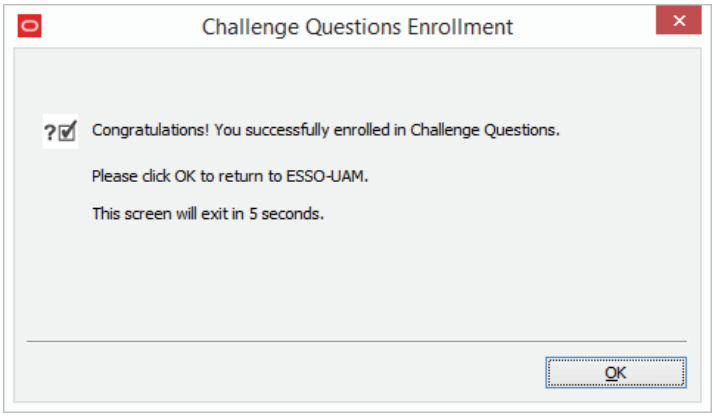
2. When prompted, authenticate to Universal Authentication Manager and click **OK** to proceed. You can authenticate through any of the available authentication methods (in the screen sample below, you can select to authenticate with either a Windows password or proximity card).



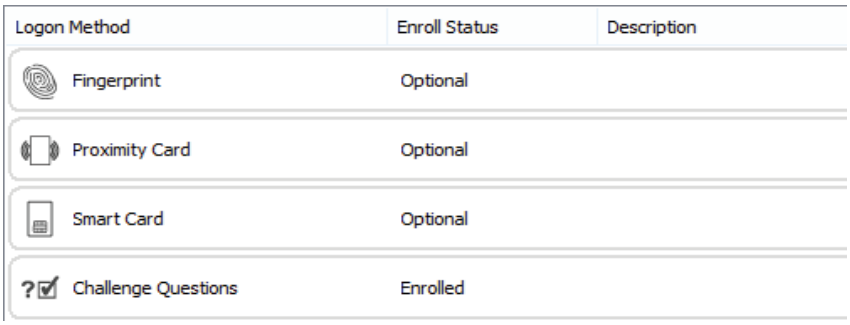
3. Select the challenge questions you want to enroll, then enter and confirm your answers.If your entries do not match, the mismatch is indicated in red; re-enter each incorrect answer and its confirmation to correct the mismatch. When you have selected and answered enough questions to satisfy the weight requirements configured by the administrator, the progress bar at the top of the window will show 100%. At this point you can select additional questions to fall back on in case you forget the answers to your main questions. When you have selected and answered all of the desired questions, click **Finish**.



4. When enrollment is complete, a message confirms that the Challenge Questions method is now enrolled. Click **OK** to dismiss the dialog.



5. The Enroll Status column shows a status of **Enrolled**.



5.5.14 Enrolling Challenge Questions Manually

To enroll challenge questions manually:

1. Launch Universal Authentication Manager.
2. Double-click the **Challenge Questions** method.
3. (Optional) If the Challenge Questions method's status is **Enrolled** and you want to replace the current enrollment with a new one, click **Re-Enroll** in the dialog that appears and proceed to the next step.
4. Authenticate with a previously enrolled logon method or your Windows password.
5. In the enrollment capture dialog that appears, select the challenge questions you want to enroll, then enter and confirm your answers. If your entries do not match, the mismatch indicated in red; re-enter each incorrect answer and its confirmation to correct the mismatch. When you have selected and answered enough questions to satisfy the weight requirements configured by the administrator, the progress bar at the top of the window will show 100%. At this point you can select additional questions to fall back on in case you forget the answers to your main questions. When you have selected and answered all of the desired questions, click **Finish**.
6. When enrollment is complete, a message confirms that the Challenge Questions method is now enrolled. Click **OK** to dismiss the dialog.
7. The method's status changes to **Enrolled**.

5.6 Managing Enrolled Credentials

Universal Authentication Manager provides you with great flexibility and control over your credentials. Click the following links to learn about:

- Viewing Properties of Enrolled Credentials
- Viewing Status of Enrolled Credentials
- Viewing and Modifying Enrolled Credentials
- Enrolling Additional Cards
- Re-Enrolling Credentials
- Deleting Credentials
- Changing Your Universal Authentication Manager PIN

5.6.1 Viewing Properties of Enrolled Credentials

To view properties of enrolled credentials:

1. From the Logon Methods tab, select the enrolled credential for which you wish to view properties.
2. Click **Modify** in the toolbar at the top of the screen, or right-click in the row for the card and select **Modify** from the pop-up menu. The dialog box that opens displays the logon method, card type, enrollment date, and card description (if any).

5.6.2 Viewing Status of Enrolled Credentials

Click **Logon Methods** to view available logon methods. The second column in the row for each method indicates the status of user enrollment for that method. Possible values are:

- **Enrolled.** You have successfully enrolled credentials for the logon method.
- **Optional.** You may enroll credentials for the logon method, but is not required.
- **Required.** You are required to enroll credentials for the logon method.
- **Not available.** The detected card is enrolled by a different user. This only applies to smart card and proximity cards.
- **Disabled.** The logon method is installed, but disabled.

5.6.3 Viewing and Modifying Enrolled Credentials

To modify credentials:

1. Select the logon method you wish to modify.
2. Click **Modify** to view or modify credentials.
   - For smart cards, you can view the card's properties.
   - For proximity cards, you can view the card's properties and change your PIN.
   - For fingerprint, you can view your enrollment date and re-enroll. Your existing credentials will be replaced.
   - For challenge questions, you can view your enrollment date and re-enroll. Your existing credentials will be replaced.

5.6.4 Enrolling Additional Cards

When a smart card or proximity card is detected, Universal Authentication Manager displays a single row of information, including a status of either OPTIONAL or REQUIRED. When you enroll the first card or token, the enrolled credential will activate the existing row and display a status of ENROLLED.

If you have enrolled at least one card, and want to enroll an additional one, click the **Enroll** button and choose either **Proximity Card** or **Smart Card** from the drop-down list that appears. Universal Authentication Manager displays a message stating that you have already enrolled one card and asks you to confirm that you want to enroll another one.

Click **OK** to continue with enrollment or click **Cancel** to cancel enrollment. If you click **OK**, follow the on-screen instructions to enroll an additional card. You will be asked to tap or insert your card to begin enrollment and then asked to enter your PIN. When

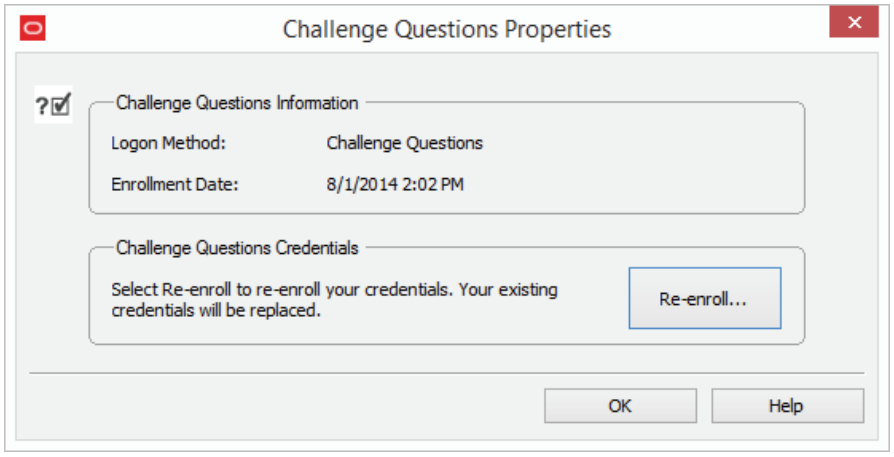
the card has been enrolled, Universal Authentication Manager displays a message confirming successful enrollment.

The Enroll Status column now shows two rows of card credentials, each with a status of **Enrolled**.

5.6.5 Re-Enrolling Credentials

When the Fingerprint or Challenge Questions logon method is enrolled, Universal Authentication Manager displays a single row of information, including a status of either **Optional** or **Required**. When you enroll the first fingerprint samples, the enrolled credential will activate the existing row and display a status of **Enrolled**.

You cannot enroll additional credentials, but you can replace your existing ones by re-enrolling. If you have enrolled at least one fingerprint sample, and want to re-enroll, highlight the logon method and click **Modify**.



Select **Re-enroll** to re-enroll your credentials and follow the on-screen instructions to re-enroll. When re-enrollment is complete, Universal Authentication Manager displays a confirmation message.

5.6.6 Deleting Credentials

To delete credentials:

> **Note:** If you are required to enroll a credential for a logon method, you will not be able to delete that logon method.

1. Select the row showing the credential you wish to delete.
2. Click the **Delete** button in the toolbar at the top of the screen; or right-click the row and select **Delete** from the drop-down menu.
3. When prompted to authenticate, authenticate with an enrolled method to complete the deletion. A message notifies you when the deletion has been completed.

Note: If you delete the set of credentials that you used to log on for a session (that is, you delete your credentials for a particular logon method), when you remove or "tap out" your card, the removal action that was set for the credential will still be enforced, even though the credential has been deleted. For more information on removal actions, see Configuring Universal Authentication Manager to Lock a Workstation

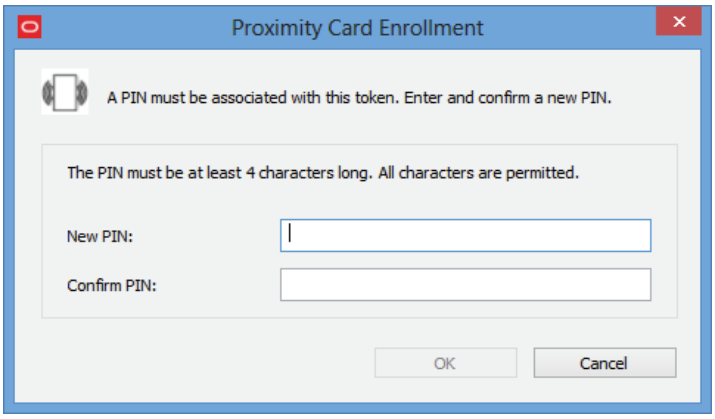
5.6.7 Changing Your Universal Authentication Manager PIN

If your Universal Authentication Manager fingerprint, smart card, or proximity card is enrolled with an associated Universal Authentication Manager PIN and you wish to change the PIN:

Note: When using a smart card, the card's own PIN cannot be changed. Only a Universal Authentication Manager PIN associated with the smart card can be changed. For more information, see Configuring Universal Authentication Manager.

To change the Universal Authentication Manager PIN for a fingerprint enrollment, follow the steps in Re-Enrolling Credentials.

1. Select the desired logon method.
2. Click **Modify** in the toolbar at the top of the window.
3. In the properties dialog that appears, click **Change…**.
4. Insert or tap your card into or on the reader, or authenticate with an enrolled logon method to proceed.
5. Enter the current PIN.
6. When prompted, enter and confirm a new PIN.



7. A message confirms that you have successfully changed your PIN.

5.7 Authenticating

Universal Authentication Manager allows you to quickly and securely log on and re-authenticate to Windows with any authentication device, such as an RFID badge or non-Windows smart card. The following actions are available:

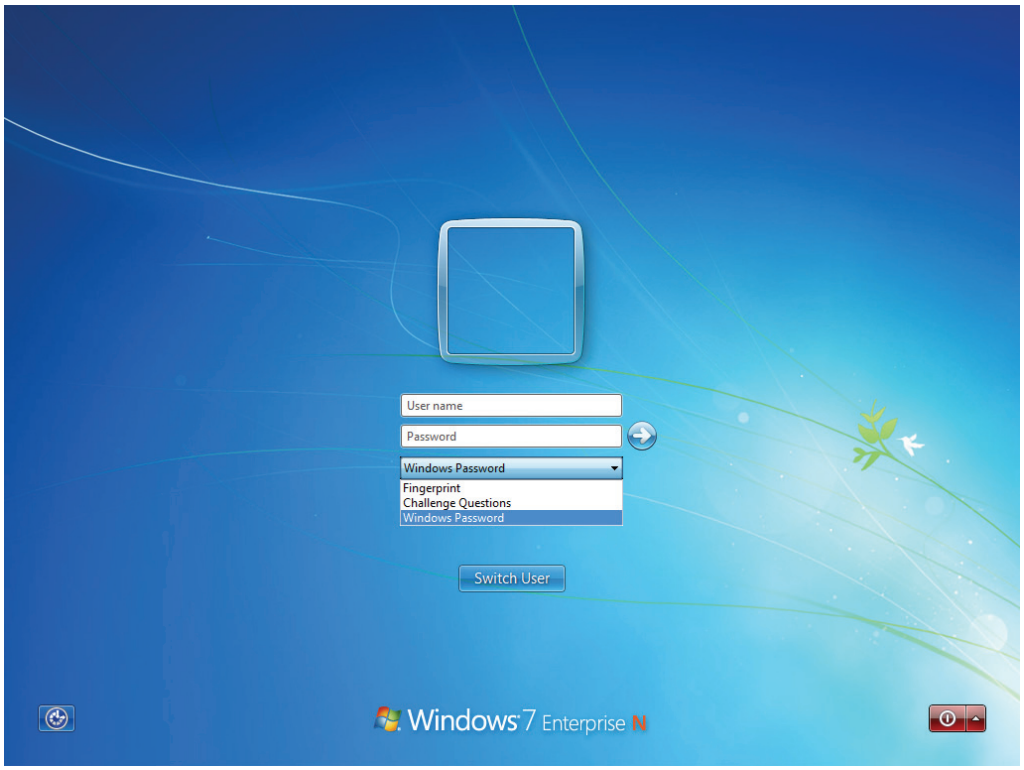
- Logging On to Windows 7 with Universal Authentication Manager using:
  - Your Fingerprint
  - Smart Card or Proximity Card
  - Challenge Questions
  - Windows Password
  - Re-authenticating to Universal Authentication Manager
  - Locking a Workstation
- Logging On to Windows 8/8.1 with Universal Authentication Manager using:
  - Your Fingerprint
  - Smart Card or Proximity Card
  - Challenge Questions
  - Windows Password
  - Re-authenticating to Universal Authentication Manager
  - Locking a Workstation
- Re-Authenticating to Universal Authentication Manager

5.7.1 Logging On to Windows 7 with Universal Authentication Manager

When Universal Authentication Manager is installed on your system, the Windows 7 logon screen displays the available users and Universal Authentication Manager logon methods.

To log on with a Smart Card or a proximity card, select the appropriate logon method tile.

To log on with a Windows password, or the Fingerprint or Challenge Questions logon methods, select the desired user (provided that user has previously enrolled those logon methods) or click **Other user**, enter the desired user name, and select the desired logon method from the drop-down list, and click the **Submit** ("right-arrow") button.



The available logon methods will depend upon what your administrator has installed. This logon dialog always defaults to the last used logon method; for example, if Fingerprint is used to log on, it will be preselected at next logon.

Upon initial logon to Universal Authentication Manager, use your Windows Password (if this is an option). You can then launch the Universal Authentication Manager client and enroll credentials. Once enrolled, you can use an enrolled credential (for example, a smart card or fingerprint) to log on to Windows or to unlock your workstation in place of a Windows password.

> **Note:** If necessary-for example, if your card is lost or damaged-you can always fall back on using your Windows password or the Challenge Questions quiz for logon (if enabled).

Universal Authentication Manager extends your system's normal Windows logon behavior. Microsoft Windows includes numerous security policies and settings that affect the Windows logon and unlock process; Universal Authentication Manager conforms with these policies. For example, if your password reaches the maximum password age, Universal Authentication Manager will still require you to change your password before you can log on.

5.7.1.1 Logging On with Your Fingerprint

The Fingerprint logon method must be manually selected from the logon dialog.

For example, to log on to or unlock Windows with an enrolled fingerprint:

1. At the logon screen, select or enter a user name (and domain, if required).
2. Select the **Fingerprint** logon method from the drop-down list.
3. Click the submit (right-arrow) button.
4. If you have enrolled a PIN, Universal Authentication Manager prompts you to enter it.
5. Universal Authentication Manager prompts you to present your fingerprint sample (for example, place or slide your finger on your reader).
6. Universal Authentication Manager validates the fingerprint sample and logs you on to Windows.

You can cancel this process at any time and return to the logon screen by clicking **Cancel**.

You may have to retry logon or unlock if:

- You enter an invalid PIN. In this case, try entering your PIN again, or click **Cancel** to return to the logon screen.
- The biometric sample you try to use for logon is not enrolled as a Universal Authentication Manager logon method. If this happens, authentication will fail. You may try again or choose a different logon method.

5.7.1.2 Logging On with a Smart Card or Proximity Card

Unlike the Fingerprint and Challenge Questions logon methods, Smart Card and Proximity Card logons are event-driven by token insertion and removal.

> **Note:** If your smart card or proximity has already been inserted or registered by the reader, its respective icon will appear in the logon screen - click the icon to log on with the card.

For example, to log on to or unlock Windows with an enrolled smart card or proximity card:

1. At the logon screen, insert or tap an enrolled card on the card reader. Universal Authentication Manager locates and validates the enrolled card and identifies you. If no PIN is required with your card, you are logged on to Windows.
2. If you click the smart card or proximity card icon, Universal Authentication Manager prompts you to tap or insert your card. (For proximity cards, hold your card near the reader until Universal Authentication Manager detects it.)
3. If a PIN is required with your card, enter your PIN when prompted. Universal Authentication Manager validates the PIN and logs you on to Windows.

You can cancel this process at any time and return to the logon dialog by clicking **Cancel**.

You may have to retry logon or unlock if:

- You enter an invalid PIN. In this case, try entering your PIN again, or click **Cancel** to return to the logon screen.
- The card you try to use for logon is not enrolled as a Universal Authentication Manager logon method. If the card is not detected, nothing will occur. If the card is detected but is not enrolled, you will see an error message.

5.7.1.3 Logging On with Challenge Questions

The Challenge Questions logon method must be manually selected from the logon dialog.

For example, to log on to or unlock Windows with Challenge Questions:

1. At the logon screen, select or enter a user name (and domain, if required).
2. Select the **Challenge Questions** logon method from the drop-down list.
3. Click the submit (right-arrow) button.
4. In the dialog that appears, read the challenge question and enter your answer, then click **Next**. If you don't know the answer to the question and have enrolled extra questions to fall back on, click **Skip**.

   (If you have not enrolled extra questions, skipping a required question will result in a failed logon since you will not be able to satisfy the weight requirement set by the administrator.)

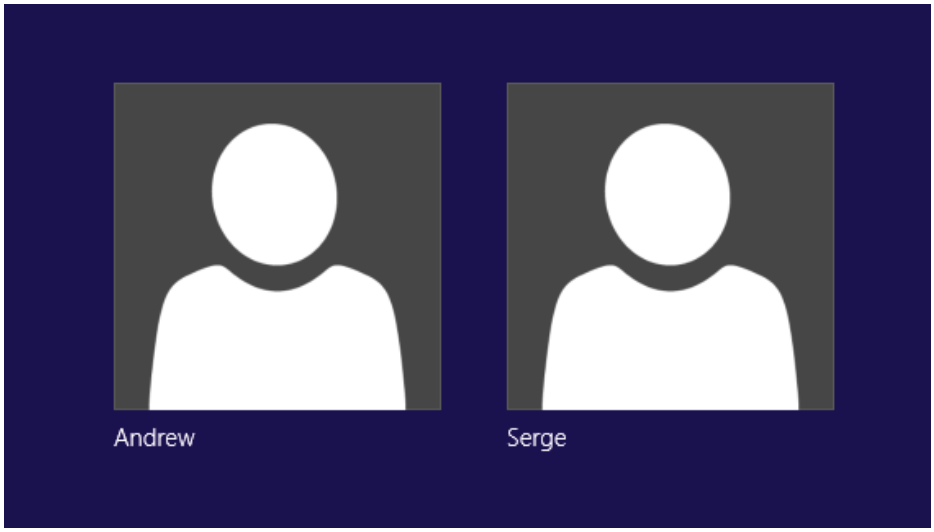
   When you have correctly answered enough questions to complete the logon, Universal Authentication Manager logs you on to Windows.

5.7.1.4 Logging On with the Windows Password

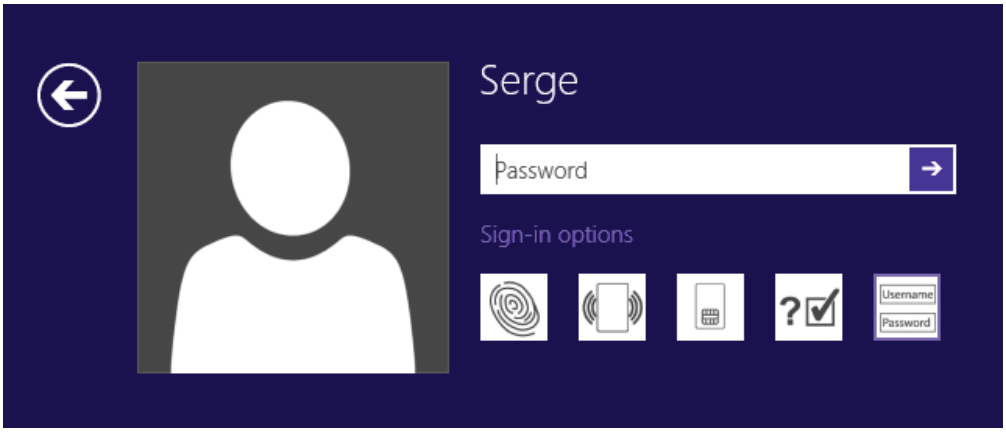
If working in Enterprise Client Mode, your Administrator may disable use of the Windows Password logon method through the Logon Method Enabled Rules. If Windows password is disabled, you will be able to continue using it until you enroll in at least one other logon method. Once you are enrolled in another logon method, you will no longer be able to log on with a Windows password.

5.7.2 Logging On to Windows 8/8.1 with Universal Authentication Manager

When Universal Authentication Manager is installed on your system, the Windows 8/8.1 logon screen displays the available users:



Selecting a user will allow you to log on as that user with the associated Windows password or click the **Sign in options** link to expose available Universal Authentication Manager logon methods. The available logon methods will depend upon what your administrator has installed.



Upon initial logon to Universal Authentication Manager, use your Windows Password (if this is an option). You can then launch the Universal Authentication Manager client and enroll credentials. Once enrolled, you can use an enrolled credential (for example, a smart card or fingerprint) to log on to Windows or to unlock your workstation in place of a Windows password.

Note: If necessary-for example, if your card is lost or damaged-you can always fall back on using your Windows password or the Challenge Questions quiz for logon (if enabled).

Universal Authentication Manager extends your system's normal Windows logon behavior. Microsoft Windows includes numerous security policies and settings that affect the Windows logon and unlock process; Universal Authentication Manager conforms with these policies. For example, if your password reaches the maximum password age, Universal Authentication Manager will still require you to change your password before you can log on.

5.7.2.1 Logging On with Your Fingerprint

The Fingerprint logon method must be manually selected from the logon dialog.

For example, to log on to or unlock Windows with an enrolled fingerprint:

1. At the logon screen, select or enter a user name (and domain, if required).
2. Click **Sign-in options** and select **Fingerprint** logon method.
3. Click the submit (right-arrow) button.
4. If you have enrolled a PIN, Universal Authentication Manager prompts you to enter it.
5. Universal Authentication Manager prompts you to present your fingerprint sample (for example, place or slide your finger on your reader).
6. Universal Authentication Manager validates the fingerprint sample and logs you on to Windows.

You can cancel this process at any time and return to the logon screen by clicking **Cancel**.

You may have to retry logon or unlock if:

- You enter an invalid PIN. In this case, try entering your PIN again, or click **Cancel** to return to the logon screen.
- The biometric sample you try to use for logon is not enrolled as a Universal Authentication Manager logon method. If this happens, authentication will fail. You may try again or choose a different logon method.

5.7.2.2 Logging On with a Smart Card or Proximity Card

Unlike the Fingerprint and Challenge Questions logon methods, Smart Card and Proximity Card logons are event-driven by token insertion and removal.

> **Note:** If your smart card or proximity has already been inserted or registered by the reader, its respective icon will appear when you click **Sign in options** in the logon screen after selecting the desired user. Simply select the icon and click the **Submit** ("right-arrow") button to log on with the card.

For example, to log on to or unlock Windows with an enrolled smart card or proximity card:

1. At the logon screen, insert or tap an enrolled card on the card reader. Universal Authentication Manager locates and validates the enrolled card and identifies you. If no PIN is required with your card, you are logged on to Windows.
2. If you click **Sign-in options** and select the smart card or proximity card icon, Universal Authentication Manager prompts you to tap or insert your card. (For proximity cards, hold your card near the reader until Universal Authentication Manager detects it.)
3. If a PIN is required with your card, enter your PIN when prompted. Universal Authentication Manager validates the PIN and logs you on to Windows.

You can cancel this process at any time and return to the logon dialog by clicking **Cancel**.

You may have to retry logon or unlock if:

- You enter an invalid PIN. In this case, try entering your PIN again, or click **Cancel** to return to the logon screen.
- The card you try to use for logon is not enrolled as a Universal Authentication Manager logon method. If the card is not detected, nothing will occur. If the card is detected but is not enrolled, you will see an error message.

5.7.2.3 Logging On with Challenge Questions

The Challenge Questions logon method must be manually selected from the logon dialog.

For example, to log on to or unlock Windows with Challenge Questions:

1. At the logon screen, select or enter a user name (and domain, if required).
2. Click **Sign-in options** and select the **Challenge Questions** logon method.
3. Click the submit (right-arrow) button.
4. In the dialog that appears, read the challenge question and provide your answer, then click **Next**. If you don't know the answer to the question and have enrolled extra questions to fall back on, click **Skip**. (If you have not enrolled extra

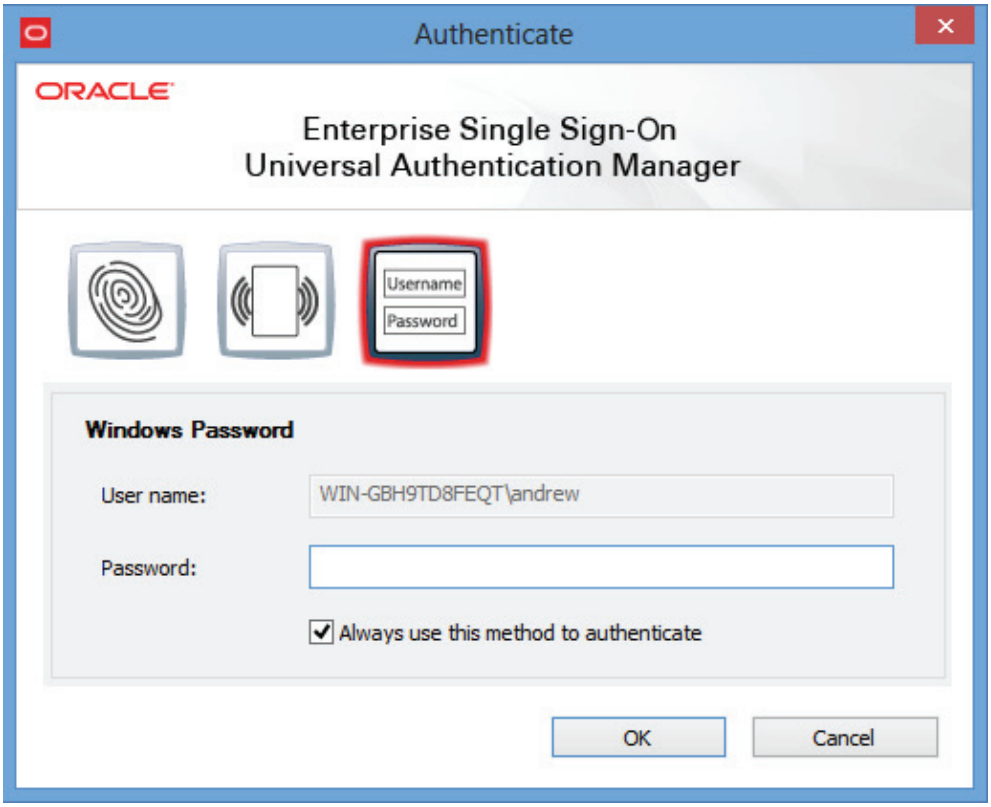
questions, skipping a required question will result in a failed logon since you will not be able to satisfy the weight requirement set by the administrator.) When you have correctly answered enough questions to complete the logon, Universal Authentication Manager logs you on to Windows.

5.7.2.4 Logging On with the Windows Password

If working in Enterprise Client Mode, your Administrator may disable use of the Windows Password logon method through the Logon Method Enabled Rules. If Windows password is disabled, you will be able to continue using it until you enroll in at least one other logon method. Once you are enrolled in another logon method, you will no longer be able to log on with a Windows password.

5.7.3 Re-Authenticating to Universal Authentication Manager

The Universal Authentication Manager re-authentication dialog box provides the ability to authenticate to Windows within the currently active user session via available logon methods. You can select your logon method from the horizontal bar of icons, which from left to right represent: Fingerprint, Proximity Card, Smart Card, Challenge Questions, and Windows Password.



Each icon presents different controls in the dialog, for example selecting the password icon will show a password field, selecting the smart card icon will hide the password field and prompt you to insert a smart card.

Insertion of smart card and proximity card tokens triggers authentication immediately. However, if no cards are inserted, selecting the button for the appropriate logon method prompts you to insert a card or tap a token.

The reauthentication dialog box:

- Filters out logon methods that are not installed, not registered, not enrolled, or that are disabled by the Logon Method Enabled policy.
- Defaults to the last used logon method, so if Fingerprint is used to log on, it will be pre-selected at next logon.

The **Always use this method to authenticate** check box is always selected by default. This means that future authentications will default to the selected logon method and you will not see the Authenticate dialog box if not necessary.

If you deselect the checkbox and click **OK**, the re-authentication dialog box is always displayed, and the previously-used method is selected by default. This is useful for users who often switch between different logon methods.