Oracle© Enterprise Single Sign-On Suite Plus

User's Guide

Release 11.1.2

E27304-03

March 2013

ORACLE®

Oracle Enterprise Single Sign-On Logon Manager User's Guide, Release 11.1.2

E27304-03

Contents

Preface

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

Audience

This user 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 Universal Authentication Manager (Universal Authentication Manager)
- Oracle Enterprise Single Sign-On Password Reset (Password Reset)

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.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/support/contact.html or visit http://www.oracle.com/accessibility/support.html if you are hearing impaired.

Related Documents

For more information, see the other documents in the Oracle Enterprise Single Sign-On Suite documentation set for this release.

Oracle Enterprise Single Sign-On Suite

Release Notes

Installation Guide

Administrator's Guide

Secure Deployment Guide

User's Guide

Oracle Enterprise Single Sign-On Logon Manager

Deploying Logon Manager with a Directory-Based Repository

Configuring and Diagnosing Logon Manager Application Templates

Oracle Enterprise Single Sign-On Provisioning Gateway

Administrator's Guide

Command Line Interface Guide

Oracle Identity Manager Connector Guide

Sun Java System Identity Manager Connector Guide

IBM Tivoli Identity Manager Connector Guide

Oracle Enterprise Single Sign-On Universal Authentication Manager

Administrator's Guide

User'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.

Introduction to Oracle Enterprise Single Sign-On Suite 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.

Oracle Enterprise Single Sign-On Logon Manager (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.

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.

Oracle Enterprise Single Sign-On Anywhere (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.

Oracle Enterprise Single Sign-On Password Reset (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.

Oracle Enterprise Single Sign-On Universal Authentication Manager (Universal Authentication Manager)

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
- BioAPI
- 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 of these components, continue to the specific component's chapter.

Part I. About 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.

Getting Started Using Logon Manager

After installing Logon Manager, 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 Menu Options.

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

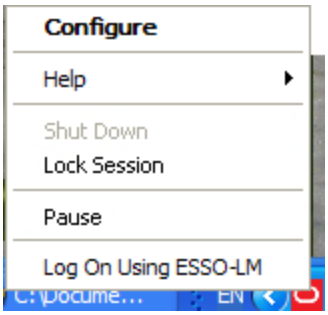
This procedure is performed the first time you start the program.

The remainder of this guide covers these topics:

- Logon Manager
- Your Primary Logon Method
- Managing Accounts
- Settings
- Managing Passwords

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.



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**.

System Tray Menu Options

Configure	Launches the Logon Manager. The Logon Manager displays stored accounts, allows you to add, delete and modify accounts, as well as 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.
Lock Session	Locks the current session.
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 turned off.  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.

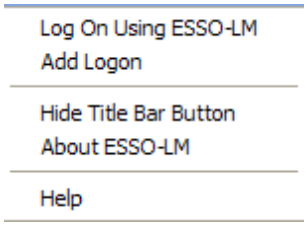
Shutting Down Logon Manager

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

The Title Bar Button Menu

You can put the Logon Manager Title Bar Button on all application window title bars. The Title Bar 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.



To Show or Hide the Title Bar Button

1. Open the 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 menu.
4. Check **Provide a dropdown menu from title bar button** to activate the Title Bar Button 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.

     or
   - Click **Apply** to confirm your changes (without closing Logon Manager), and select another Settings tab.

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

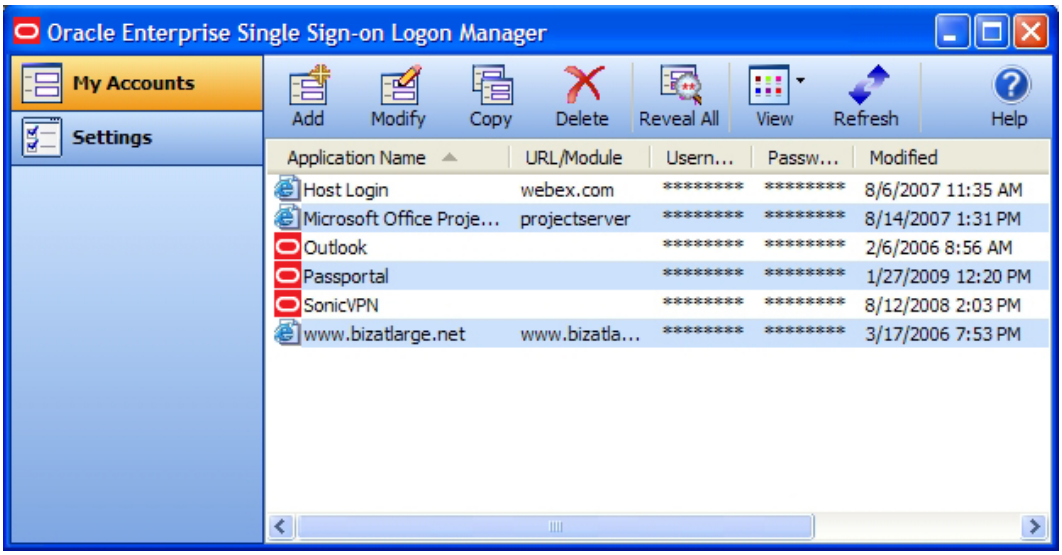
> To hide the Title Bar Button and menu at any time, click the Title Bar Button on any application title bar and select **Hide Title Bar Button**.

Using Logon Manager

The 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 on 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 the Logon Manager.
- Logon Manager configuration options are available in the Settings panel.



My Accounts

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 controls on this panel:

	**Add**	Launches the New Logon dialog box to set up a new account.
	**Modify**	Launches the Modify Account dialog box, 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.
	**Delete**	Remove a selected account from Logon Manager. A confirmation message 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 the Logon Manager. (This feature is only available if the administrator has activated it.)
	**View**	Allows you to change 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.

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.

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.

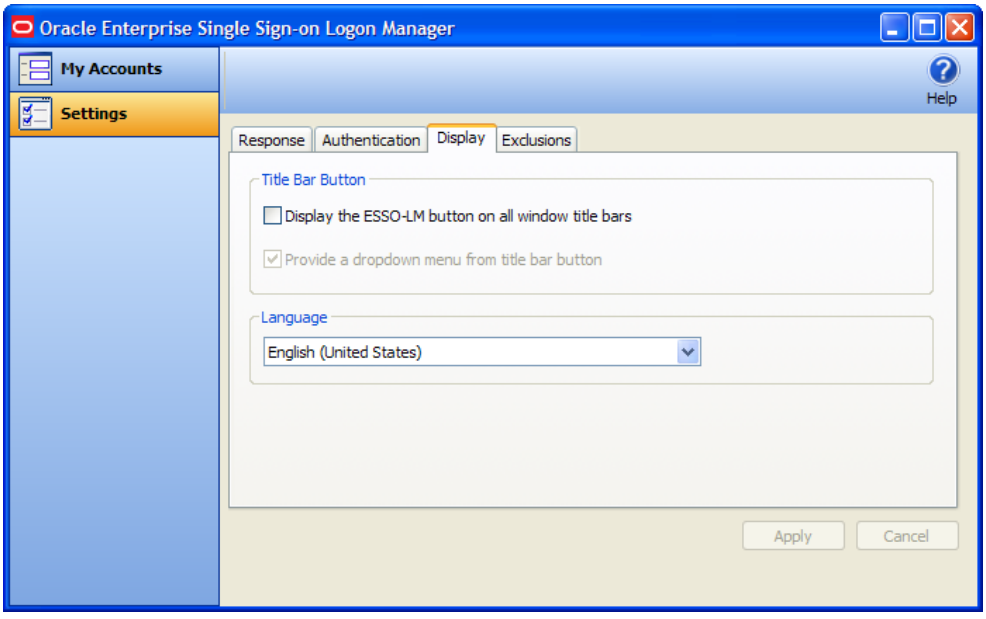
This message typically appears when Logon Manager has been upgraded from a previous version. It means that your credentials are safely stored, but the application configuration (that tells Logon Manager where to put the credentials) needs to be upgraded as well. Contact your administrator to acquire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

Language Settings

The Logon Manager Agent 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 the Logon Manager.
2. Open the **Settings** panel and select the **Display** tab.
3. Select from the list of available languages in the **Language** drop-down.



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

Using the Setup Wizard to Set Up 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.

> If you cancel the Setup Wizard, it will re-appear each time you try to start Logon Manager until you've completed the Wizard.

Completing the Setup Wizard Tasks

The wizard takes you through one or more 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.

> The Setup Wizard may skip any or all of the above tasks, depending on the installation options selected and your network's configuration.

Setup Tasks to Perform

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

Click **Next** to begin setup.

Choosing a Logon Method

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. Plug-in that enables logging onto Logon Manager by logging on to Windows. If you choose Windows Logon v2, one or more passphrase questions appear. This is used for additional security.
   - Windows Logon. Plug-in that enables logging on to Logon Manager by logging on to Windows. (This authenticator has been deprecated as of version 11.1.2.).
   - LDAP. Plug-in that enables logging onto Logon Manager by logging on to an LDAP directory.
   - LDAP v2. Plug-in that enables logging on to Logon Manager by logging on to an LDAP directory. If you choose LDAP v2, one or more passphrase questions appear. This is used for additional security.
   - Entrust. Plug-in that enables logging onto Logon Manager by logging on to the Entrust PKI and Entelligence client.
   - Proximity Card. Authenticator plug-in that supports authentication with HID Proximity Cards.
   - Smart Card. Plug-in that enables logging onto Logon Manager using an MS-CAPI-capable smart card. If you choose smart card, one or more passphrase questions appear. This is used for additional security.
   - Read-Only Smart Card. Plug-in that enables logging onto Logon Manager using a Read-Only Smart Card

- RSA SecurID. Plug-in that enables logging onto Logon Manager using one-time passwords generated by RSA SecurID tokens.
- Authentication Manager. 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. Adds the capability to authenticate to Logon Manager through a variety of strong authenticator options. This option is available if you have also installed the Universal Authentication Manager client.

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

Selecting Your Primary Logon Method

If you choose Windows Authentication 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**.

Insert a Smart Card

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**.

Enter a Passphrase Answer

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

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

Adding Application Logons

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.

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. You can now begin using Logon Manager.

Your Primary Logon Method

When you first set up Logon Manager, you are prompted to choose your *primary logon method*, also known as an *authenticator*.

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.

Depending on your installation and resources, your primary logon can be any of the following:

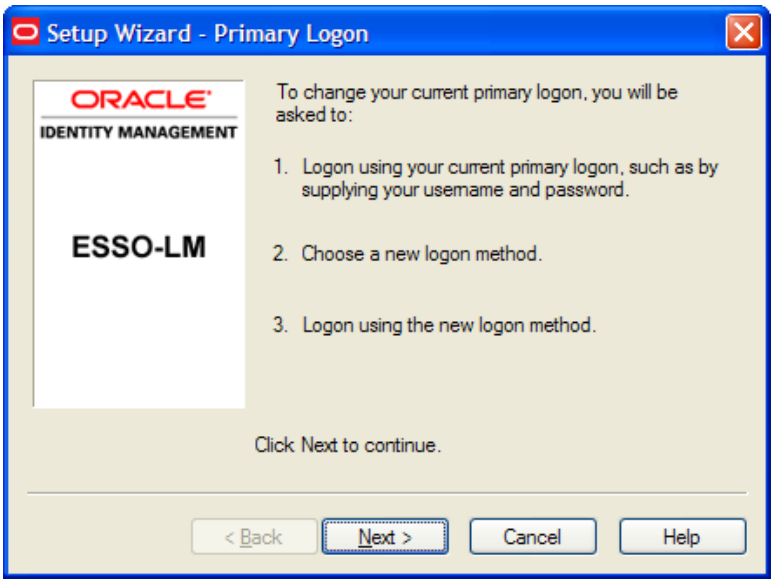
- Windows Logon v2. Plug-in that enables logging on to Logon Manager by logging on to Windows. If you choose Windows Logon v2, one or more passphrase questions appear. This is used for additional security.
- Windows Logon. Plug-in that enables logging on to Logon Manager by logging on to Windows. (This authenticator has been deprecated as of version 11.1.2.).
- LDAP. Plug-in that enables logging on to Logon Manager by logging on to an LDAP directory.
- LDAP v2. Plug-in that enables logging on to Logon Manager by logging on to an LDAP directory. If you choose LDAP v2, one or more passphrase questions appear. This is used for additional security.
- Entrust. Plug-in that enables logging on to Logon Manager by logging on to the Entrust PKI and Entelligence client.
- Proximity Card. Authenticator plug-in that supports authentication with HID Proximity Cards.
- Smart Card. Plug-in that enables logging on to Logon Manager using an MS-CAPI-capable smart card. If you choose smart card, one or more passphrase questions appear. This is used for additional security.
- Read-Only Smart Card. Plug-in that enables logging on to Logon Manager using a Read-Only Smart Card
- RSA SecurID. Plug-in that enables logging on to Logon Manager using one-time passwords generated by RSA SecurID tokens.
- Authentication Manager. 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. Adds the capability to authenticate to Logon Manager through a variety of strong authenticator options. This option is available if you have also installed the Universal Authentication Manager client.

Changing Your Primary Logon Method

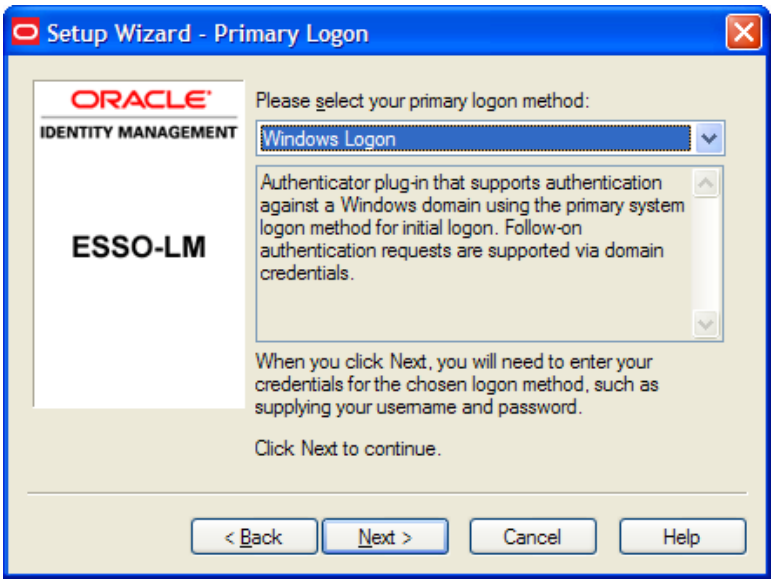
You can change your primary logon method at any time, and you can install or remove authenticators as needed.

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 are prompted for your new primary logon credentials. Enter your user ID and password, and enter or select any additional information, then click **OK**.

> 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 box appears. Click **Close** to close it.

Confirming Your Primary Logon Method

Logon Manager can be configured to periodically check 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.

Installing Primary Logon Methods

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

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

Installing Additional Primary Logon Methods

1. Open Control Panel, and depending on your operating system:
   - If you are using Windows XP or Windows Server 2003, double-click **Add/Remove Programs**.

     or

   - If you are using Windows 7 or Windows Server 2008, 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 **+** 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.

Managing 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 box. 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.*

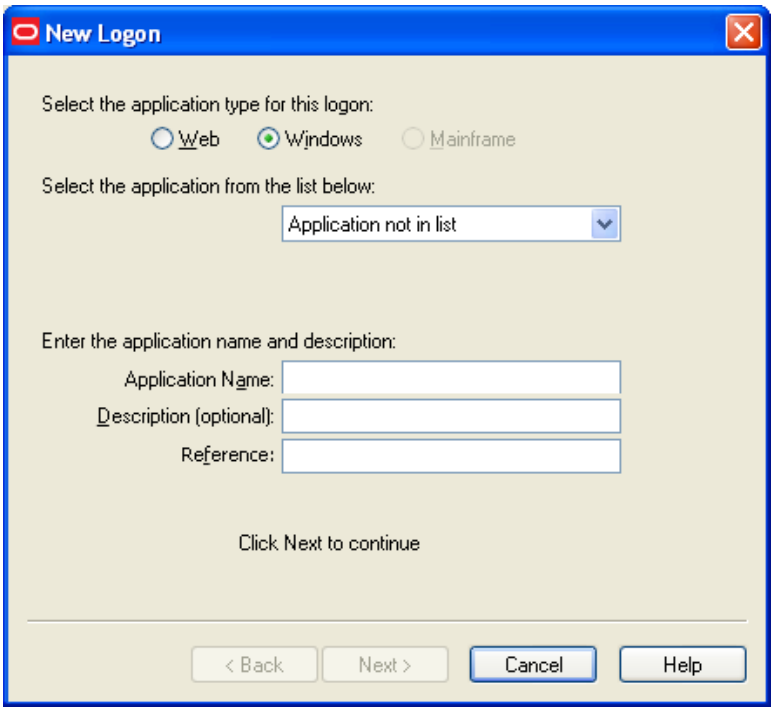
**This functionality is new as of version 11.1.1.5.0.*

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.

Using Logon Manager to Set Up Accounts That You Select

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



The following procedures describe how to use the New Logon dialog box 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.

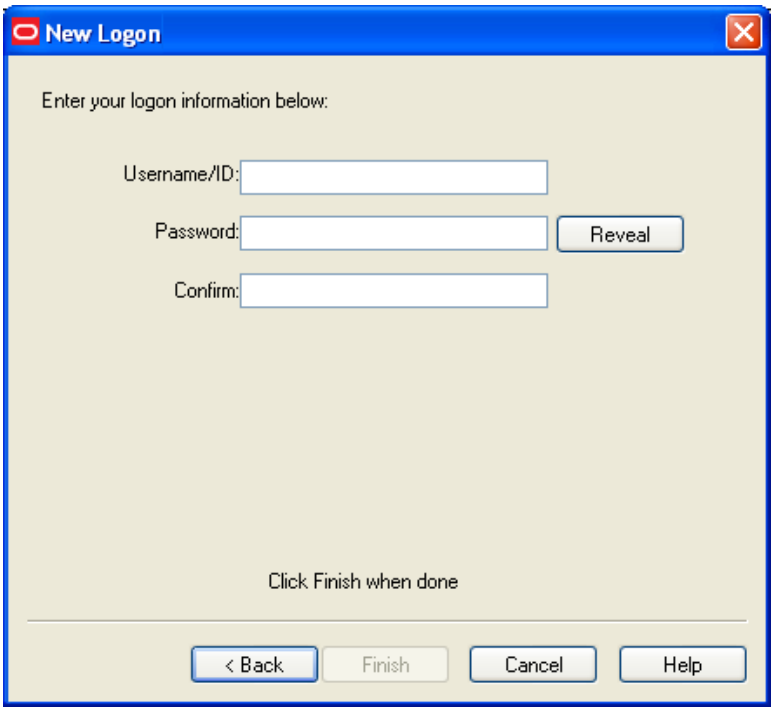
You are also given the option to create more than one account for a single application. This is useful for applications for which you have more than one set of credentials; for example, if you have multiple email accounts from one account.

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

Adding an Account for a Windows Application

Select an Application

1. In the New Logon dialog box, 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 requesting credentials.



1. Type your **Username/ID** for the application, type your **Password**, and retype your password in **Confirm Password**. You can display the password by clicking **Reveal**.

> 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.

2. Do one of the following:
   - Click **Finish**. Logon Manager returns you to the Logon Manager, which now lists the account you have just created.

     or
   - If the setting is available, select **Add another set of credentials**, then click **Finish**. Logon Manager adds the account to the Logon Manager and re-displays the New Logon dialog box.

> 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 the section, "Applications that share credentials" in the *Oracle Enterprise Single Sign-On User's Guide* for more information.

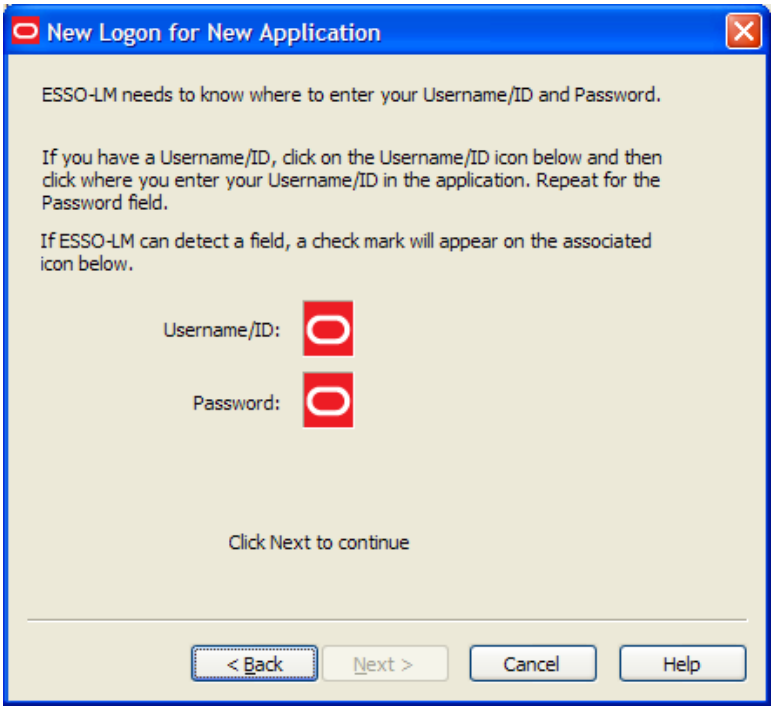
Adding an Account for an Unlisted Windows Application

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.

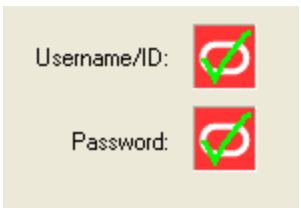
1. Open the Windows application for which you want to set up an account. This is the target application.

> 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.

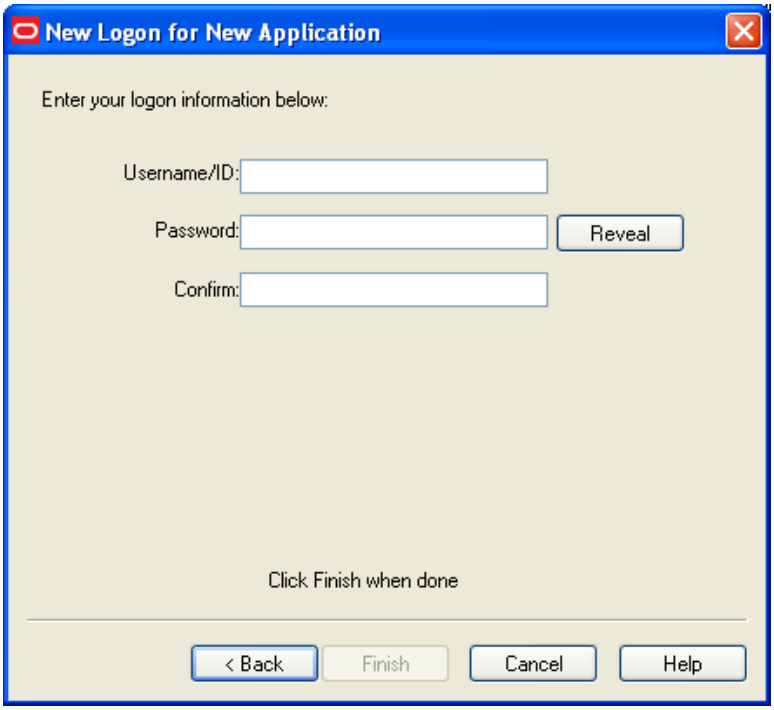
2. When the target application's logon dialog box displays, switch back to Logon Manager. Arrange the windows so that Logon Manager and the target application's logon dialog box are both visible.
3. In the New Logon dialog box, select the **Windows** option and select **Application not in list** (the 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 box. 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 box. A green check mark appears over the icon.



9. Click **Next**. The New Logon dialog box appears, requesting credentials.



1. Type your **Username/ID** for the application, type your **Password**, and retype your password in **Confirm Password**. You can display the password by clicking **Reveal**.
2. Do one of the following:
   - Click **Finish**. Logon Manager returns you to the Logon Manager, which now lists the account you have just created.

     or

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

> 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.

Adding an Account for a Web Site

1. In the New Logon dialog box, 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 box appears, requesting credentials.

1. Enter the **Username/ID** for the Web site, enter the **Password**, and reenter the password in **Confirm Password**. You can display the password by clicking **Reveal**.

2. Do one of the following:
   - Click **Finish**. Logon Manager returns you to the Logon Manager, which now lists the account you have just created.

     or

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

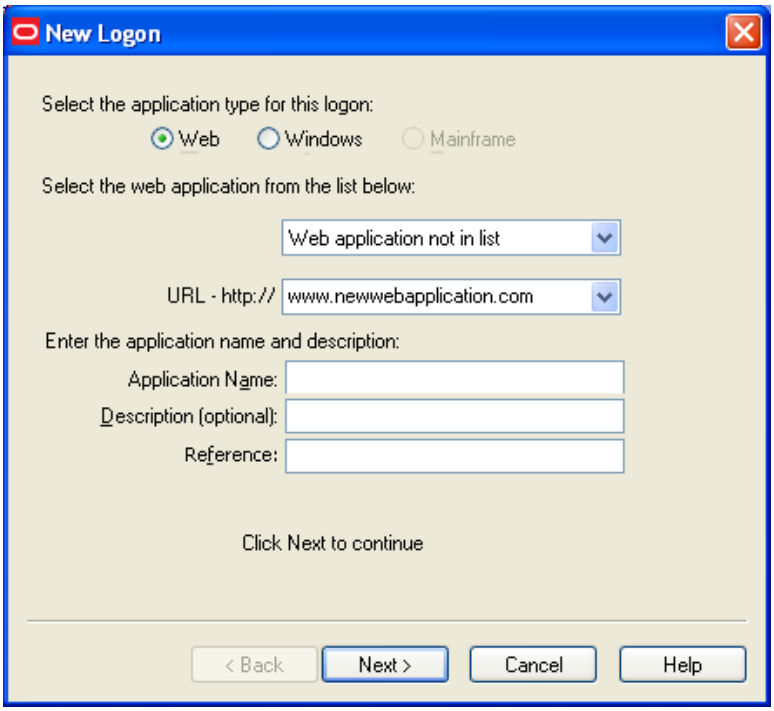
If you are adding a new account for an existing application that is part of a credential sharing group, select **Exclude from credential sharing group**. If this is the first account you have created for this application, leave this check box unselected. See the section, "Applications that share credentials" in the *Oracle Enterprise Single Sign-On User's Guide* for more information.

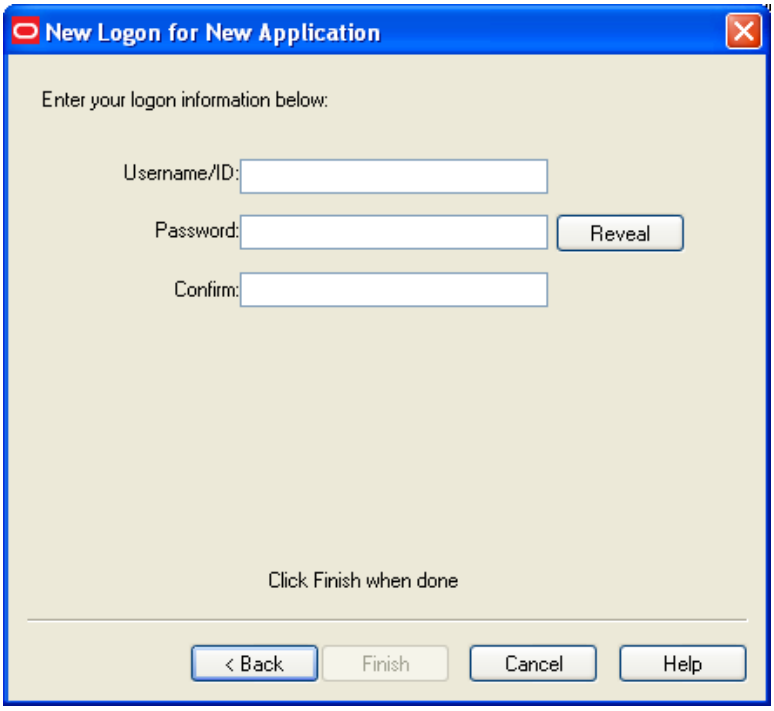
Adding an Account for an Unlisted Web Site

1. In the New Logon dialog box, 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.

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.
3. Enter the **Application Name** and (optionally) a **Description**.
4. Click **Next**. The New Logon dialog box appears requesting credentials.

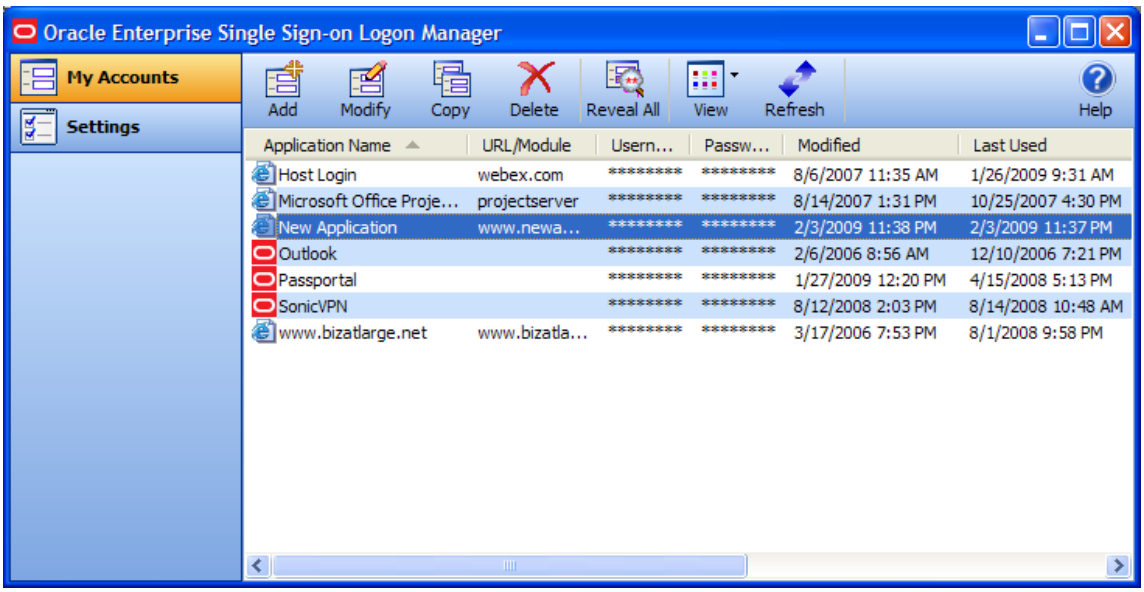




1. Enter the **Username/ID** for the Web site, type the **Password**, and reenter the password in **Confirm Password**. You can display the password by clicking **Reveal**.

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

     or
   - If the setting is available, select **Add another set of credentials**, then click **Finish**. Logon Manager adds the account to the Logon Manager and re-displays the New Logon dialog box.



Adding an Account for a Host/Mainframe Application

1. In the New Logon dialog box, 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 box appears, requesting credentials.

Enter Your Credentials

1. Enter the **Username/ID** for the Web site, enter the **Password**, and reenter the password in **Confirm Password**. You can display the password by clicking **Reveal**.
2. Do one of the following:
   - Click **Finish**. Logon Manager returns you to the Logon Manager, which now lists the account you've just created.

     or
   - If the setting is available, select **Add another set of credentials**, then click **Finish**. Logon Manager adds the account to the Logon Manager and re-displays the New Logon dialog box.

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 the 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**.

> 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've 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:

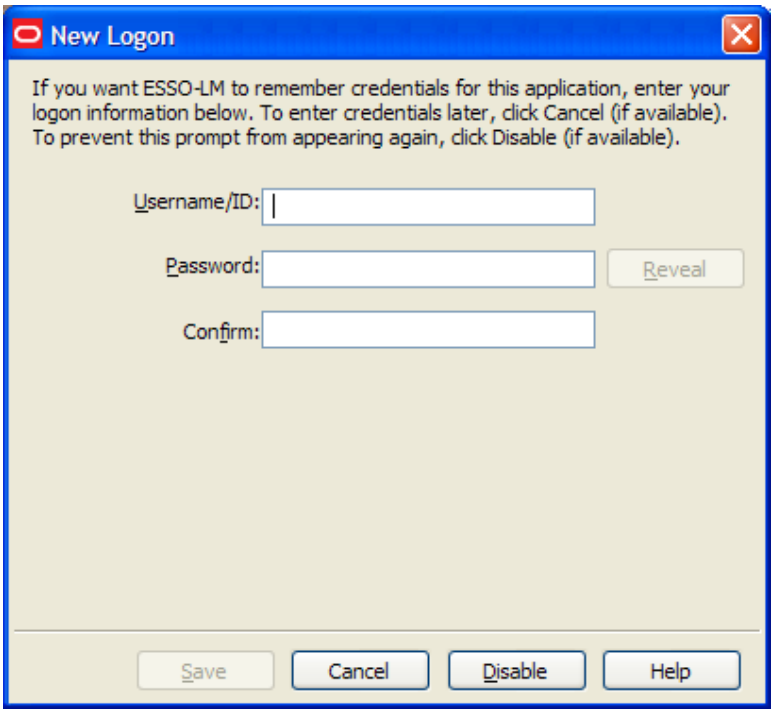
You launch Lotus Notes, an application for which you have already provided credentials. As soon as you open Lotus Notes, Logon Manager recognizes this logon screen's request for credentials.

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 box, 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 box, 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). Logon Manager prompts you to add an account the next time you launch the application.
- 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.

> 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.

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 box, with empty fields, appears so that the user can enter his credentials. Users from the group who create subsequent accounts receive the New Logon dialog box 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 box 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.

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.

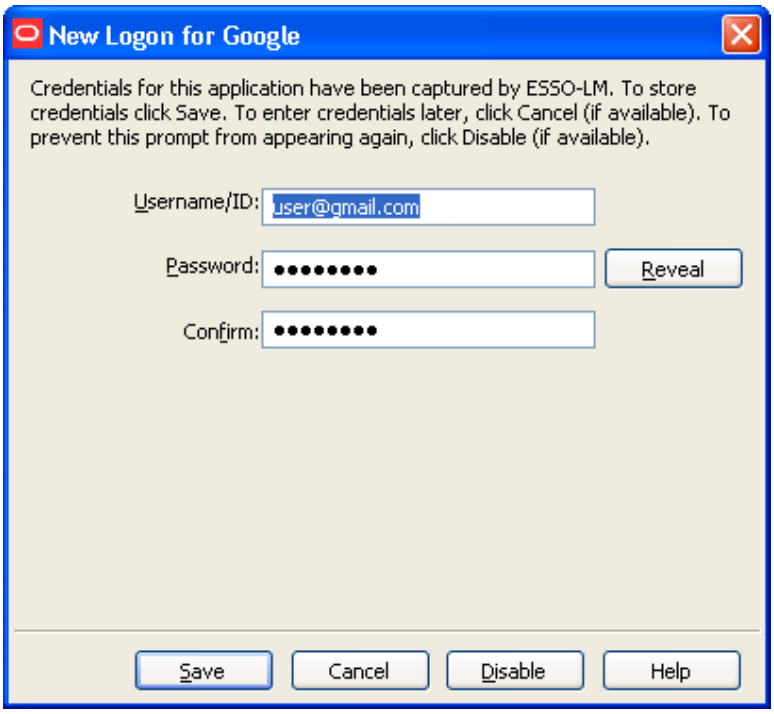
  or

- A balloon tip appears in the icon tray menu, notifying you that the credentials are being captured. You will not be required to verify them afterward.

  or

- A balloon tip appears in the icon tray menu, notifying you that the credentials are being captured, and then the New Logon dialog box 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 box or inform you that credentials have not been captured.

This feature is new as of version 11.1.1.5.0.

Modifying Accounts

You can modify account information or automatic behavior for *individual* accounts using the Modify icon  on the Logon Manager or by double-clicking the account. From this dialog box, 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**, **Application Name** 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:

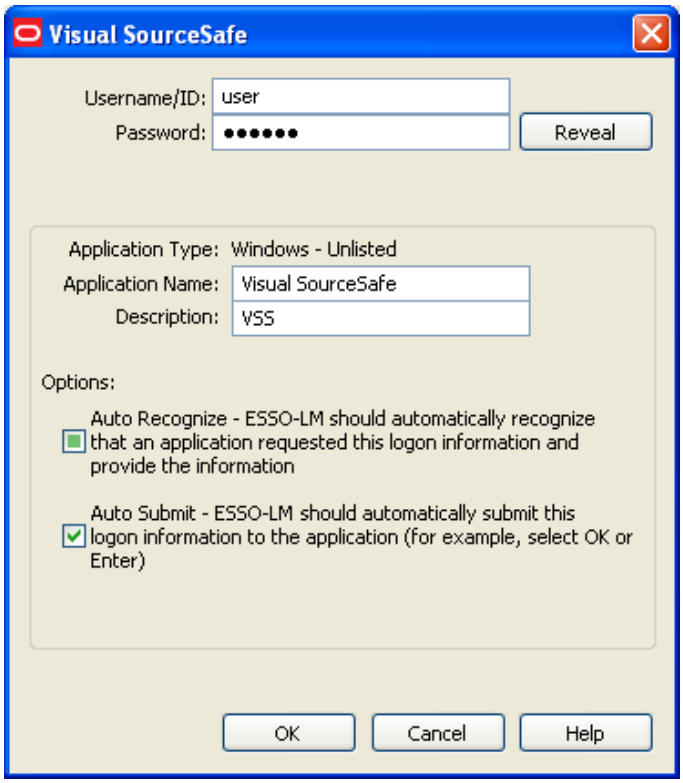
- A blank checkmark means it is off for the selected application.
- A checkmark means it is on for the selected application.
- A green box means that the global setting defines the action for the selected application.

- **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.

> 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 box overrides the global **Auto-Recognize** setting.

Modifying an Account

1. Open the 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 box for the selected account appears.



> 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 the section, Accounts Without Configured Credentials for more information.

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

Action Chooser Dialog Box

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

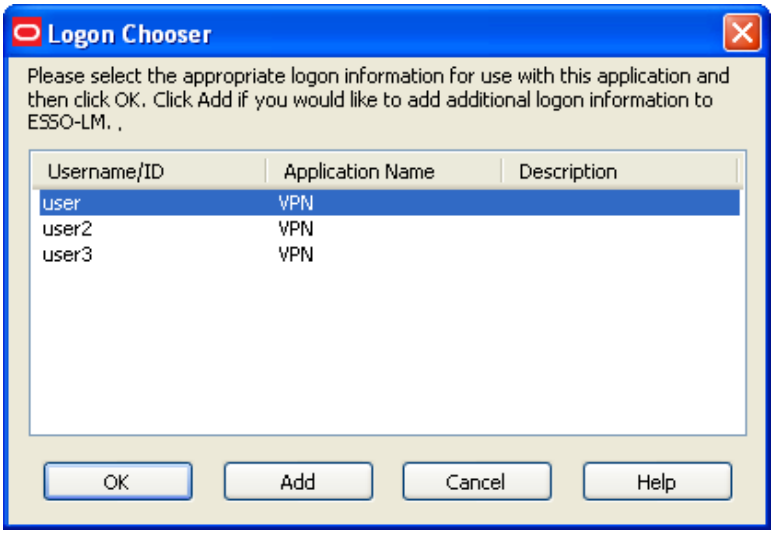
To choose the desired action:

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

Logon Chooser Dialog Box

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

When you open the application or Web site, Logon Manager prompts you with the Logon Chooser dialog box.



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.

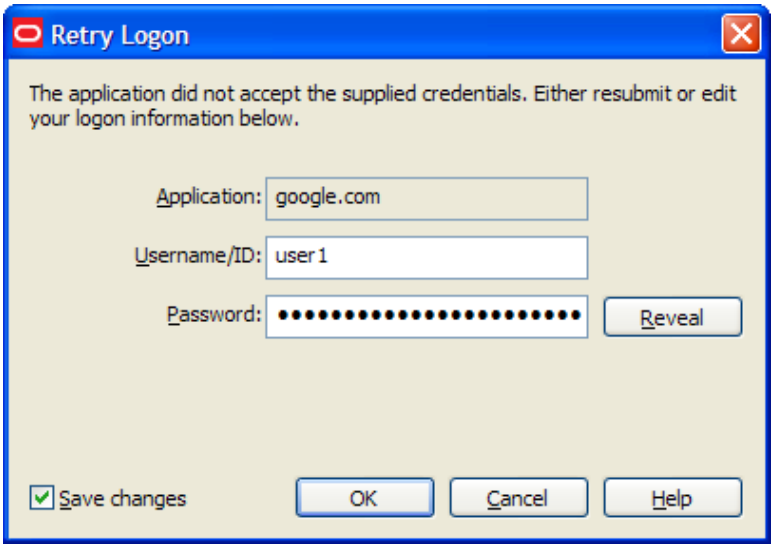
Do one of the following:

- 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.

Retry Logon Dialog Box

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 computer, Logon Manager will supply an incorrect password. When this happens, the application repeats the logon request and Logon Manager displays the Retry Logon dialog box.



The Retry Logon dialog box appears if you entered the wrong password, or if the password was changed from another computer.

This dialog box 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.

> 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 Logon Manager or modify the account in Logon Manager.

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.

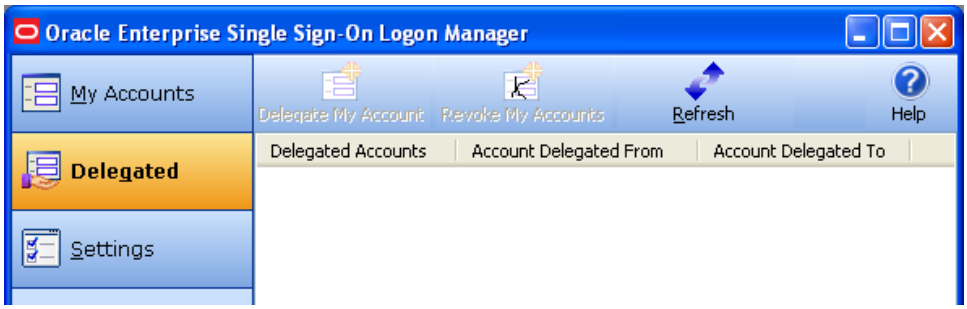
If you are experiencing logon loops, contact your administrator about enabling the grace period feature.

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.

Delegated Credentials in Logon Manager

When your Logon Manager 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.

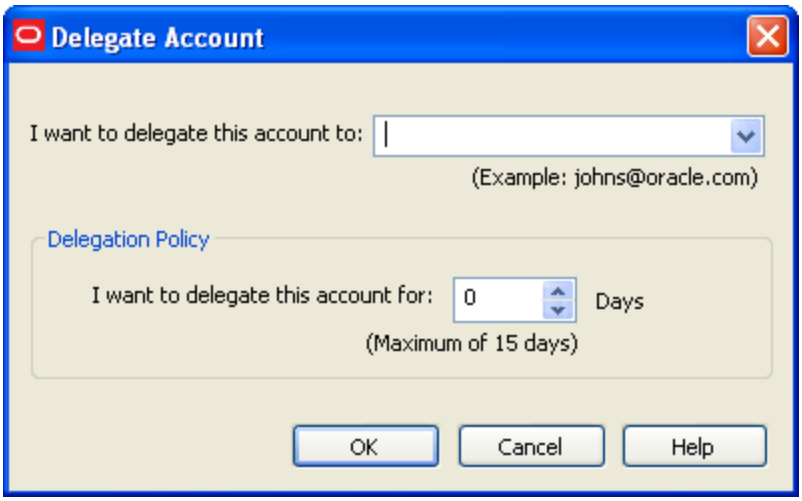
	Delegate My Account	Initiates the account delegation process. You will be prompted to designate another user to receive your account credentials and specify the conditions for the account access. After you delegate an account, it appears in the Delegated Accounts column.
	Revoke My Account	Allows you 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.

Delegating an Account to Another User

To delegate an account:

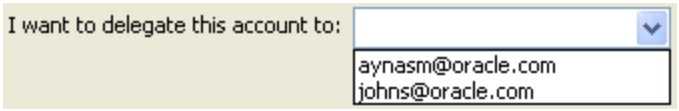
1. In the Delegated view of Logon Manager, select the account that you want to delegate.
2. Click the **Delegate My Account** icon.
3. Enter your password at the prompt.

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

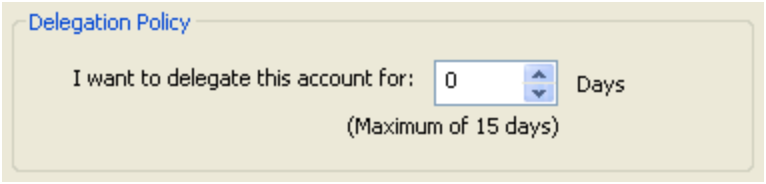


- To specify the delegatee:
  - Enter the delegatee's username (typically the user's email address).

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

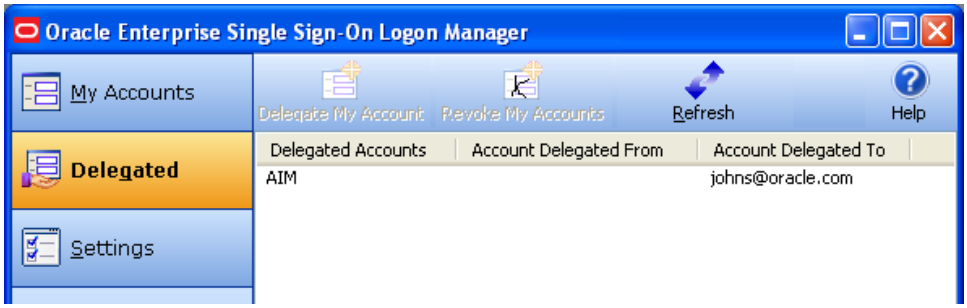


- To configure the policy, set the number of days that the delegatee can use this account. The maximum number of days appearing below this setting reflects what the administrator has set in the template policy.



5. Click **OK**.

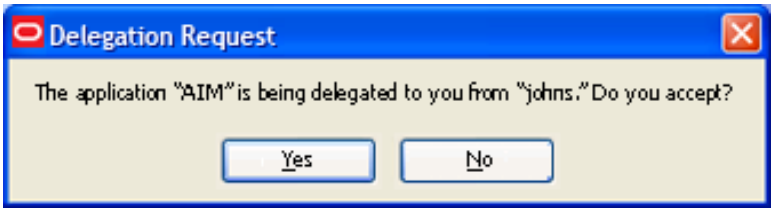
The account is delegated and the server receives an instruction to delegate the credential. After you complete the delegation process, the account appears on the Delegated tab in your Delegated Accounts list.



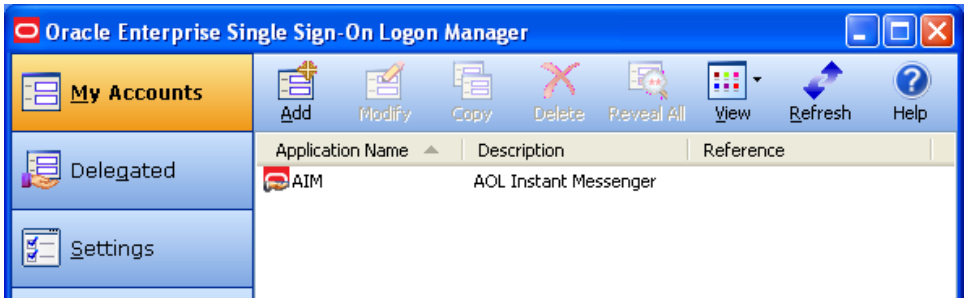
Receiving a Delegated Account from Another User

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

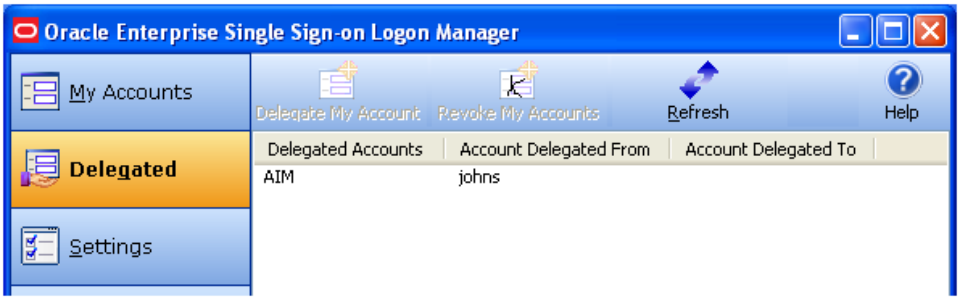
After you authenticate, a prompt appears asking you whether you accept the delegation.



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.

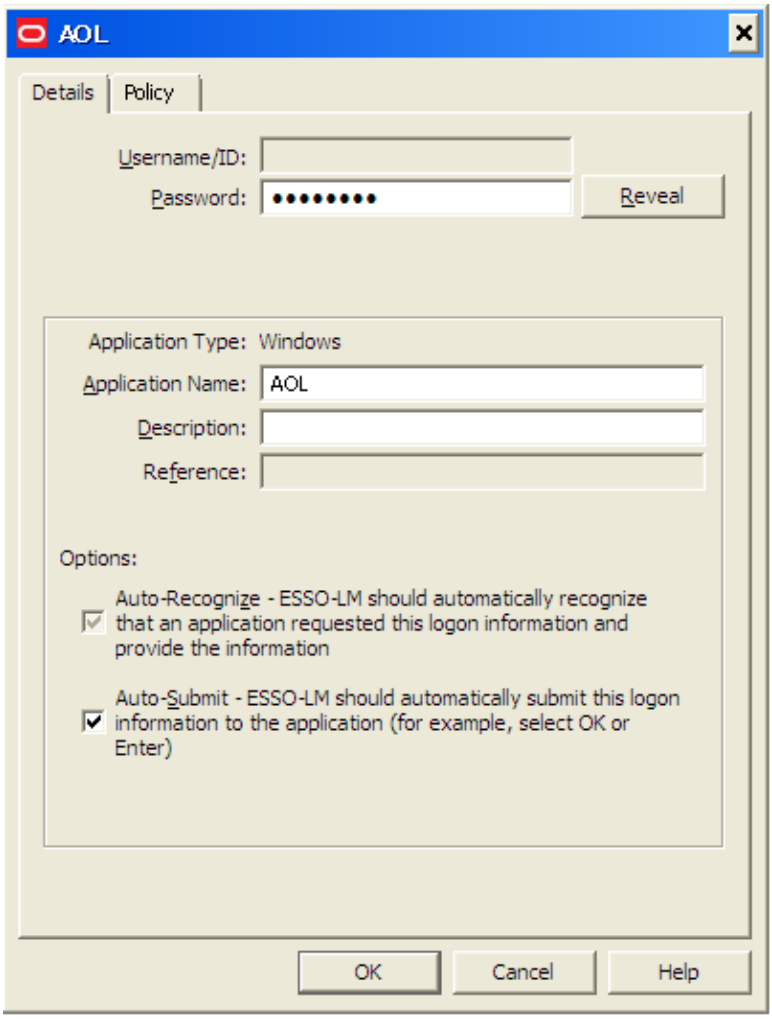


The account also appears in the Delegated Accounts column of the Delegated tab, with the name of the user who has delegated the account to you.

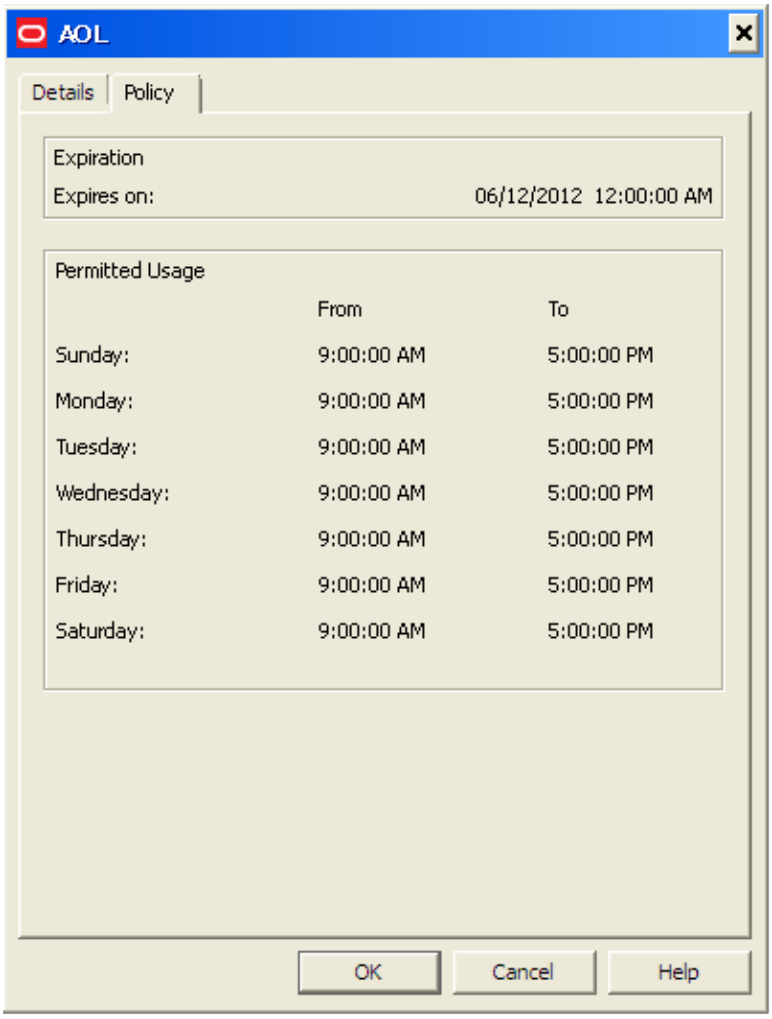


Viewing Delegated Account Properties

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.



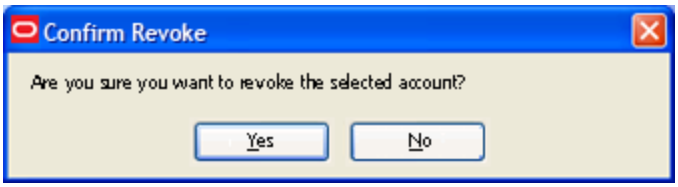
Updating Delegated Credentials

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.

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.

Working with Privileged Accounts

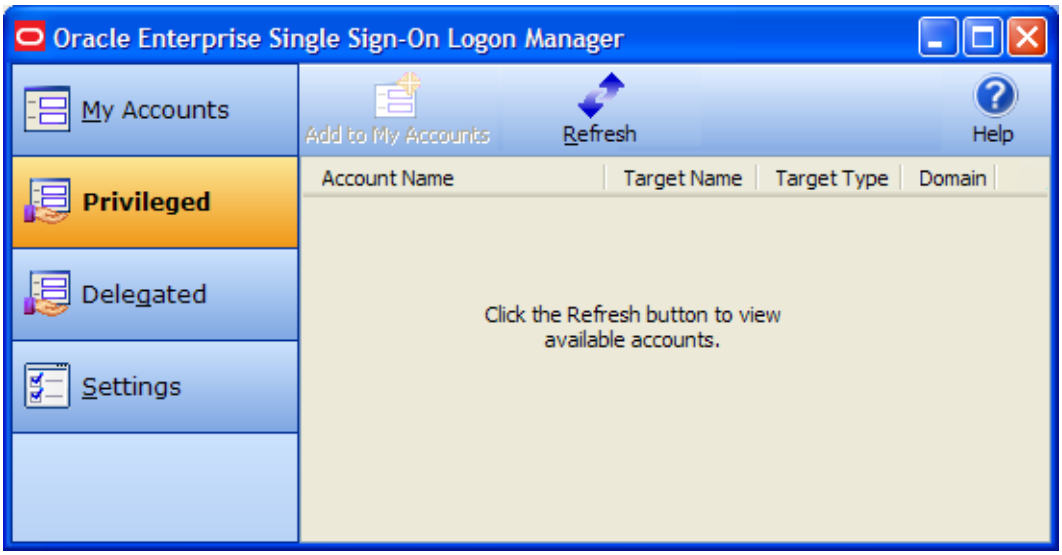
Privileged accounts apply to users responsible for key Information Technology resources, such as servers and databases. When you have been assigned the use of a privileged account, that account appears in the Privileged tab of Logon Manager.

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.

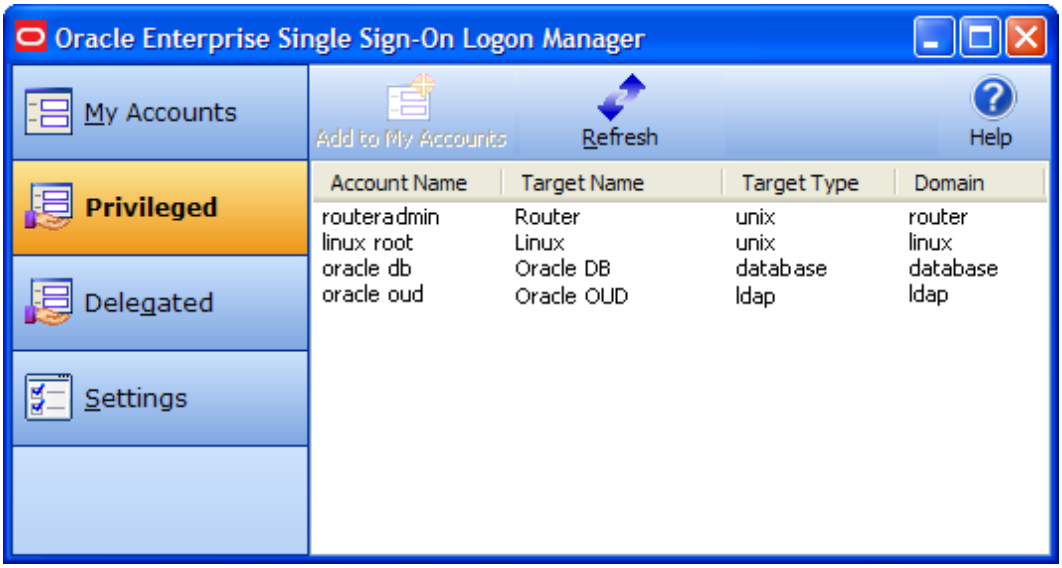
Displaying and Using Privileged Accounts

To display your privileged accounts:

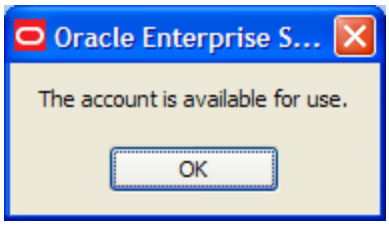
1. Open Logon Manager and select the **Privileged** tab.



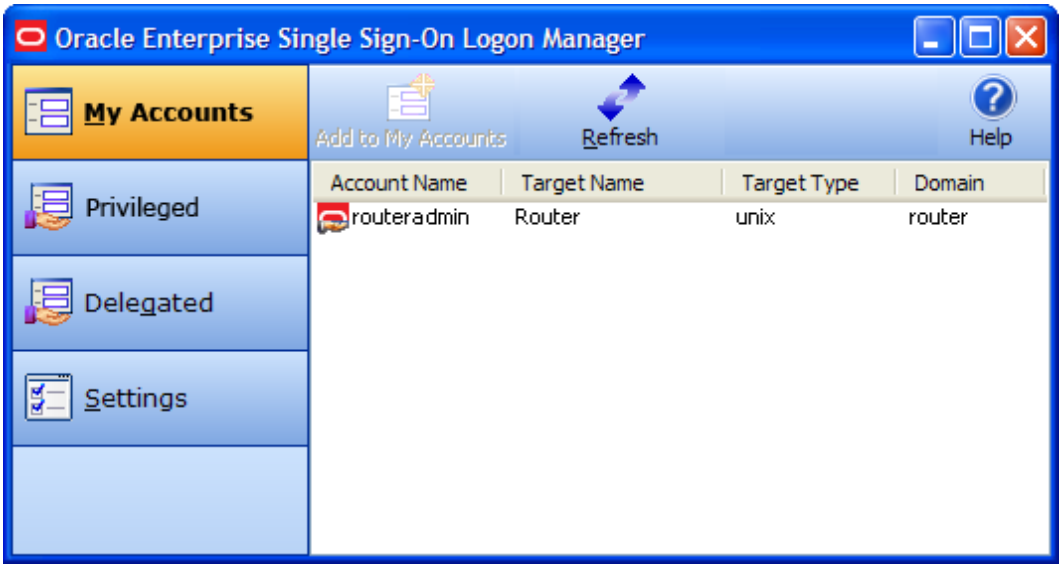
2. Click **Refresh** and fill in the fields in the Authentication dialog that appears. When the screen refreshes, you will see a list of all available privileged accounts assigned to you.



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.



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 if 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.

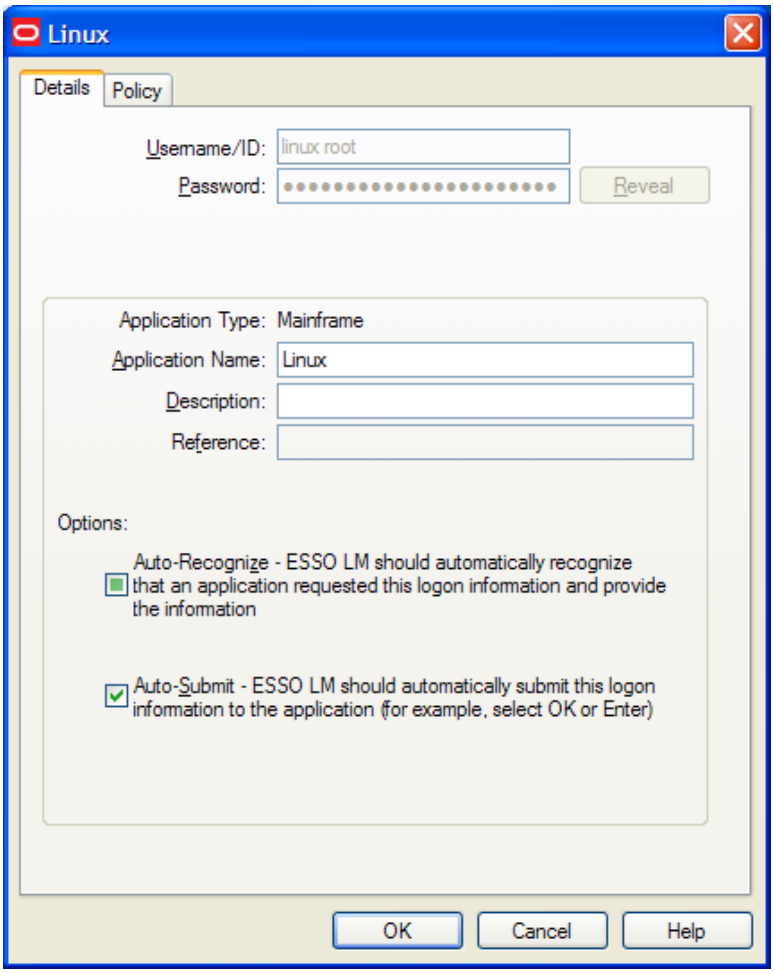
If an Account Is Unavailable

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

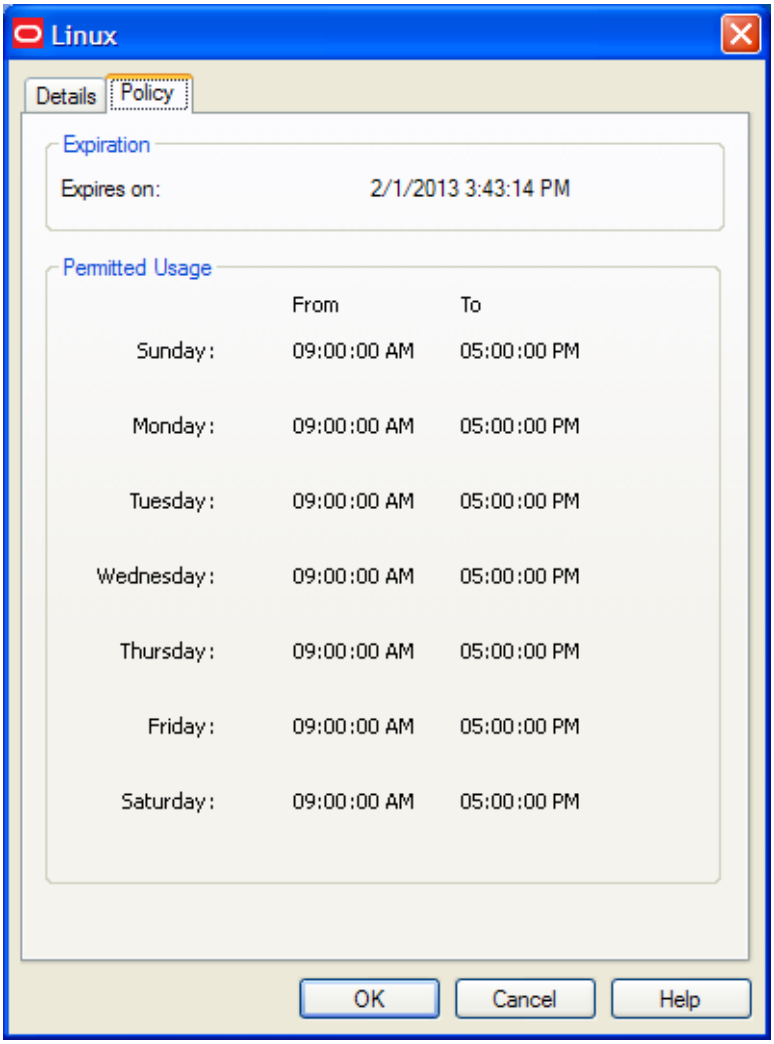
- Your attempt occurs outside of the policy's schedule. Review the account's properties to verify that you are working within the permitted schedule.
- The Provisioning Gateway server might be unavailable. Contact your administrator for help.
- An unspecified system error has occurred. Contact your administrator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

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.



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.

Settings

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

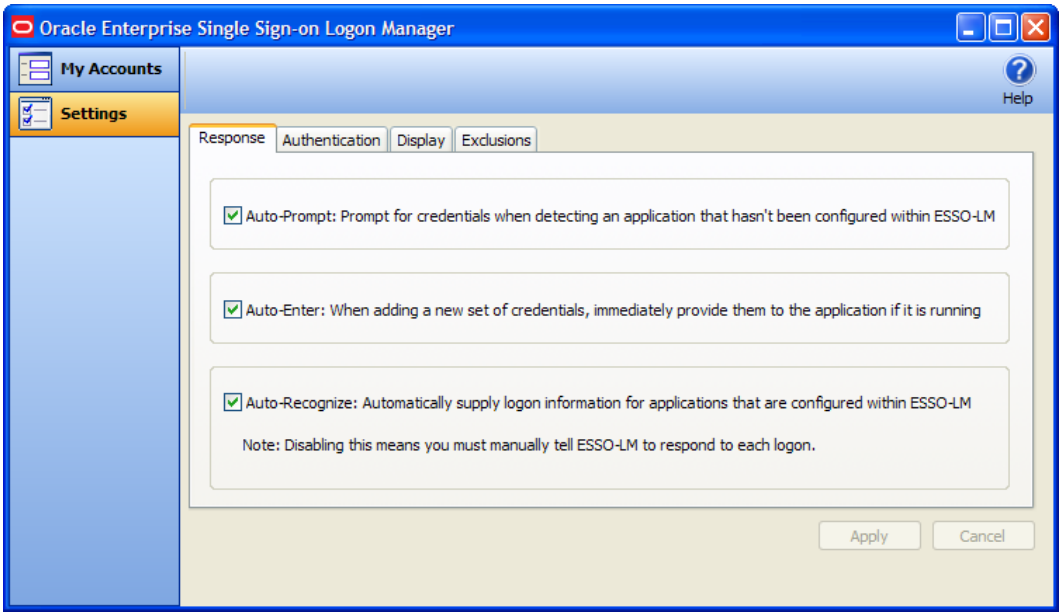
> Throughout the settings tabs, the **Apply** and **Cancel** buttons are unavailable until a change is made. Once a change is made, you can implement the changes by clicking **Apply**, or discard the changes by clicking **Cancel**.
>
> Changes made on the settings tabs take effect once **Apply** is clicked.

To View or Modify Logon Manager Settings:

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

Settings: Response Tab

The Response tab lets you control Logon Manager account features.



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

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 Logons Using Auto-Prompt for more information.

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.

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**.

Viewing or Modifying Response Settings

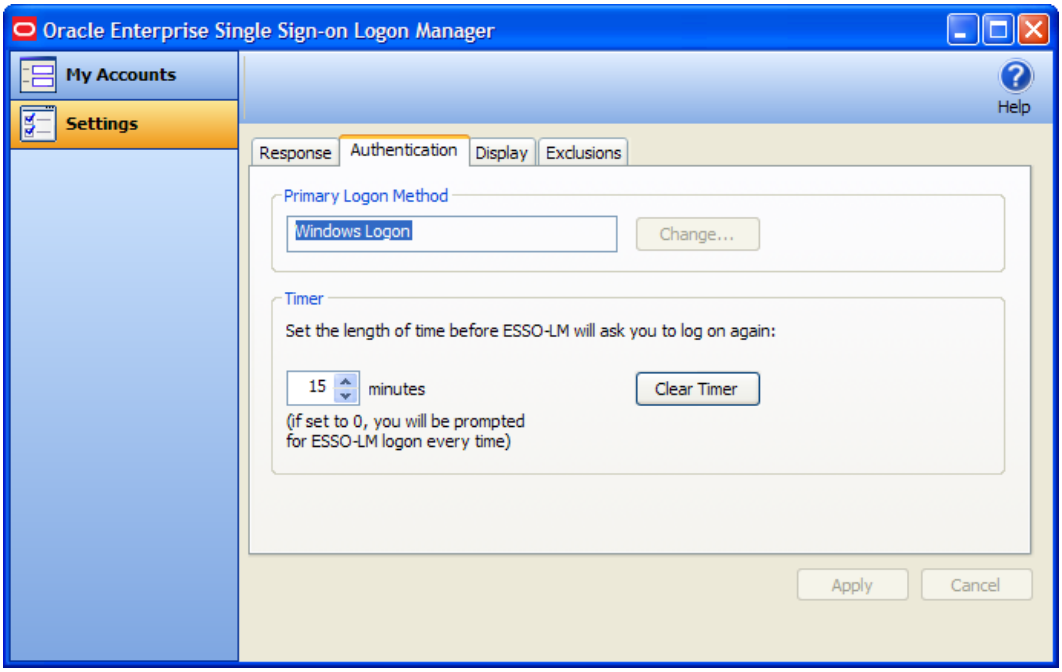
1. Open the Logon Manager.
2. On the **Settings** panel, click the **Response** tab.
3. When you have completed your changes, do one of the following:
   - Click **Apply** to confirm your changes (without closing the Logon Manager), then select another settings tab.

     or

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

Settings: Authentication Tab

The Authentication tab lets you control Logon Manager authentication features.



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

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 for more information.

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.

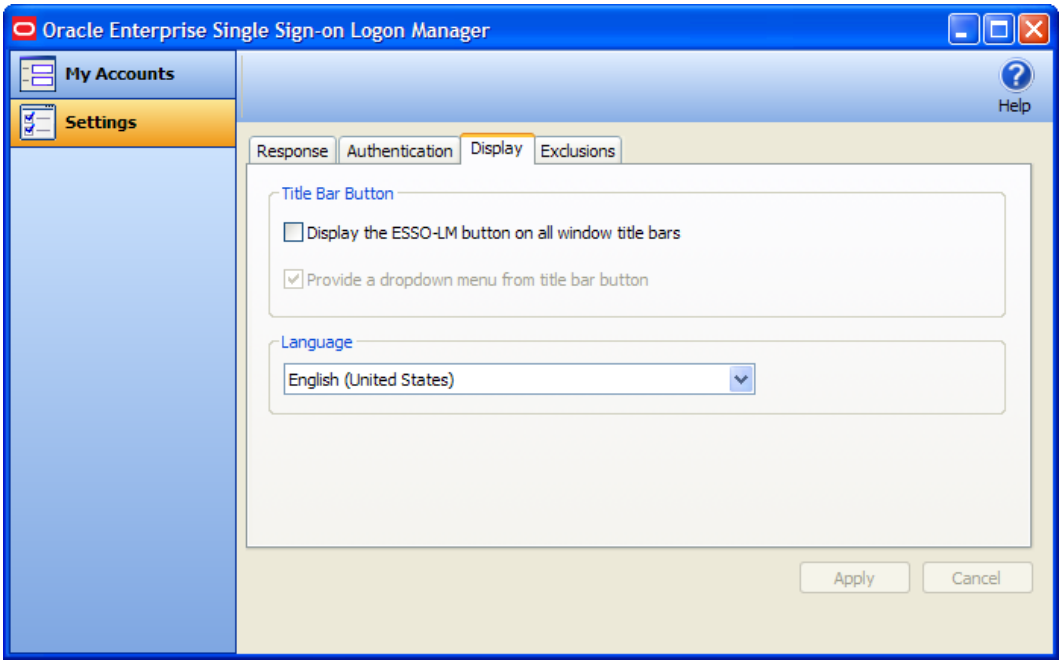
Viewing or Modifying Authentication Settings

1. Open the 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.

Settings: Display Tab

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



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

Title Bar Button

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 drop-down 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**.

Language

The Logon Manager Agent 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** drop-down.

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

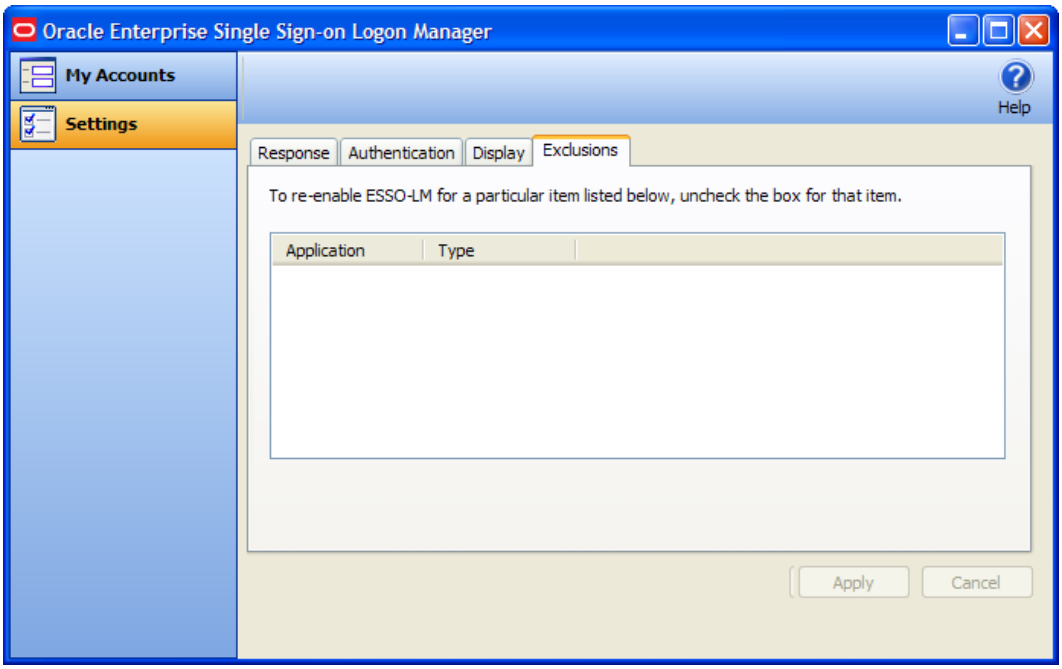
Viewing or Modifying Display Settings

1. Open the 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 the Logon Manager), then select another settings tab.

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

Settings: Exclusions Tab

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



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 an 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 box for now, and click **Cancel**.
- Permanently dismiss the logon dialog box 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.

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.

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.

Changing Your Application Password

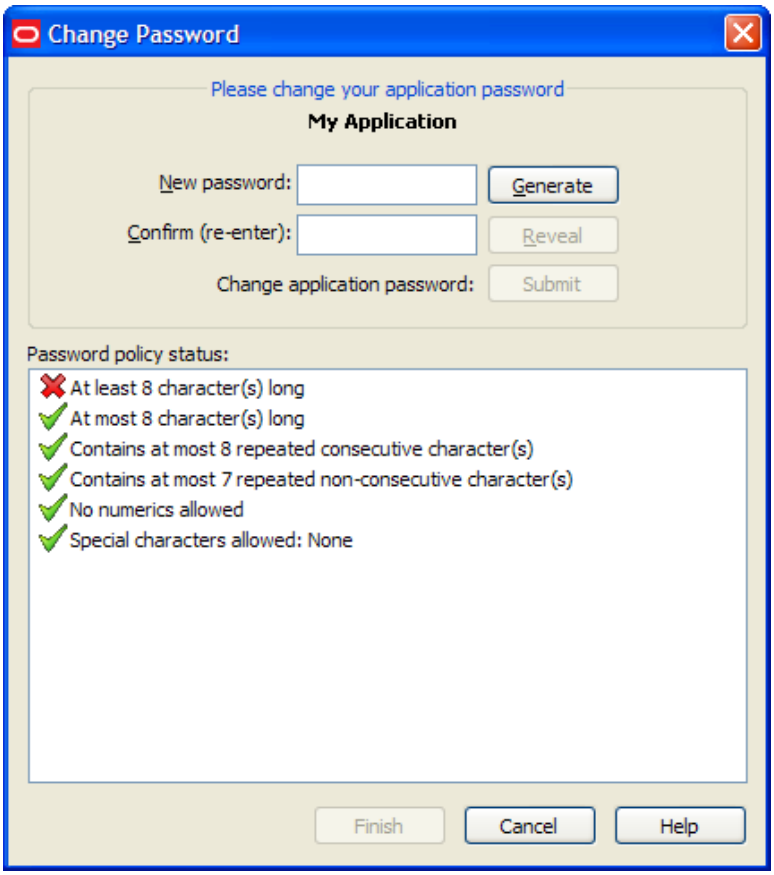
The Logon Manager automated password change increases security by eliminating the potential for poor password selection and poor password management. It also increases usability by saving you the trouble of creating, changing, and remembering passwords.

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 box, 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).



If the application displays its logon and password change fields in the same window, the Logon Manager 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.

     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 once 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."

     or

   - 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 the **OK** button and Logon Manager saves the password.

  If the password is rejected by the application, a message appears advising you that the password has been rejected by the application. You can either try a different password and resubmit, or click on the **Cancel** button.

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

About 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.

> 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.

Desktop Manager

The Desktop Manager is a logon dialog box 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:

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.

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.

Session Logon

The Desktop Manager includes 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 box appears, prompting you for your password. Enter your password and click **OK**.

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.

Resetting a Password

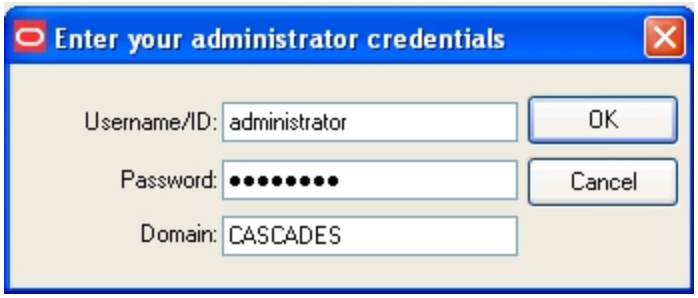
Depending on your system's configuration, a password reset banner might appear at the top of the Desktop Manager.

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

Terminating Sessions

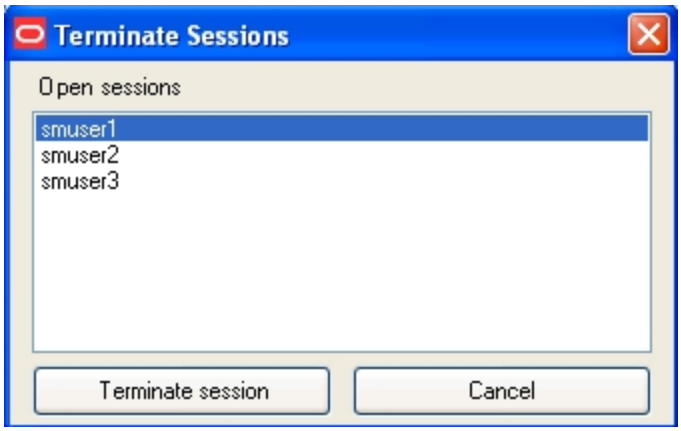
Administrators can terminate Kiosk Manager user sessions from the Desktop Manager by clicking **Terminate Sessions** from the **Administration** menu.

When clicked, the Authenticate as Administrator dialog appears prompting you to enter administrative credentials before performing this action.



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

The Terminate Sessions dialog appears prompting you to select a session to terminate.



Only one session can be selected at a time. Select a session from the **Open Sessions** list box and click **Terminate session**. The session will be removed from the Open sessions list.

Click **Cancel** to close this dialog.

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.

Locking and Unlocking Sessions

Do one of the following to lock a session:

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

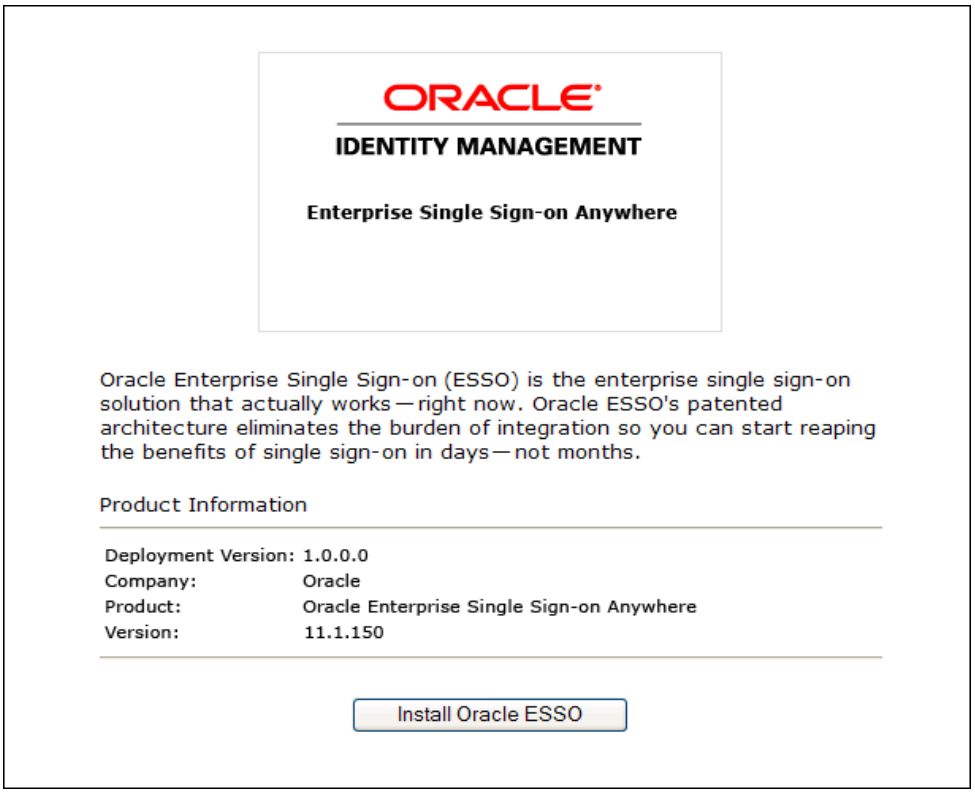
Part II. About Oracle Enterprise Single Sign-On Anywhere

Anywhere is the latest innovation in single sign-on (SSO) technology, using Microsoft's ClickOnce technology to deploy Oracle Enterprise Single Sign-On Logon Manager (Logon Manager) and Oracle Enterprise Single Sign-On Provisioning Gateway (Provisioning Gateway) to end users' desktops.

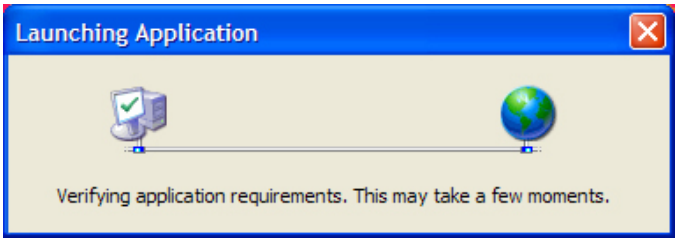
Using the Anywhere Console, the administrator creates a deployment package configured with the Oracle products needed by users of an enterprise, making the package available over a Web server or file share. Users download this deployment package from an HTML interface that is included with the Anywhere package, and which the administrator customizes. Users can then perform installations of the Oracle suite on their own workstations at the click of a button, with assurance that configurations are correct and ready to run, and without administrator intervention.

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, if applicable, (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.

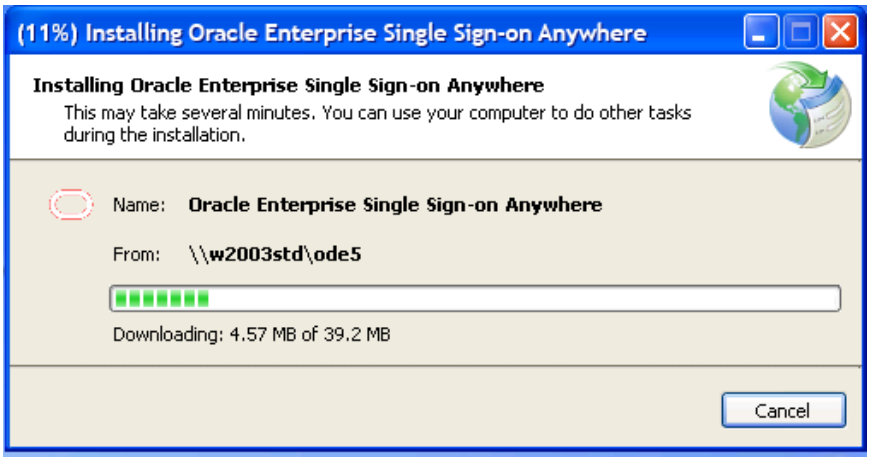


After Anywhere ascertains that all prerequisites are present on your workstation, Anywhere may ask you to verify that the installation certificate is valid. There are two possibilities:

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, and Provisioning Gateway if it is included in the Anywhere installation.

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:

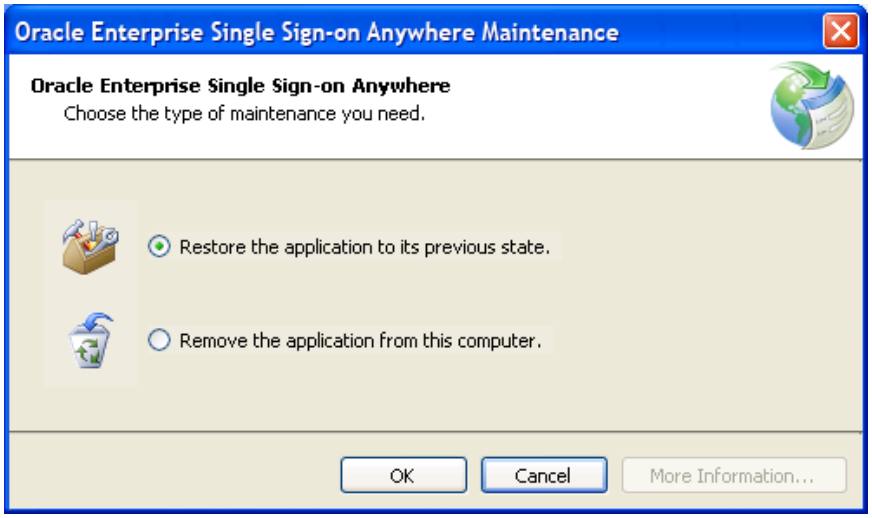
If your administrator has given you the option, you can choose to click **Skip** and not install the update. If you do not have the option or want to install the update, click **OK**.

Rolling Back Anywhere

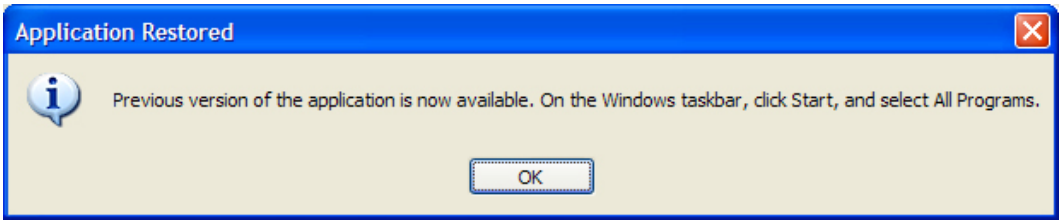
If your administrator decides to roll back your version of Anywhere to an earlier version, you will receive a notification.

To perform a rollback:

1. Go to **Control Panel** > **Add or Remove Programs**.
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.



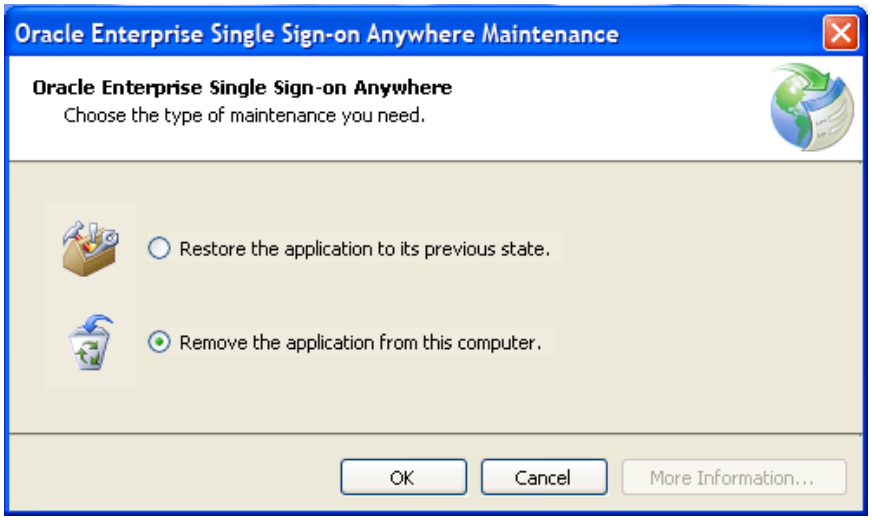
4. When the **Application Restored** window displays, click **OK**.



Uninstalling Anywhere

To uninstall Anywhere:

1. Go to **Control Panel** > **Add or Remove Programs**.
2. Select **Anywhere** from the program list, and click **Change/Remove**.
3. Select **Remove the application from this computer**.
4. Click the **OK** button.



Part III. About Oracle Enterprise Single Sign-On 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 a separate component in the Oracle Enterprise Single Sign-On Suite, 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 Password Reset Enrollment Interview.

After you complete your Enrollment Interview, you can take the Password Reset 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.

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."

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.

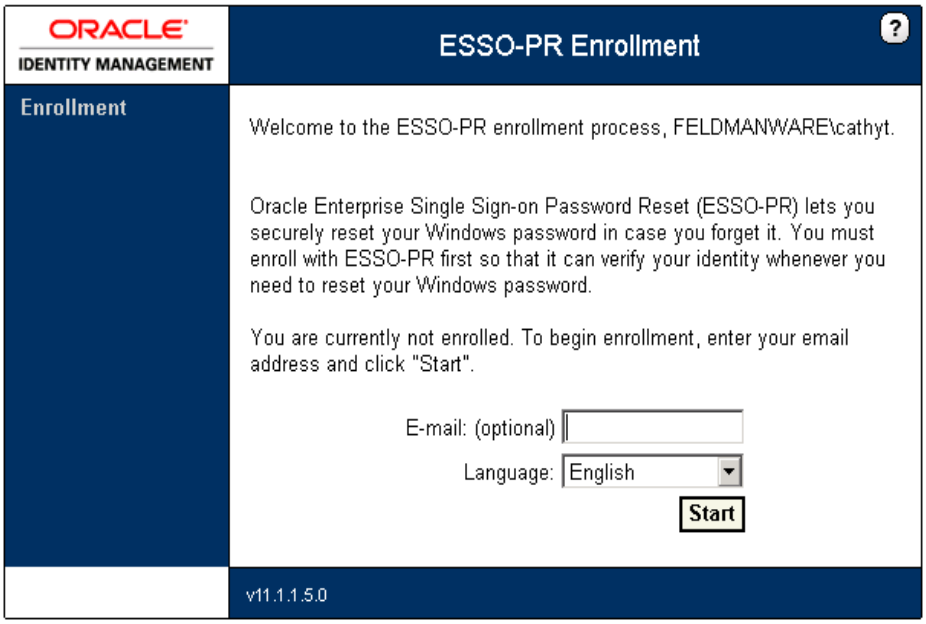
There are no wrong answers during enrollment, but the answers that you supply here must match your answers if you ever have to take the Reset Quiz, so it is important that you select answers that you will remember easily. During enrollment, Password Reset continues to present questions until you have 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.

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.

> 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.

> It is important that you keep your answers to the questions as brief and as memorable as possible.

Enrollment Questions

There are two types of questions in the Enrollment Interview.

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**.

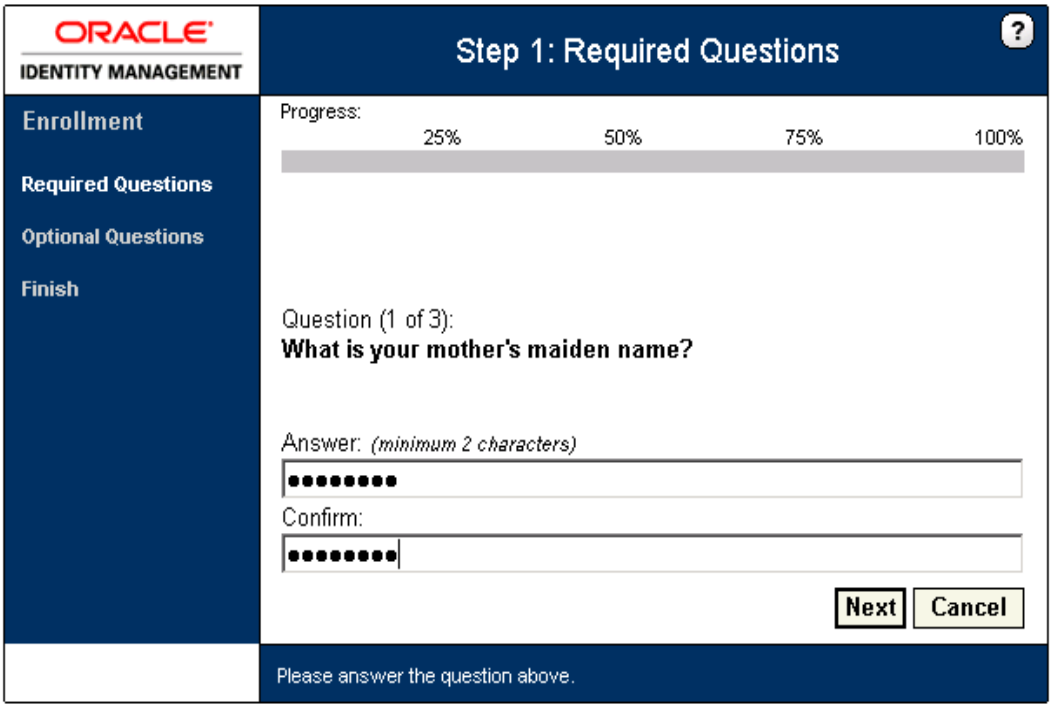
Optional Questions

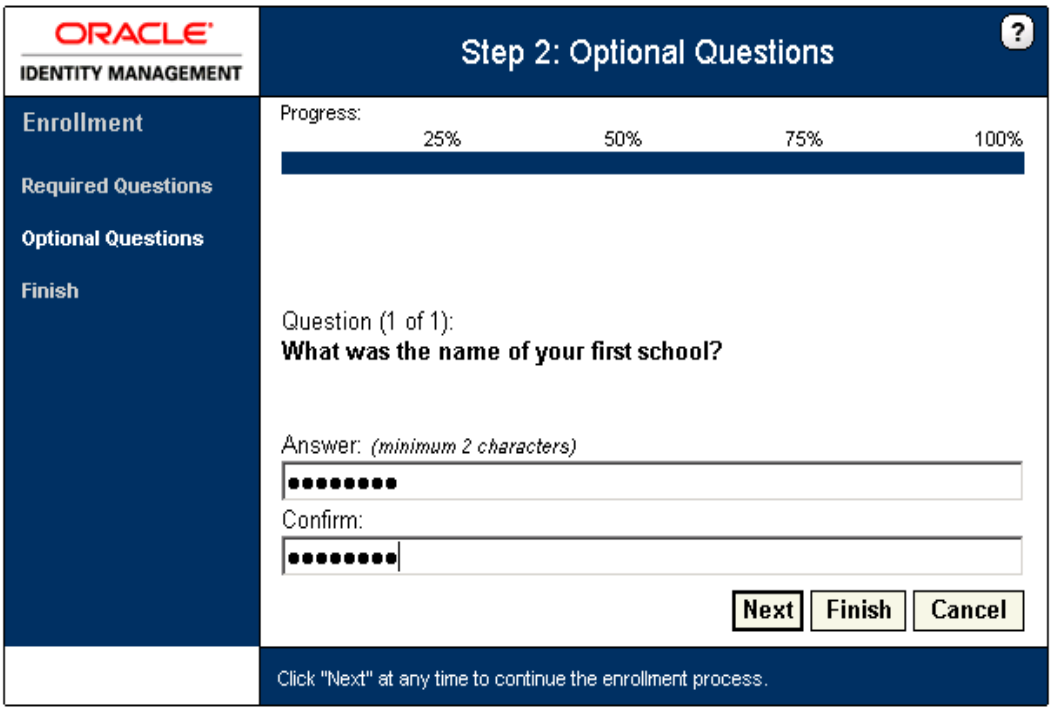
You have the option to answer these questions or skip them. Remember that the more questions you choose to answer, the more secure the quiz will be.

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.



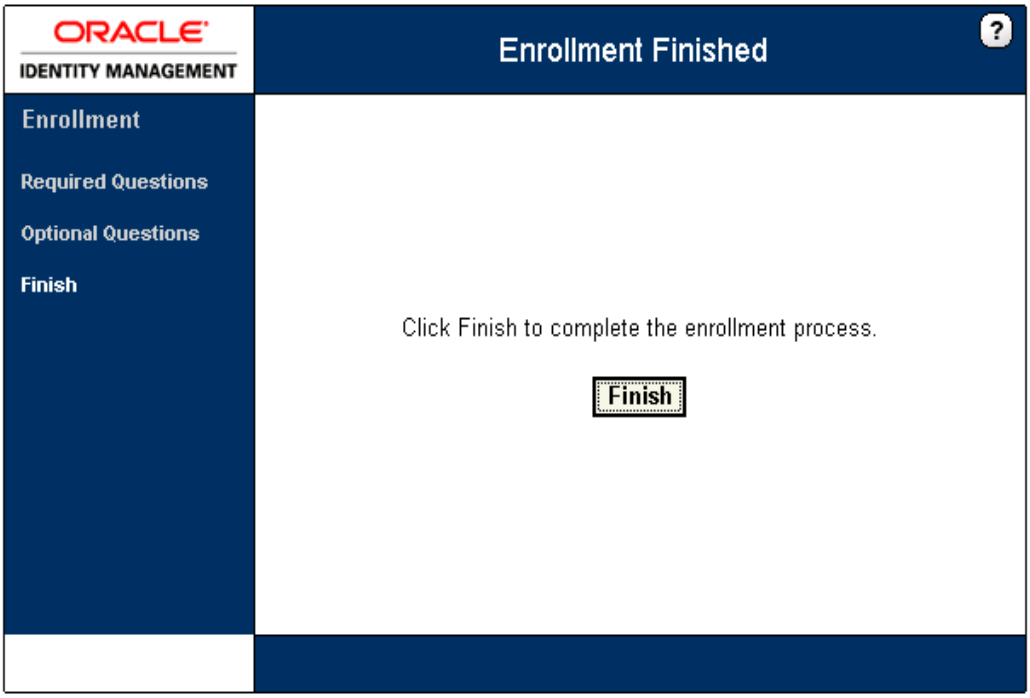


After you answer each question, click **Next** to proceed with the interview. If at any time you decide not to answer any more optional questions, or when you have answered all the questions presented, click **Finish**.

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** .

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 box. At the Password Reset reset logon dialog box, 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 box 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.

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.

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.

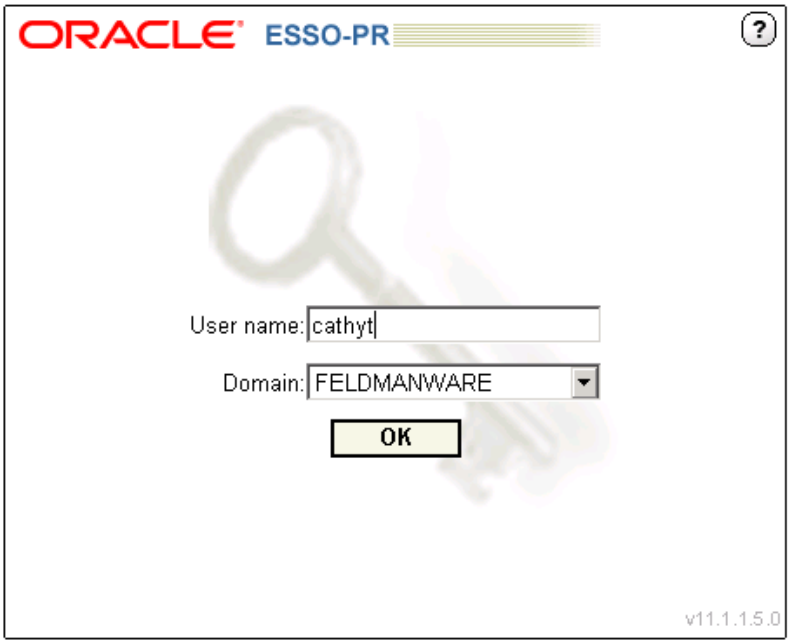
Starting the Reset Quiz at the Windows Logon (On Your Own Workstation)

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.

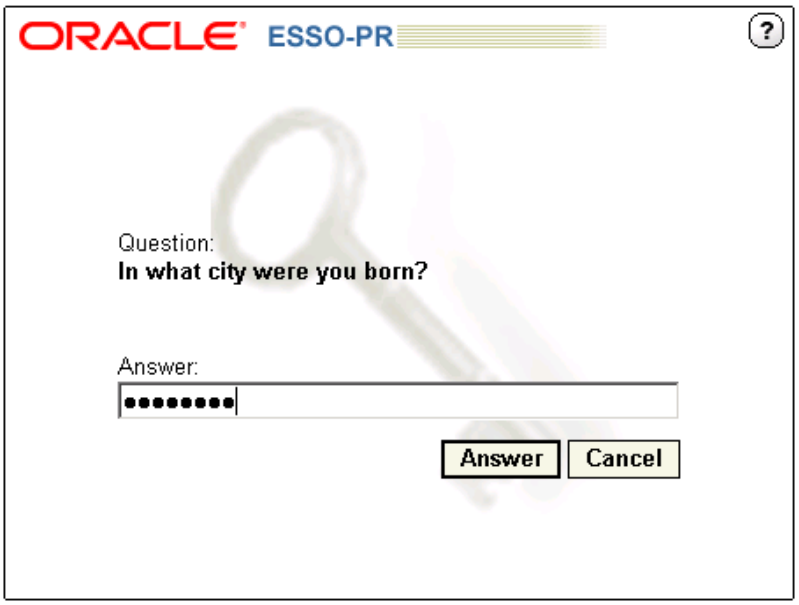
Starting the Reset Quiz From a Logged-On Workstation

> 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. Type 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.

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.

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.

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.