

**Oracle® Enterprise Single Sign-On
Universal Authentication Manager**

User's Guide

Release 11.1.2

E29808-02

August 2012

E29808-01

Copyright © 2012, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Table of Contents

Use the Welcome page to connect to the help sections below.....	4
About Universal Authentication Manager.....	4
Configuring Universal Authentication Manager.....	6
Using Universal Authentication Manager.....	16

Use the Welcome page to connect to the help sections below.

- [Selecting the Client Mode](#)
- [Settings](#)
- [Enrolling Credentials](#)

See the *Oracle Enterprise Single Sign-On User's Guide* for a full discussion of using Universal Authentication Manager.

About Universal Authentication Manager

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

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

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

- [Logon Methods](#)
- [Settings](#)

The Universal Authentication Manager logon and re-authentication dialogs allow you to quickly and securely log on to Windows with any authentication device, such as an RFID badge or non-Windows smart card. For more information, see [Using Universal Authentication Manager](#).

Fingerprints

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



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

The following actions are available:

- [Enrolling a Fingerprint at Windows Logon](#)
- [Enrolling a Fingerprint when Launching the Universal Authentication Manager Client](#)
- [Changing Your Universal Authentication Manager PIN](#)
- [Fingerprint Settings](#)

Proximity Cards

A passive proximity card or token is an identity object (such as a workplace ID badge) containing a circuit that a card-reading device can detect and decipher. When you place a proximity card close to a card reader, the reader detects the token's presence and recognizes identifying information that is associated with you. Universal Authentication Manager also gives you the option (depending on your system configuration) to require a secret PIN during logon for more secure two-factor authentication.

The following actions are available:

- [Enrolling a Proximity Card at Windows Logon](#)
- [Enrolling a Proximity Card when Launching the Universal Authentication Manager Client](#)
- [Enrolling a Proximity Card Manually](#)
- [Changing Your Universal Authentication Manager PIN](#)
- [Proximity Card Settings](#)

Smart Cards

A smart card is a credit card-sized token containing a chip or embedded circuits that can store and process data securely. Information stored on a smart card can also be used for identification and authentication. Universal Authentication Manager enables you to enroll and use smart cards for logon and authentication without writing any data on the smart card chip. Universal Authentication Manager also gives you the option (depending on your system configuration) to require a smart card PIN during logon for more secure authentication.

The following actions are available:

- [Enrolling a Smart Card at Windows Logon](#)
- [Enrolling a Smart Card when Launching the Universal Authentication Manager Client](#)
- [Changing Your Universal Authentication Manager PIN](#)
- [Enrolling a Smart Card Manually](#)
- [Smart Card Settings](#)



When using a smart card, the card's own PIN cannot be changed. Only a Universal Authentication Manager PIN associated with the smart card can be changed. For more information, see [Configuring Universal Authentication Manager](#).

Challenge Questions

Challenge Questions is a question-and-answer quiz that your administrator may choose to enable as a fallback logon method when authentication via other enrolled methods fails. Challenge Questions requires you to correctly answer enough questions (which you have selected and provided answers for when you first enrolled this method) to satisfy the weight requirement for successful logon set by the administrator.

- [Enrolling Challenge Questions at Windows Logon](#)
- [Enrolling Challenge Questions when Launching the Universal Authentication Manager Client](#)
- [Enrolling Challenge Questions Manually](#)
- [Challenge Questions Settings](#)


Configuring Universal Authentication Manager

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

- [Fingerprint](#)
- [Proximity Card](#)
- [Smart Card](#)
- [Challenge Questions](#)
- [Windows Password](#)
- [Availability of Settings Depending on Client Mode](#)


Fingerprint Settings

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

Logon Method Enabled	<p>Controls if an installed authenticator is enabled or disabled. This policy setting enhances security by controlling the specific logon methods you are allowed to use. Options are Yes (default setting) and No.</p> <div data-bbox="511 907 1339 1008" style="border: 1px solid black; background-color: #ffffcc; padding: 5px;">  The Logon Method Enabled setting is only displayed if you are working in local mode. In enterprise mode, this setting is not displayed. </div>
Number of fingers	<p>Specifies the number of finger samples you are required to enroll. This policy requires you to enroll exactly the specified number of finger samples during enrollment. Default is 1. Maximum is 10.</p>
PIN Required	<p>Specifies whether you must submit a PIN in order to be authenticated. Options are Yes (default setting) or No.</p>
PIN Minimum Length	<p>The minimum allowed length for the PIN. Possible values are 4-16 characters (default setting is 4 characters).</p>
PIN Allowed Characters	<p>Restricts the character type(s) you can use in your PIN. Options are numeric only, alphanumeric, or any characters (default setting).</p>


Proximity Card Settings

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

Logon Method Enabled	<p>Controls if an installed authenticator is enabled or disabled. This policy setting enhances security by controlling the specific logon methods you are allowed to use. Options are Yes (default setting) and No.</p> <div data-bbox="548 472 1310 573" style="border: 1px solid black; background-color: #ffffcc; padding: 5px;"> The Logon Method Enabled setting is only displayed if you are working in local mode. In enterprise mode, this setting is not displayed.</div>
Removal Action	<p>Controls how Universal Authentication Manager behaves when you "tap out" your proximity card (tap your card against the reader a second time during a session). Options are:</p> <ul style="list-style-type: none">• No Action• Lock workstation (locks the workstation; you must re-authenticate to return to your session)• Force Logoff (automatically logs you off the workstation)
PIN Required	<p>Specifies whether you must submit a PIN for your card in order to be authenticated. Options are Yes (default setting) or No.</p>
PIN Minimum Length	<p>The minimum allowed length for the proximity card PIN. Possible values are 4-16 characters (default setting is 4 characters).</p>
PIN Allowed Characters	<p>Restricts the character type(s) you can use in your proximity card PIN. Options are numeric only, alphanumeric, or any characters (default setting).</p>


Smart Card Settings

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

<p>Logon Method Enabled</p>	<p>Controls if an installed authenticator is enabled or disabled. This policy setting enhances security by controlling the specific logon methods you are allowed to use. Options are Yes (default setting) and No.</p> <div data-bbox="548 474 1308 575" style="border: 1px solid black; background-color: #ffffcc; padding: 5px;">  The Logon Method Enabled setting is only displayed if you are working in local mode. In enterprise mode, this setting is not displayed. </div>
<p>Removal Action</p>	<p>Controls how Universal Authentication Manager behaves when you remove your smart card. Options are:</p> <ul style="list-style-type: none"> • No Action • Lock workstation (locks the workstation; you must re-authenticate to return to your session) • Force Logoff (automatically logs you off the workstation)
<p>PIN Type</p>	<p>Specifies whether to use the card's internal preconfigured PIN or create and store a PIN within Universal Authentication Manager's secure data store. Options are Smart Card PIN (default setting) or ESSO-UAM PIN.</p>
<p>PIN Minimum Length</p>	<p>(ESSO-UAM PIN type only) The minimum allowed length for the smart card PIN. Possible values are 4-16 characters (default setting is 4 characters).</p>
<p>PIN Allowed Characters</p>	<p>(ESSO-UAM PIN type only) Restricts the character type(s) you can use in your smart card PIN. Options are numeric only, alphanumeric, and any characters (default setting).</p>


Challenge Questions Settings

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

<p>Logon Method Enabled</p>	<p>Controls if an installed authenticator is enabled or disabled. This policy setting enhances security by controlling the specific logon methods you are allowed to use. Options are Yes (default setting) and No.</p> <div data-bbox="548 1377 1308 1478" style="border: 1px solid black; background-color: #ffffcc; padding: 5px;">  The Logon Method Enabled setting is only displayed if you are working in local mode. In enterprise mode, this setting is not displayed. </div>
------------------------------------	--

Windows Password Settings

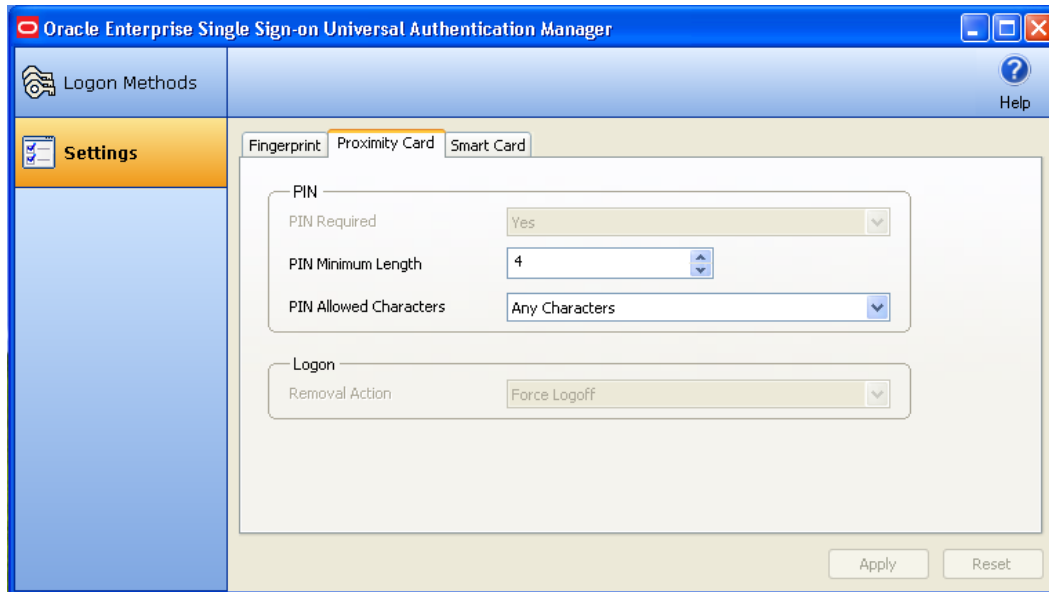
On the **Windows Password** tab, you may be able to view or configure the following settings:

<p>Logon Method Enabled</p>	<p>Controls if an installed authenticator is enabled or disabled. This policy setting enhances security by controlling the specific logon methods you are allowed to use. Options are Yes (default setting) and No.</p> <div data-bbox="548 1772 1308 1873" style="border: 1px solid black; background-color: #ffffcc; padding: 5px;">  The Logon Method Enabled setting is only displayed if you are working in local mode. In enterprise mode, this setting is not displayed. </div>
------------------------------------	--

Availability of Settings in Enterprise Mode

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

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



For more information, see [Selecting the Client Mode](#).

Selecting the Client Mode

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

Enterprise Client Mode

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

Local Client Mode

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

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

the bottom of the screen. To cancel your changes and return settings to their previous state, click **Reset**.

For more information, see [Settings](#).

Integrating with Logon Manager

Universal Authentication Manager can operate as a stand-alone application and also integrate seamlessly with Logon Manager. If your administrator has enabled and installed the Universal Authentication Manager authenticator during a Universal Authentication Manager custom installation, the Universal Authentication Manager authenticator will be added to the list of Logon Manager logon methods. If you wish to configure Logon Manager to use Universal Authentication Manager as its primary logon method, you must make this change using the first-time use wizard, or manually from Logon Manager.

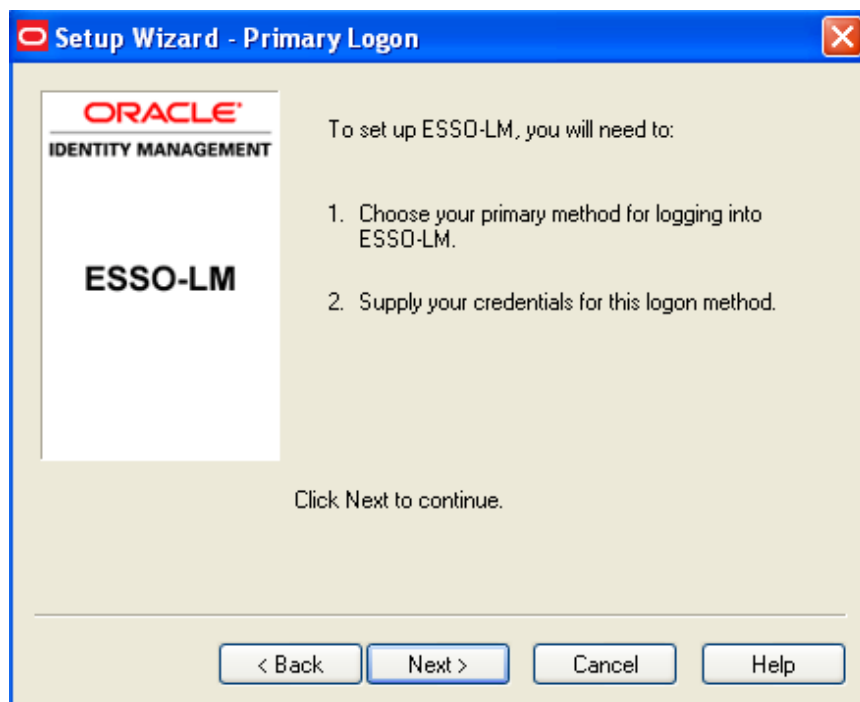


Universal Authentication Manager authenticator must be installed before you can configure Universal Authentication Manager as the primary logon method for Logon Manager. For details on installing the necessary integration components, see the *Oracle Enterprise Single Sign-On Suite Plus Installation Guide*.

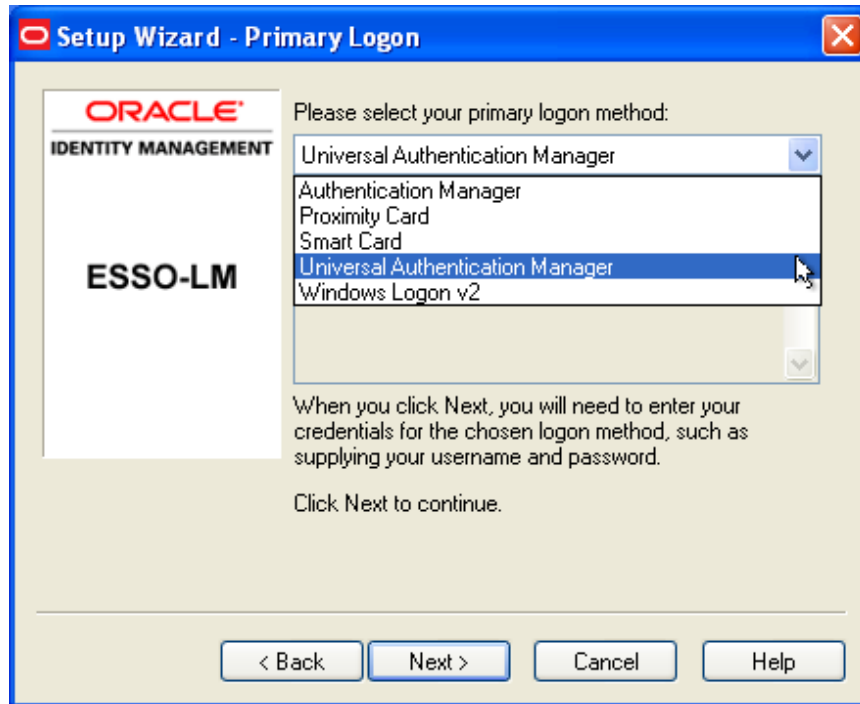
Configuring Universal Authentication Manager as the Primary Logon Method with the First-Time Use Wizard

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

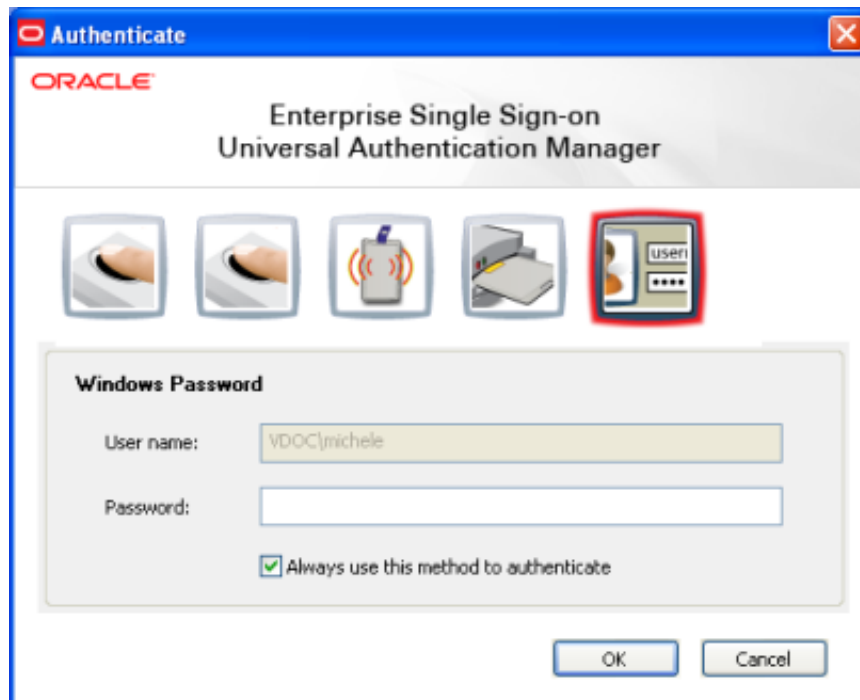
1. Click **Start** > **Programs** > **Oracle** > **Logon Manager** > **Logon Manager**. The First-Time Use wizard opens. Click **Next** on the first screen of the wizard.



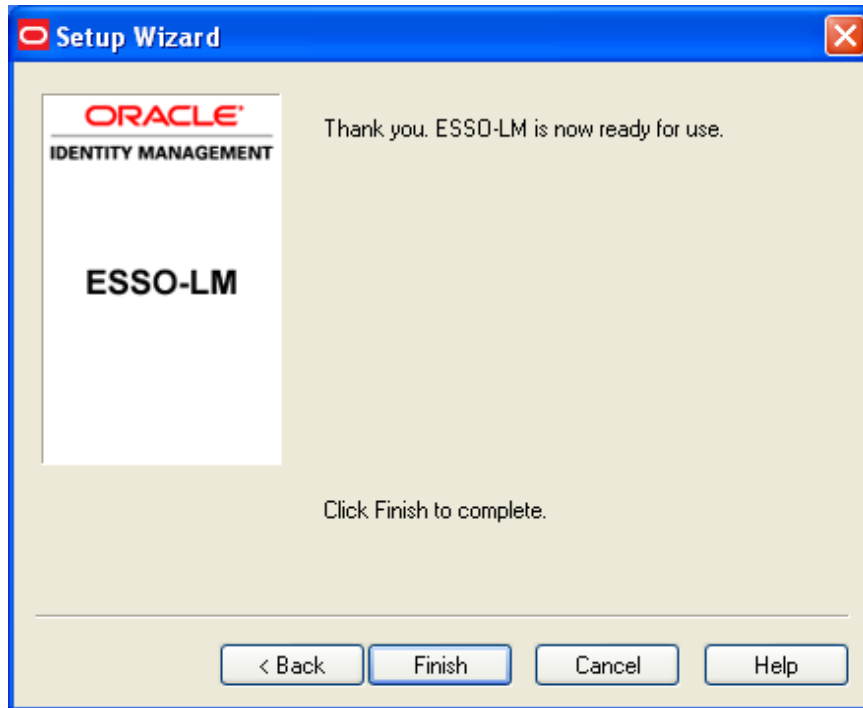
2. Click **Next** again.
3. Select **Universal Authentication Manager** from the list of available primary logon methods and click **Next**.



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



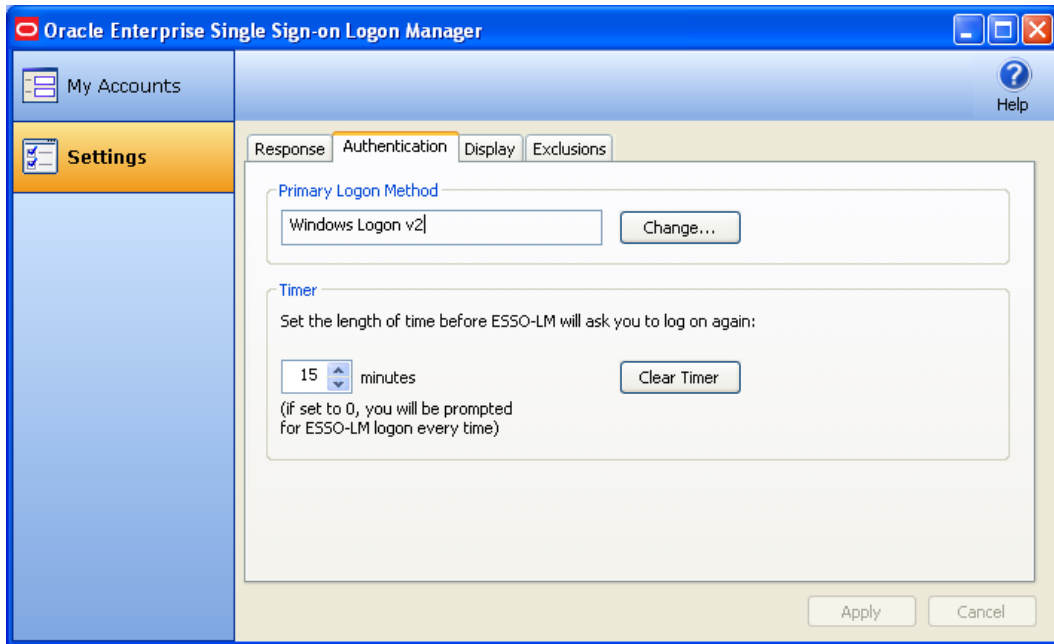
5. Logon Manager displays a message informing you that it is ready for use. Universal Authentication Manager is now configured as your primary logon method. Click **Finish** to complete the wizard.



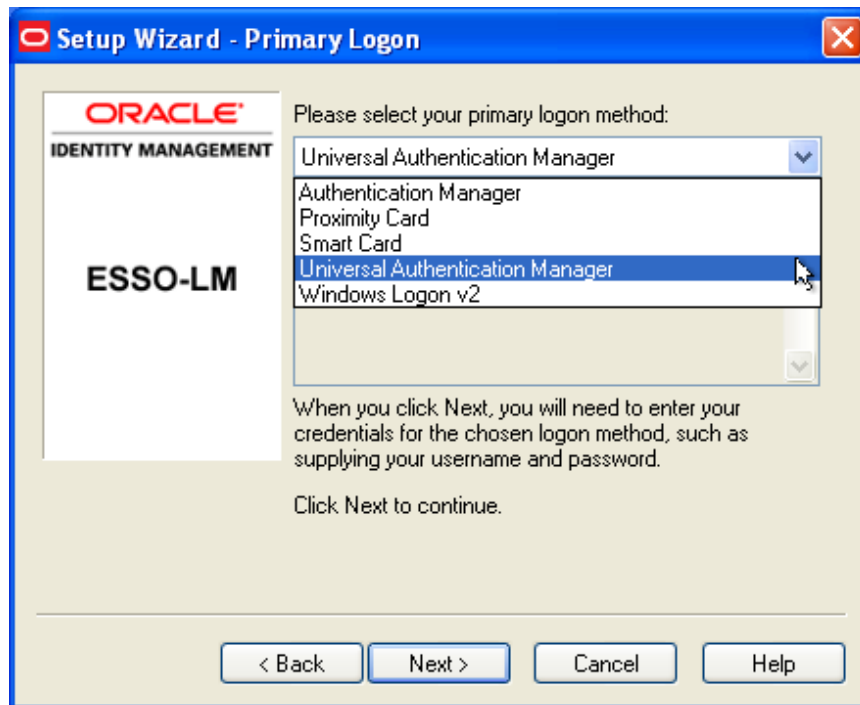
Configuring Universal Authentication Manager as the Primary Logon Method Using Logon Manager

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

1. Click **Start > Programs > Oracle > Logon Manager > Logon Manager**. The Logon Manager icon appears in the system tray. Launch Logon Manager.
2. Select **Settings**, then click the **Authentication** tab.



3. In the Primary Logon Method section, click **Change...**The Primary Logon Setup Wizard opens. Click **Next** to proceed.
4. Enter your Windows password or authenticate to your currently enrolled logon method when prompted.
5. From the list of available primary logon methods, select **Universal Authentication Manager**. Click **Next**.

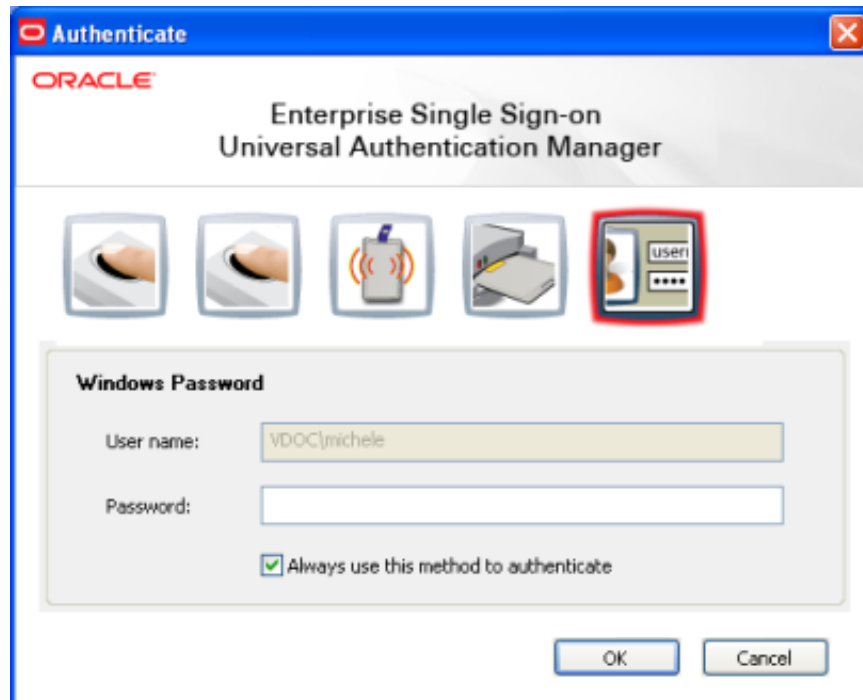


- The Universal Authentication Manager authentication dialog is displayed; enter your Windows password or authenticate with another enrolled logon method.

Authenticating With Universal Authentication Manager When Prompted by Logon Manager

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

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



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

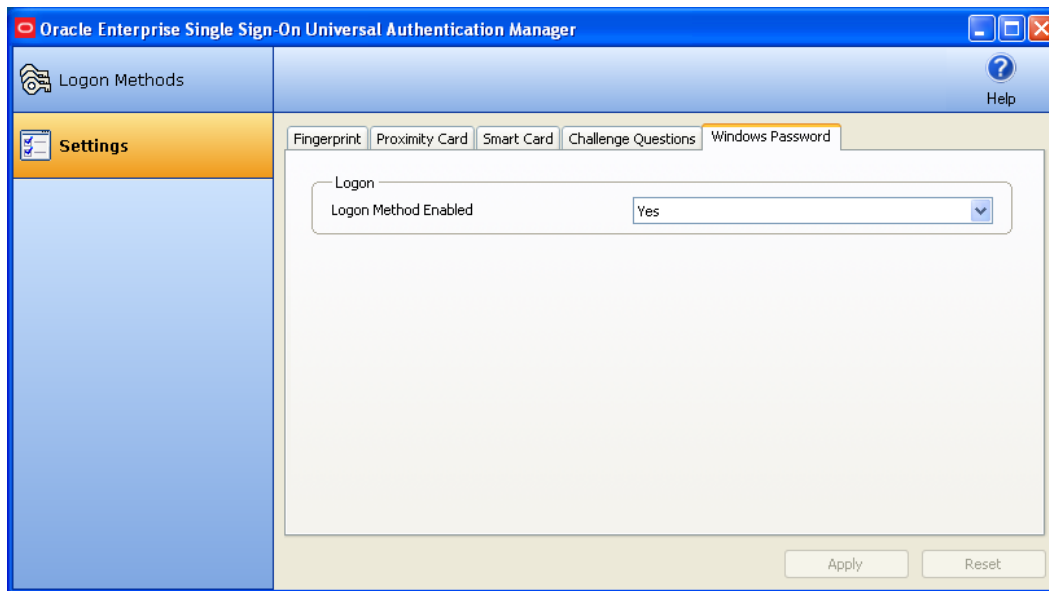
Logon Method Enabled

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

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

- In enterprise mode, the Logon Method Enabled policy setting is an Administrative policy only. This means that the policy will never appear in the Universal Authentication Manager settings.


- In the local client mode, the Logon Method Enabled policy setting is an end-user policy setting. You can manage the policy setting right from the Settings tab in the Universal Authentication Manager :



Windows Password Exception

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

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

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

Logon Method Enabled Rules

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

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

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

Configuring Universal Authentication Manager to Lock a Workstation



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

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

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



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

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

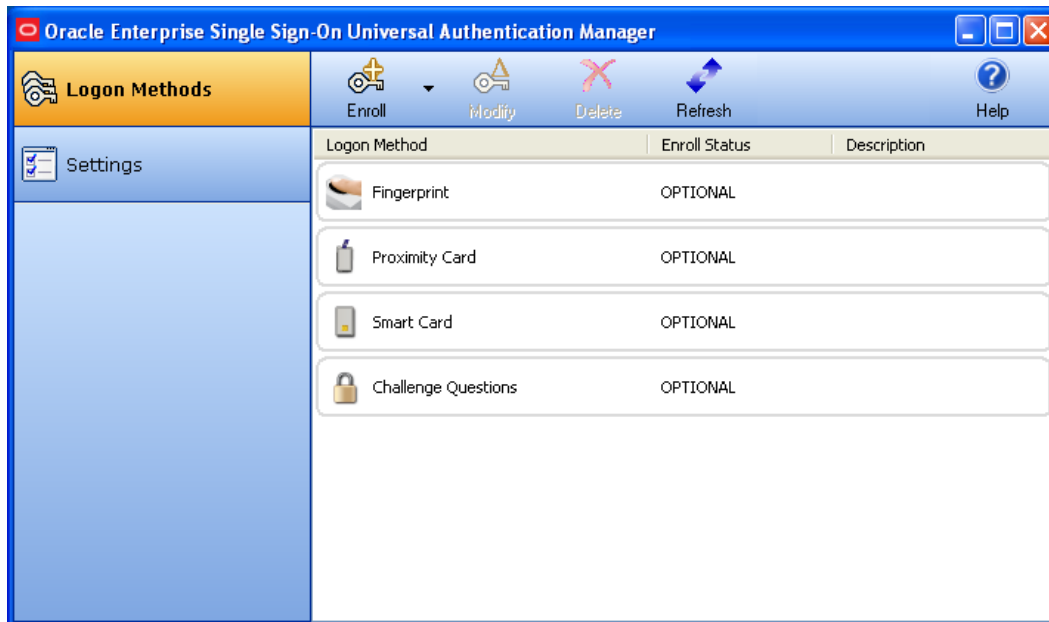
For more information about **Removal Action** and other settings, see [Settings](#).

Using Universal Authentication Manager

To start Universal Authentication Manager:

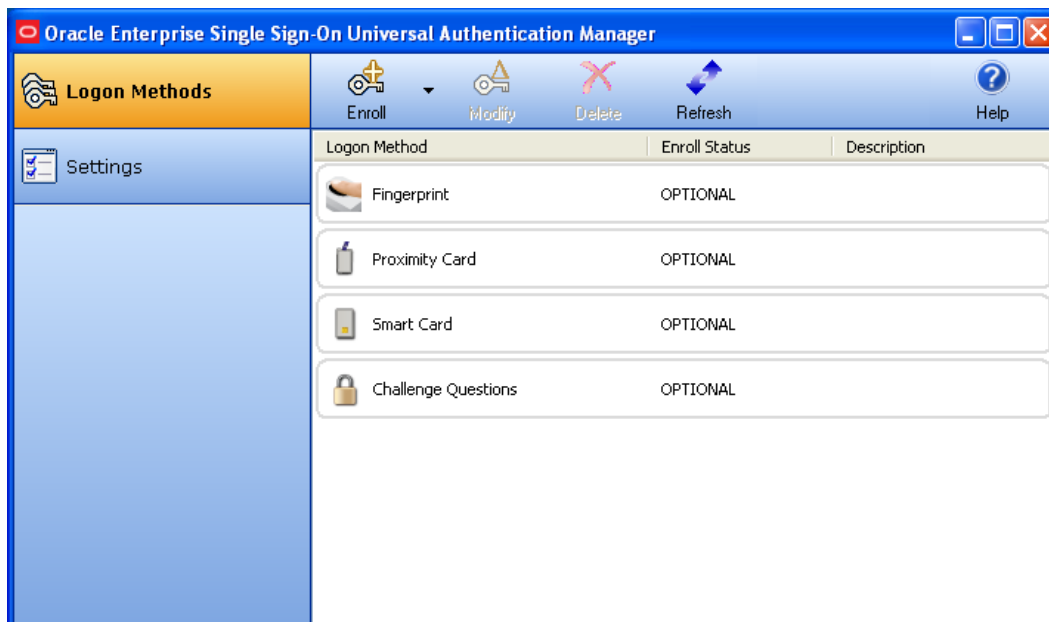
1. Click **Start**, then **Programs**.
2. Point to **Oracle**, then **Universal Authentication Manager**.
3. Click **Universal Authentication Manager**.

Universal Authentication Manager opens.



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





- Manage enrolled credentials.
- Change a Universal Authentication Manager PIN associated with a fingerprint, smart card, or proximity card.
- Refresh your account to synchronize changes made by your administrator.
- Access the help system.



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

- [Fingerprint](#)
- [Proximity Card](#)
- [Smart Card](#)
- [Challenge Questions](#)

The controls on this panel are:

 Enroll	Enroll	Enrolls a new credential. When you click Enroll , a drop-down list of available logon methods appears; from this menu, select the logon method you wish to use.
 Modify	Modify	Modifies the selected enrollment. For some enrollment methods, you can modify properties of your credential. For example, if you are authenticating with a proximity card that has an associated PIN code, click Modify to change your PIN.
 Delete	Delete	Deletes an enrolled credential. If you do not have permission to delete the enrolled credential, you will receive an error message stating so.
 Refresh	Refresh	Synchronizes with the Universal Authentication Manager repository and updates any policy settings that were changed by your administrator (in Enterprise client mode).

Shortcut Keys

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

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

Enrolling Credentials

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

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

- [Enrolling a Fingerprint](#)
- [Enrolling a Smart Card](#)
- [Enrolling a Proximity Card](#)
- [Enrolling Challenge Questions](#)

Ways To Enroll

Enrollment can occur in one of the following ways:

- Prompted
- Prompted with a grace period
- Manual

Prompted Enrollment

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



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

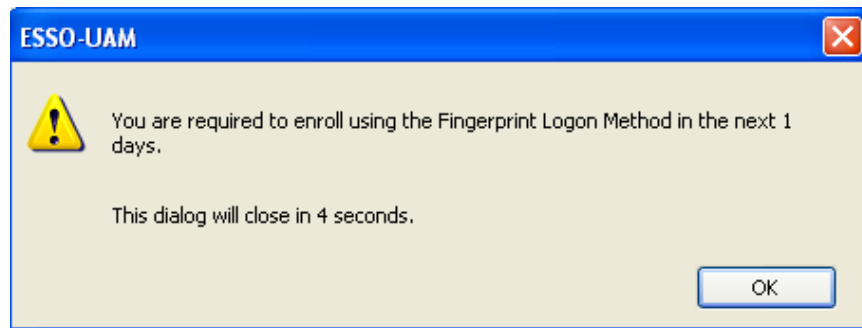
- **Enroll.** Enroll in the logon method now.
- **Not Now.** Exit and ask me to enroll later.
- **Never.** Exit and do not ask me to enroll again.

Grace Period

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



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



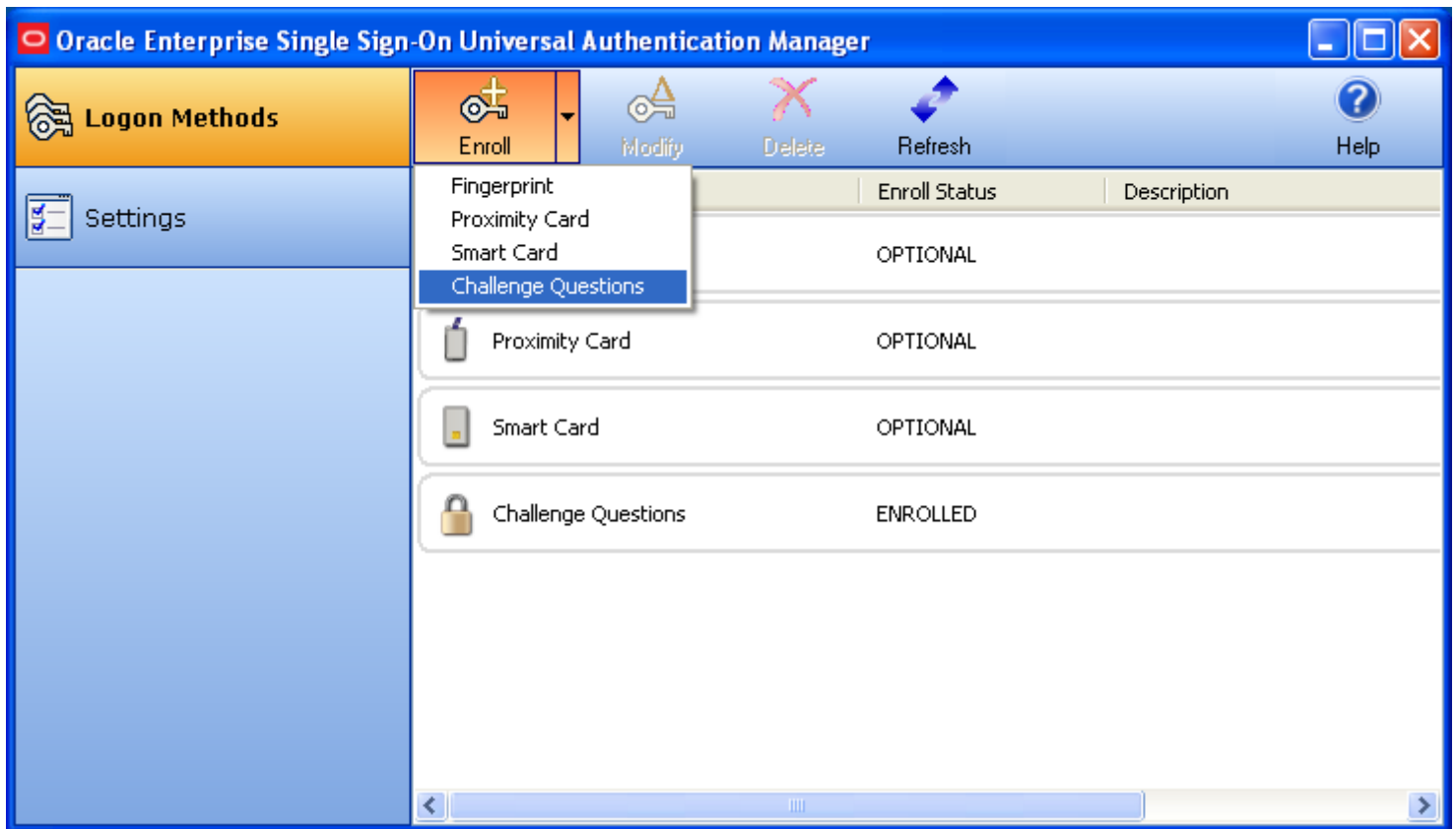
You must enroll this logon method within the configured number of days. Once the Grace Period has ended, you will be required to enroll in this logon method before logging on to Windows.

Manual Enrollment

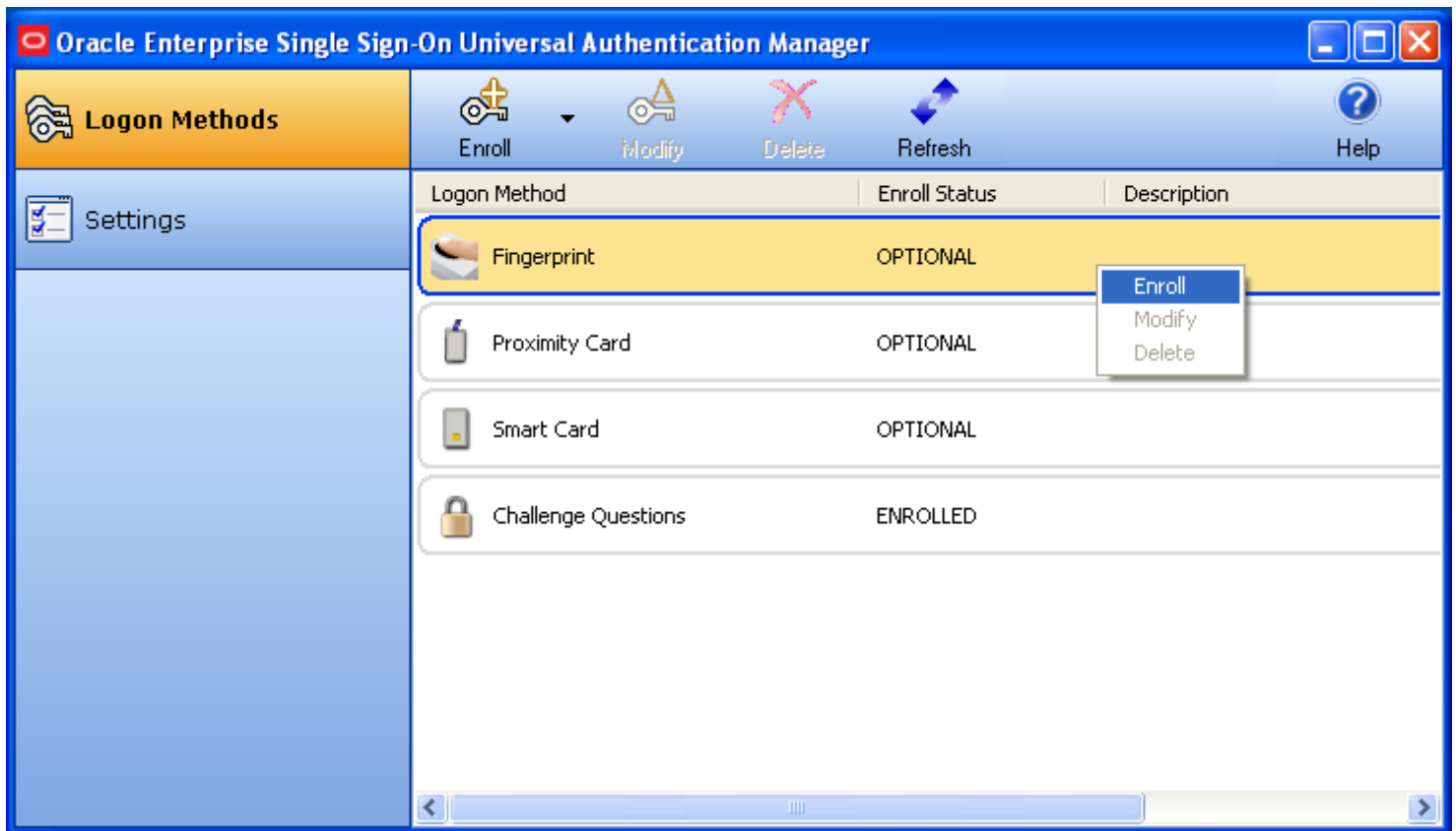
If prompted enrollment is configured to optional or required with a grace period, you will be prompted to enroll when you launch the Universal Authentication Manager.

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

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



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



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

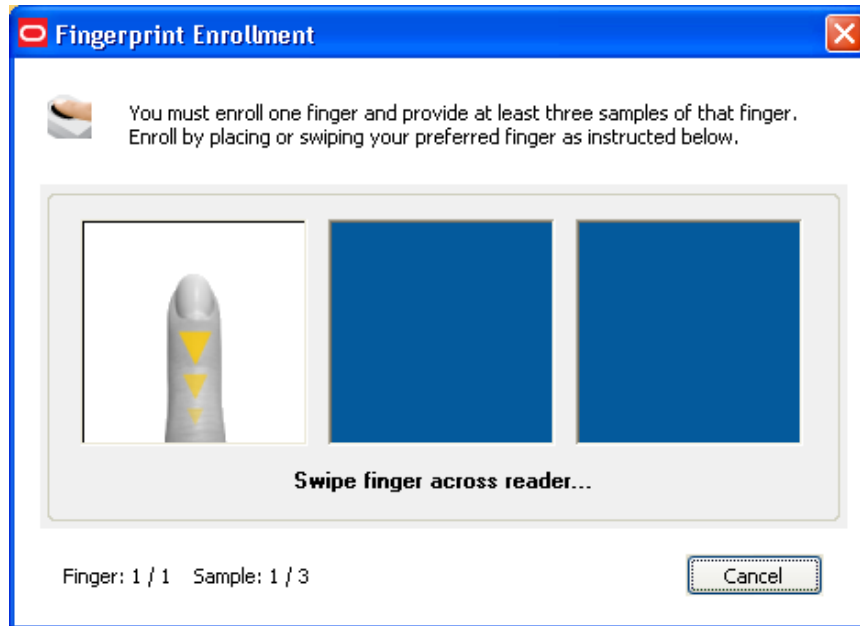
Enrolling a Fingerprint at Windows Logon

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

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



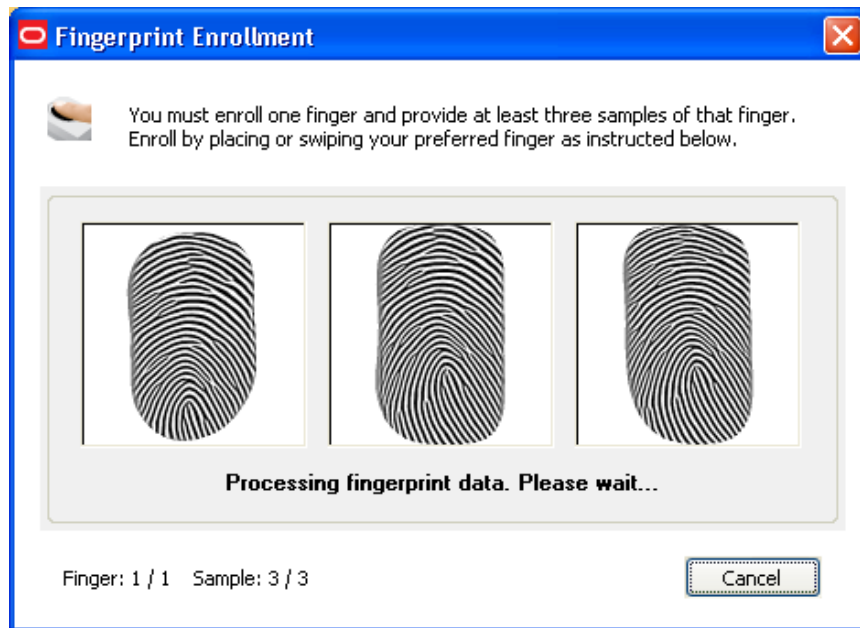
2. If your system is configured to require a PIN with the fingerprint, enter and confirm a PIN.
3. Enroll at least one fingerprint sample. The number of fingerprint samples is configured by your administrator. Enroll by placing or swiping your preferred finger.



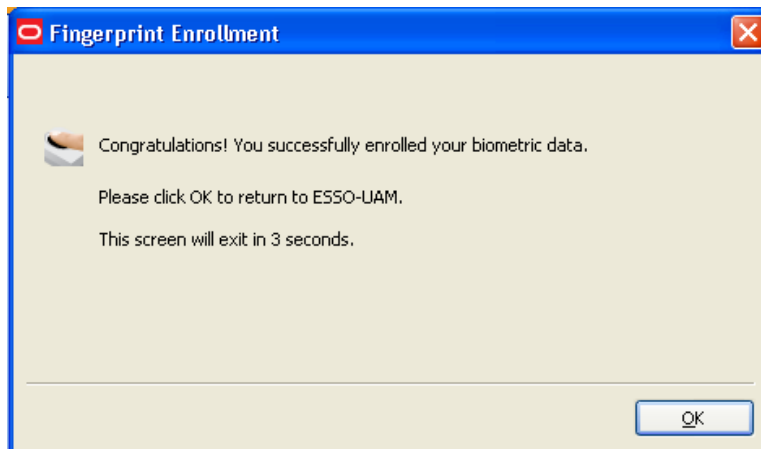
4. Swipe your finger on the reader again and repeat as many times as requested.



5. Once all fingerprint samples have been enrolled, a message informs you that the data is processing. Wait until it completes.



6. When enrollment is complete, a message confirms that your biometric data is enrolled. Click **OK** to exit and resume log on to Windows. If other Universal Authentication Manager logon methods are installed, you may be prompted to enroll in additional methods.



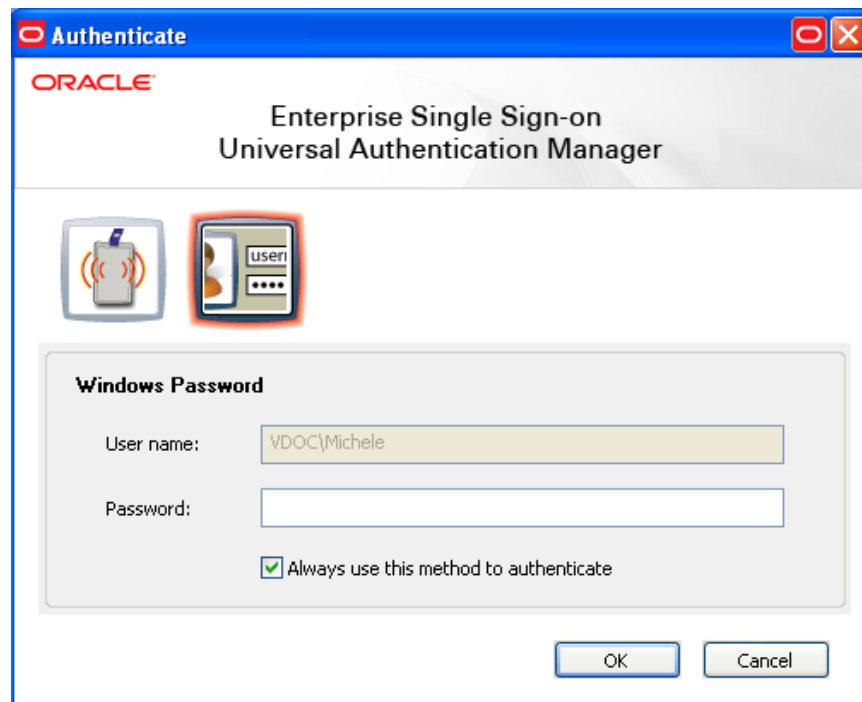
Enrolling a Fingerprint When Launching Universal Authentication Manager

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

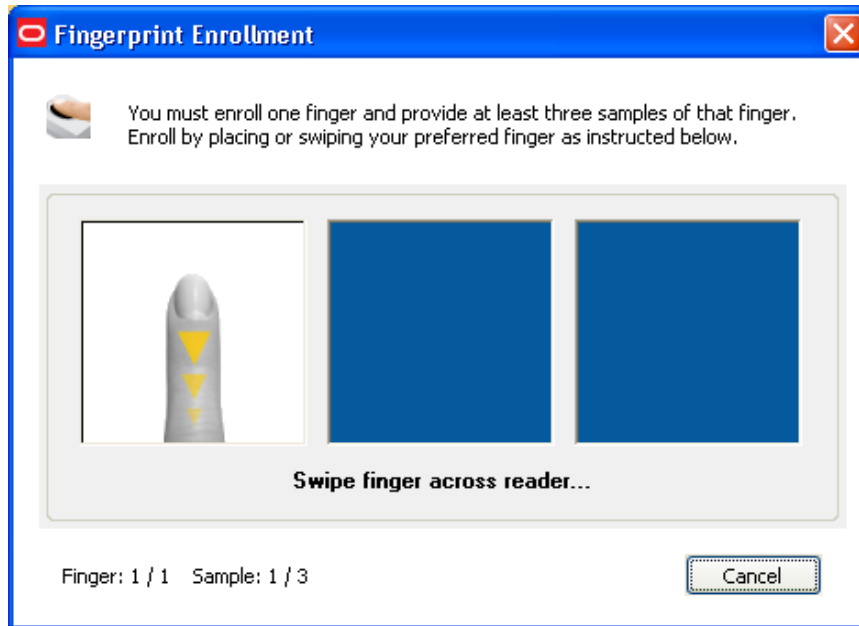
1. Click **Enroll** to enroll a fingerprint.



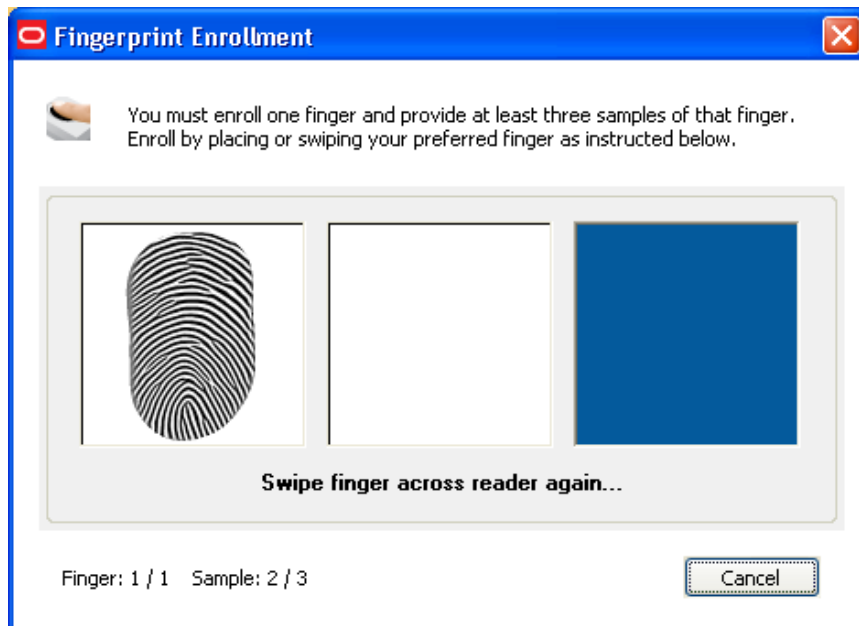
2. Authenticate using a previously enrolled logon method or your Windows password.



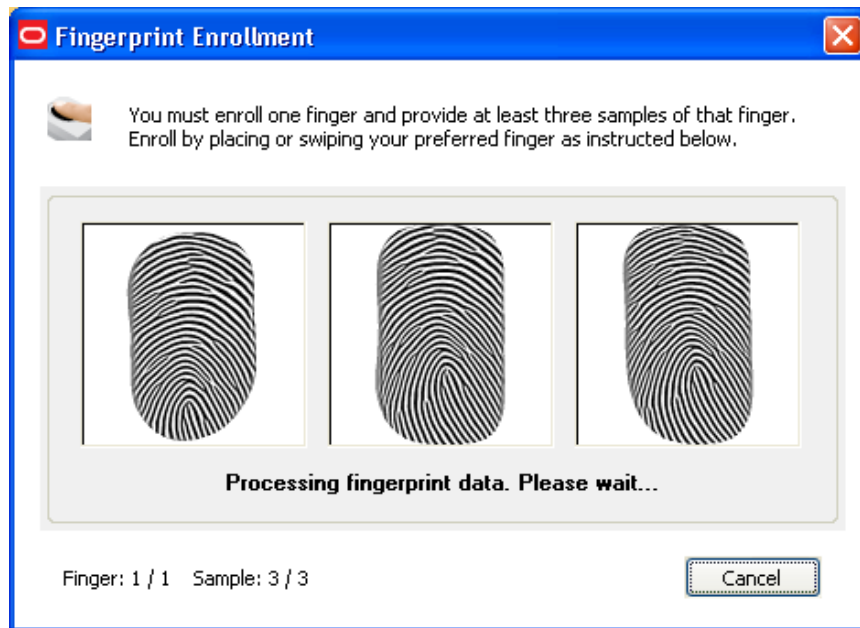
3. If your system is configured to require a PIN with the fingerprint, provide a PIN when prompted.
4. Enroll at least one fingerprint sample. The number of fingerprint samples is configured by your administrator. Enroll by placing or swiping your preferred finger.



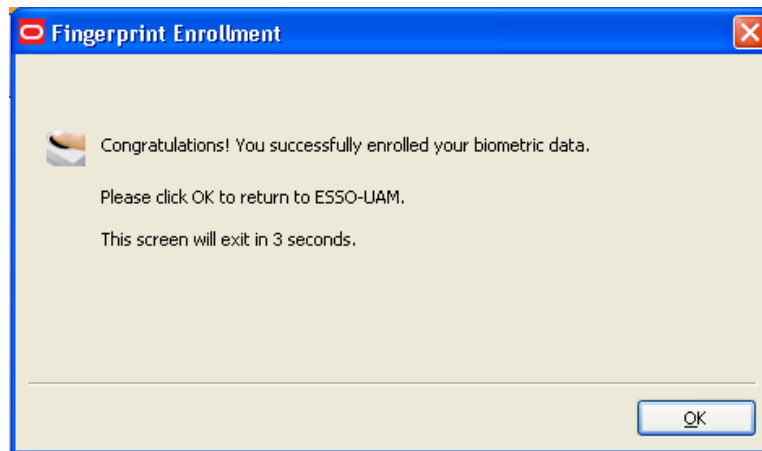
5. Swipe your finger on the reader again and repeat as many times as requested.







6. Once all fingerprint samples have been enrolled, a message informs you that the data is processing. Wait until it completes.



- When enrollment is complete, a message confirms that your biometric data is enrolled. Click **OK** to return to Universal Authentication Manager.



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

Logon Method	Enroll Status	Description
 Fingerprint	ENROLLED	
 Proximity Card	OPTIONAL	
 Smart Card	OPTIONAL	
 Challenge Questions	ENROLLED	

Enrolling a Fingerprint Manually

To enroll a fingerprint manually:

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

Enrolling a Proximity Card at Windows Logon

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

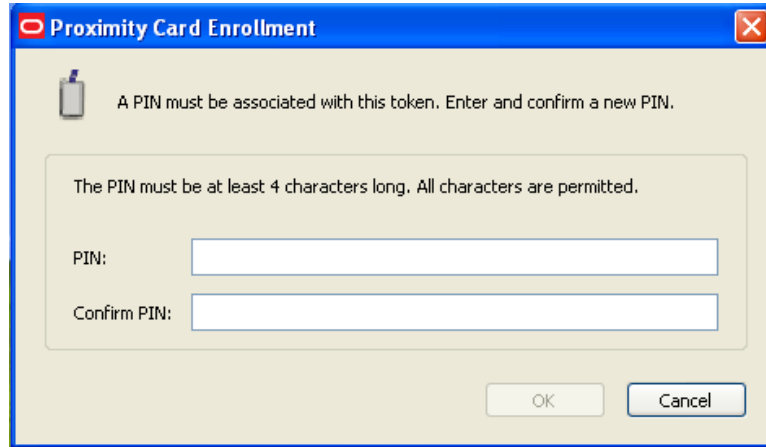
1. Click **Enroll** to enroll a proximity card.



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

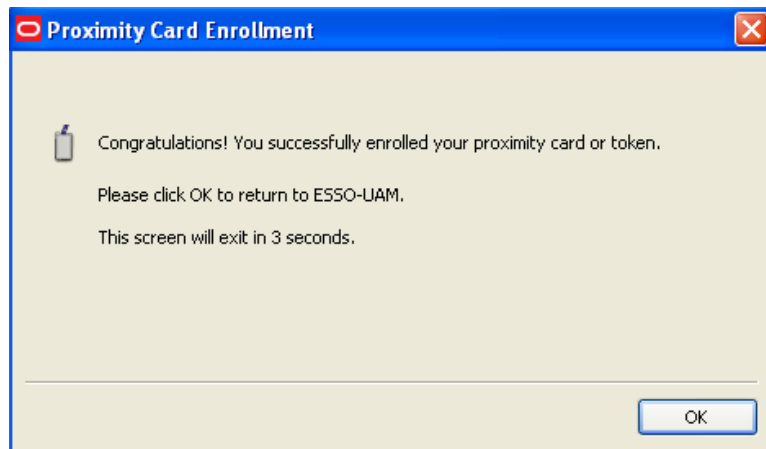


3. If your system is configured to require a PIN with a proximity card, enter and confirm a PIN, then click **OK**.



The screenshot shows a Windows-style dialog box titled "Proximity Card Enrollment". It features a blue title bar with a close button (X) in the top right corner. The main content area has a light beige background. At the top left, there is a small icon of a proximity card. To its right, the text reads: "A PIN must be associated with this token. Enter and confirm a new PIN." Below this, a light gray box contains the instruction: "The PIN must be at least 4 characters long. All characters are permitted." Underneath this box are two text input fields. The first is labeled "PIN:" and the second is labeled "Confirm PIN:". At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

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



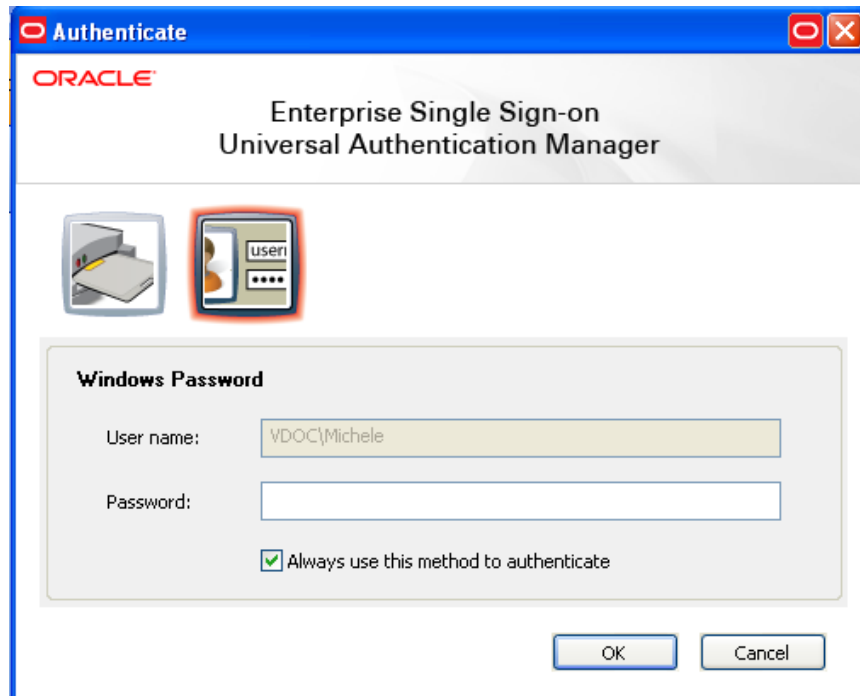
The screenshot shows the same "Proximity Card Enrollment" dialog box, but now it displays a success message. The text reads: "Congratulations! You successfully enrolled your proximity card or token." Below this, it says: "Please click OK to return to ESSO-UAM." and "This screen will exit in 3 seconds." At the bottom right, there is a single "OK" button.

Enrolling a Proximity Card when Launching Universal Authentication Manager

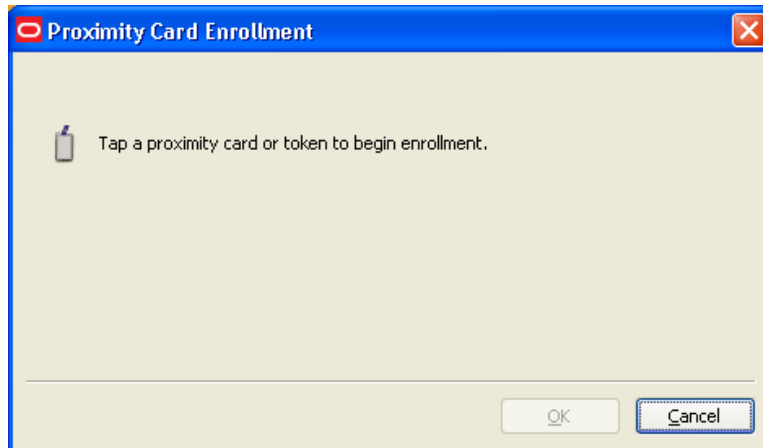
When you launch Universal Authentication Manager, you are automatically prompted to enroll installed logon methods. If one of those methods is a proximity card, you will be prompted to enroll it.



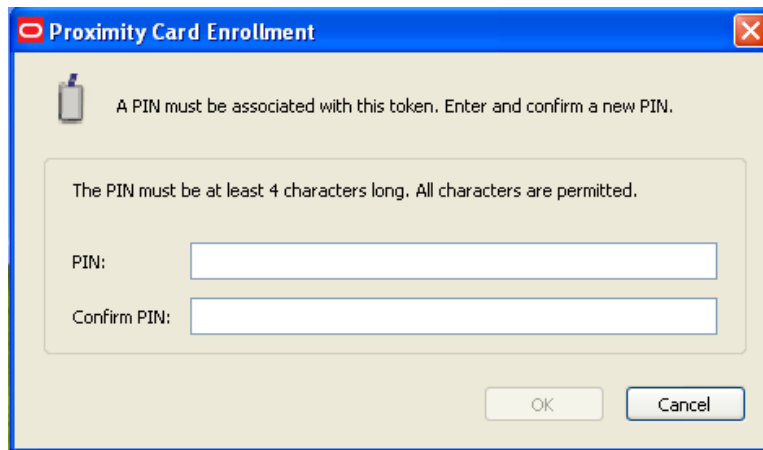
1. Click **Enroll** to enroll a proximity card. You are prompted to authenticate to continue. You can authenticate through any of the available authentication methods.



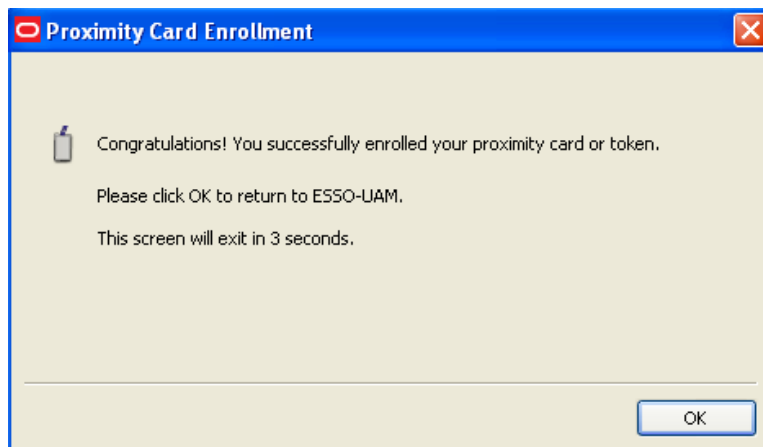
2. Hold your card near the reader until Universal Authentication Manager detects it.







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



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



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

Logon Method	Enroll Status	Description
 Fingerprint	OPTIONAL	
 Proximity Card	ENROLLED	
 Smart Card	OPTIONAL	
 Challenge Questions	ENROLLED	

Enrolling a Proximity Card Manually

To enroll a proximity card manually:

1. Launch Universal Authentication Manager.
2. Click **Enroll** in the Logon Methods toolbar and select **Proximity Card** from the drop-down list; or right-click in the highlighted proximity card row and select **Enroll**; or double click in the proximity card row.
3. Authenticate with a previously enrolled logon method or your Windows password.
4. Hold your card near the reader until Universal Authentication Manager detects it.
5. If your system is configured to require a PIN with a proximity card, enter and confirm a PIN. (see detailed instructions in [previous section](#)).
6. A message confirms that you have successfully enrolled your card. Click **OK** to return to Universal Authentication Manager.
7. The Enroll Status column shows a status of **Enrolled**.



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

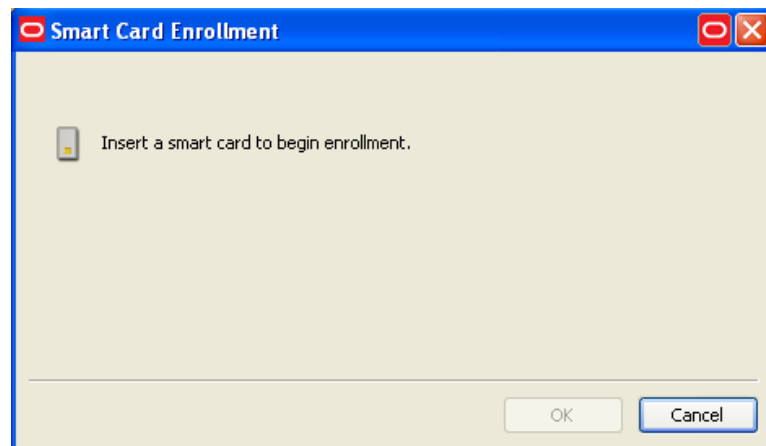
Enrolling a Smart Card at Windows Logon

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

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

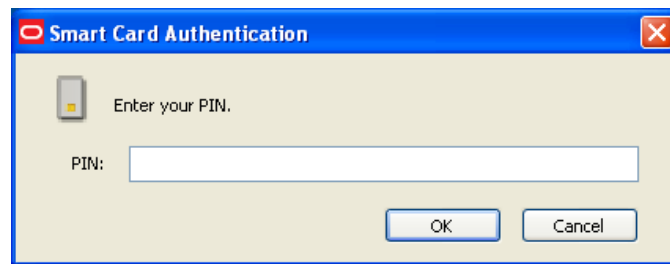


2. Insert your card into the reader.



3. Do one of the following:

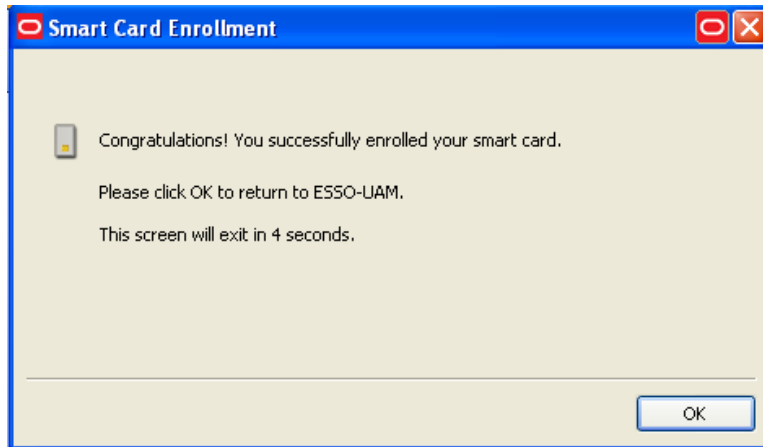
- If the smart card logon method is configured to use the card's own PIN, enter the PIN and click **OK**.



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

For more information, see [Smart Card Settings](#).

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



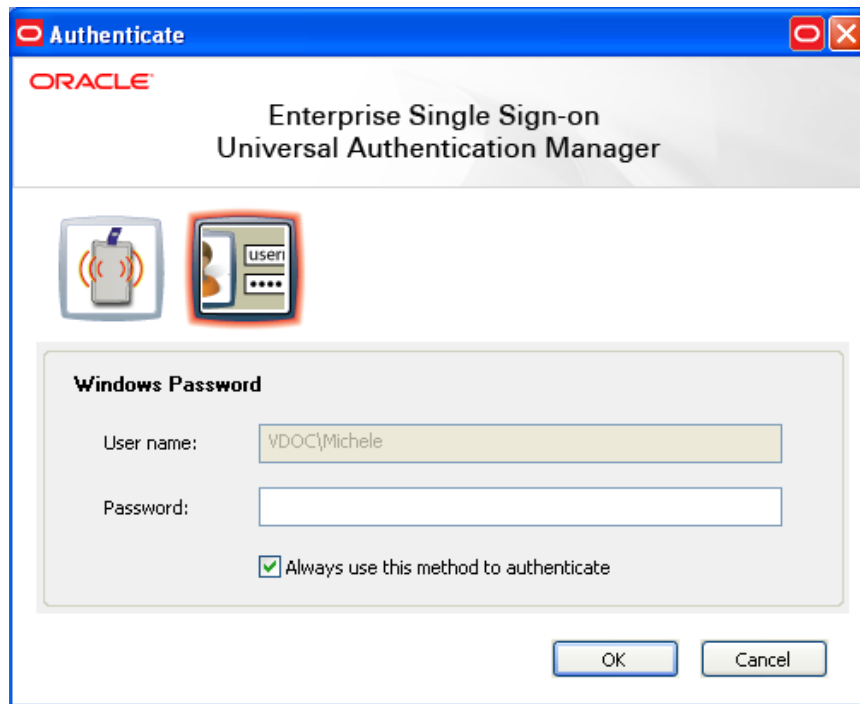
Enrolling a Smart Card when Launching Universal Authentication Manager

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

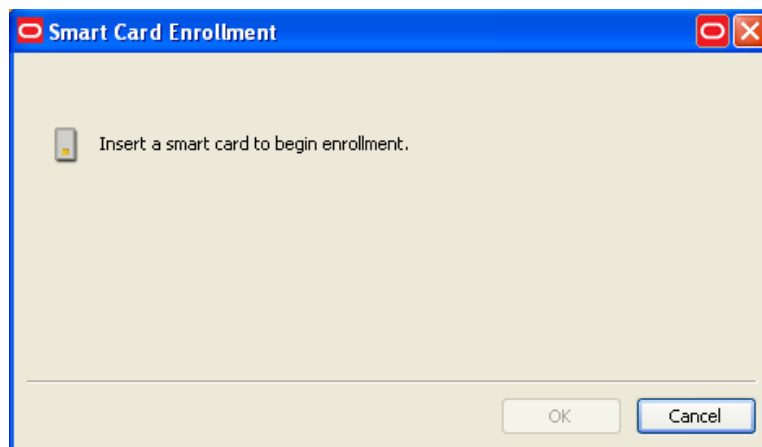
1. Click **Enroll** to enroll a smart card.



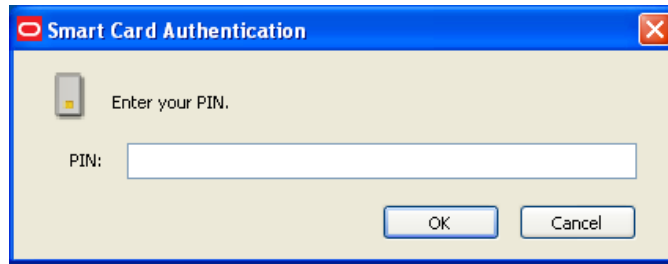
2. Authenticate using a previously enrolled logon method or your Windows password.



3. Insert your card into the reader.



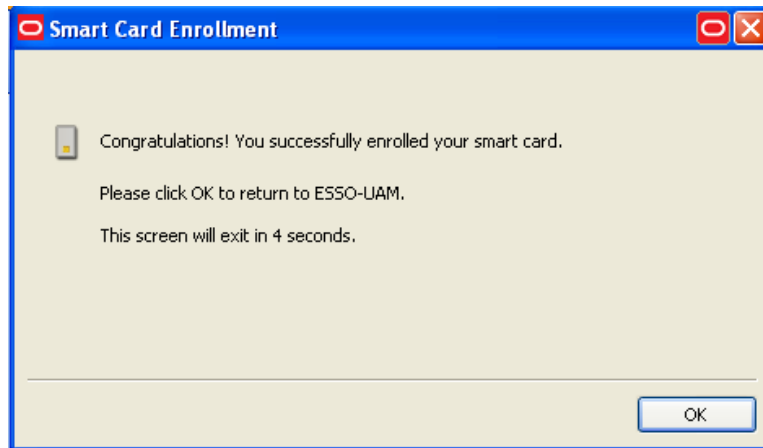
4. Do one of the following:
 - If the smart card logon method is configured to use the card's own PIN, enter the PIN and click **OK**.






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

For more information, see [Smart Card Settings](#).

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



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

Logon Method	Enroll Status	Description
 Fingerprint	OPTIONAL	
 Proximity Card	OPTIONAL	
 Smart Card	ENROLLED	

Enrolling a Smart Card Manually

To enroll a smart card manually:

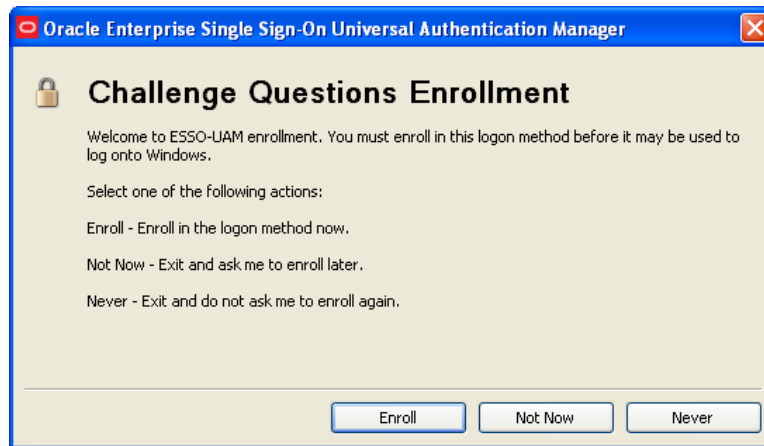
1. Launch Universal Authentication Manager.
2. Insert the card in the card reader.

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

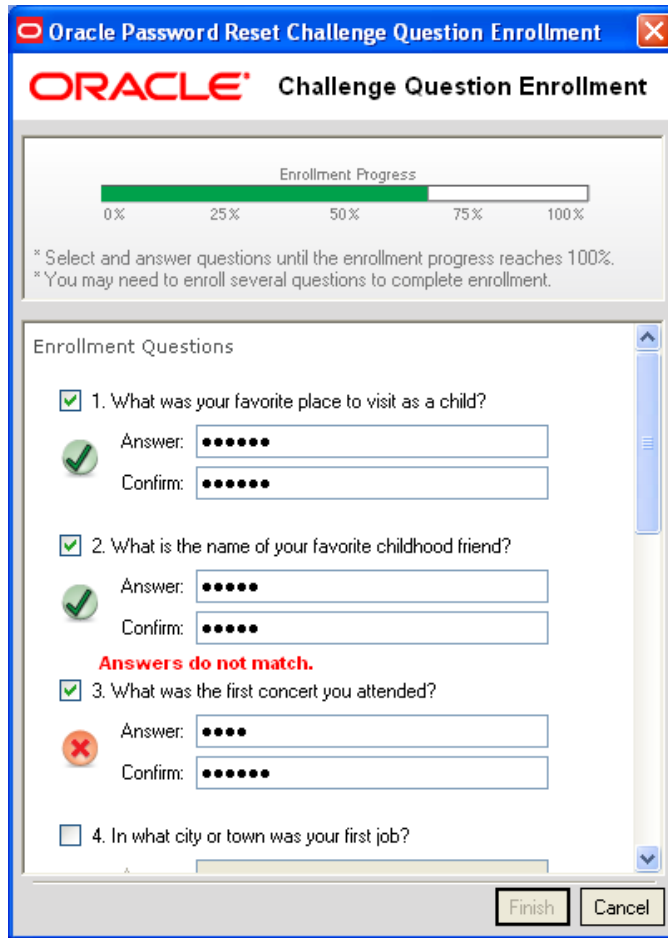
Enrolling Challenge Questions at Windows Logon

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

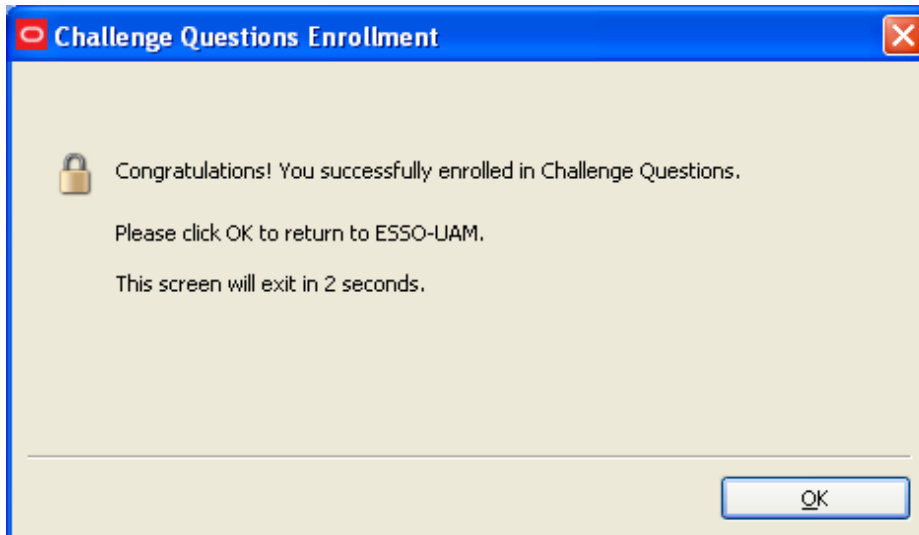
1. Click **Enroll** to begin the enrollment process.



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



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

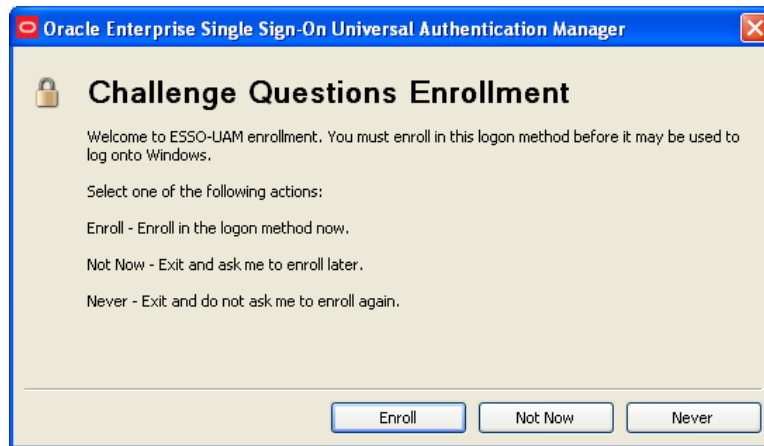


4. If other Universal Authentication Manager logon methods are installed, you may be prompted to enroll in additional methods.

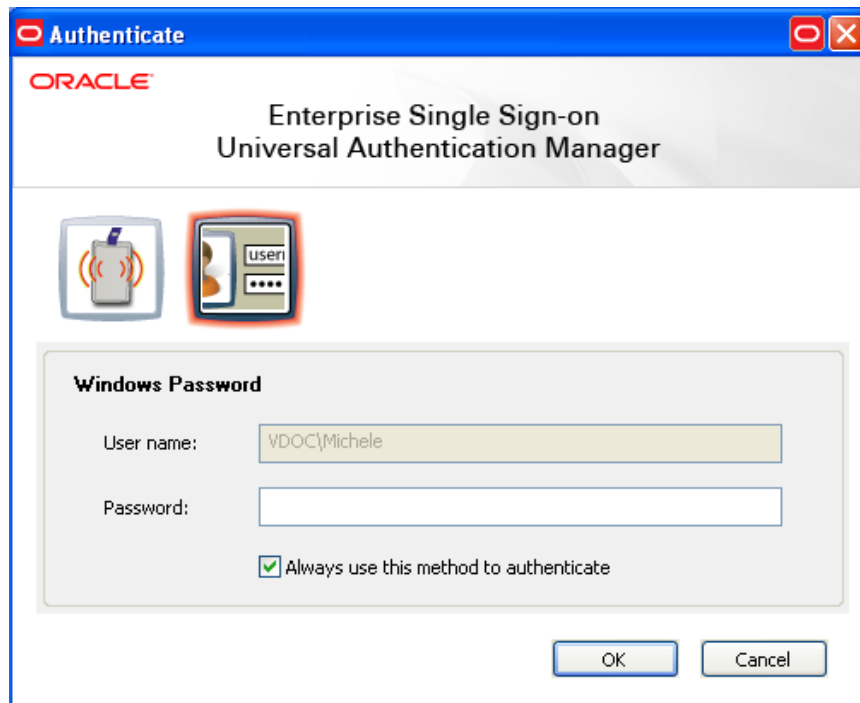
Enrolling Challenge Questions when Launching Universal Authentication Manager

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

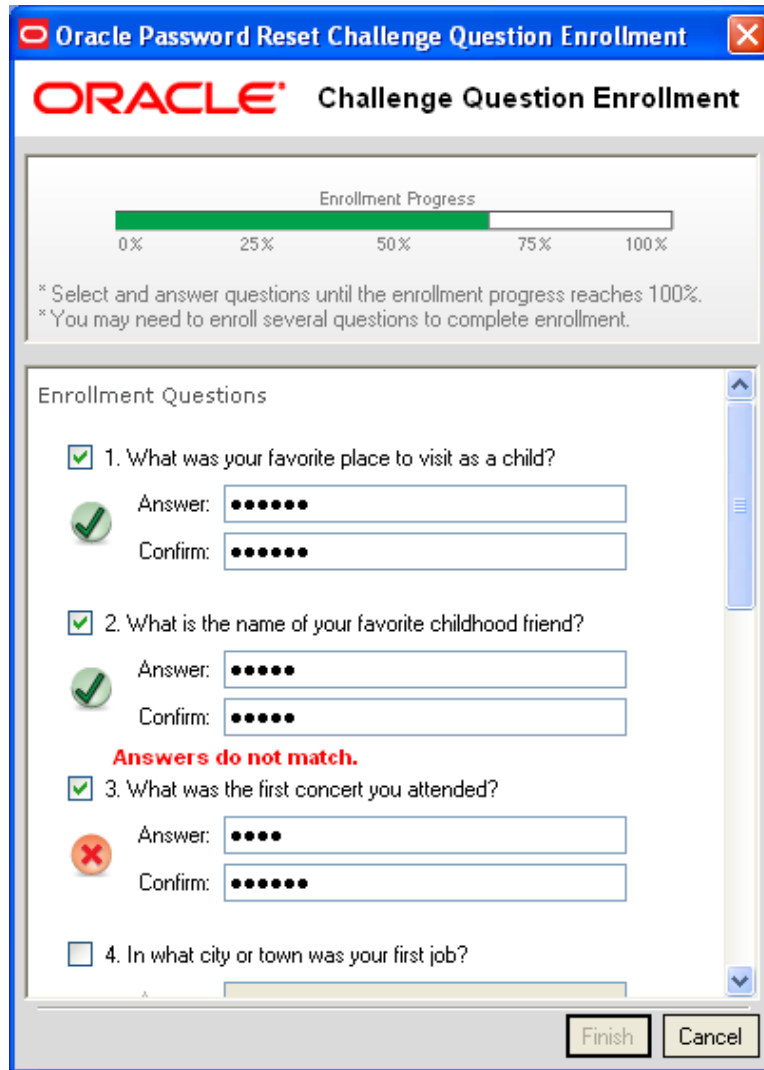
1. Click **Enroll** to begin the enrollment process.



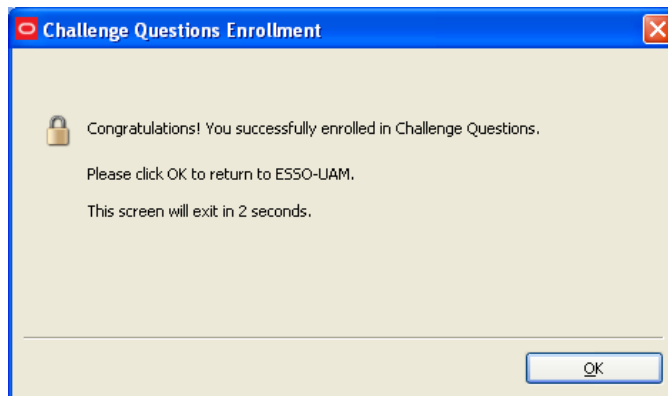
2. When prompted, authenticate to Universal Authentication Manager and click **OK** to proceed. You can authenticate through any of the available authentication methods (in the screen sample below, you can select to authenticate with either a Windows password or proximity card).







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



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



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

Logon Method	Enroll Status	Description
 Fingerprint	OPTIONAL	
 Proximity Card	OPTIONAL	
 Smart Card	OPTIONAL	
 Challenge Questions	ENROLLED	

Enrolling Challenge Questions Manually

To enroll challenge questions manually:

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

Managing Enrolled Credentials

Viewing Properties of Enrolled Credentials

To view properties of enrolled credentials:

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

Viewing Status of Enrolled Credentials

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

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

Viewing and Modifying Enrolled Credentials

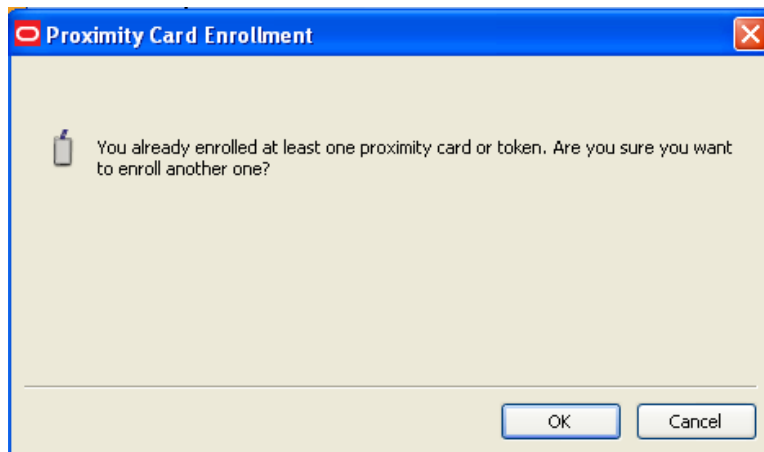
To modify credentials:

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

Enrolling Additional Cards

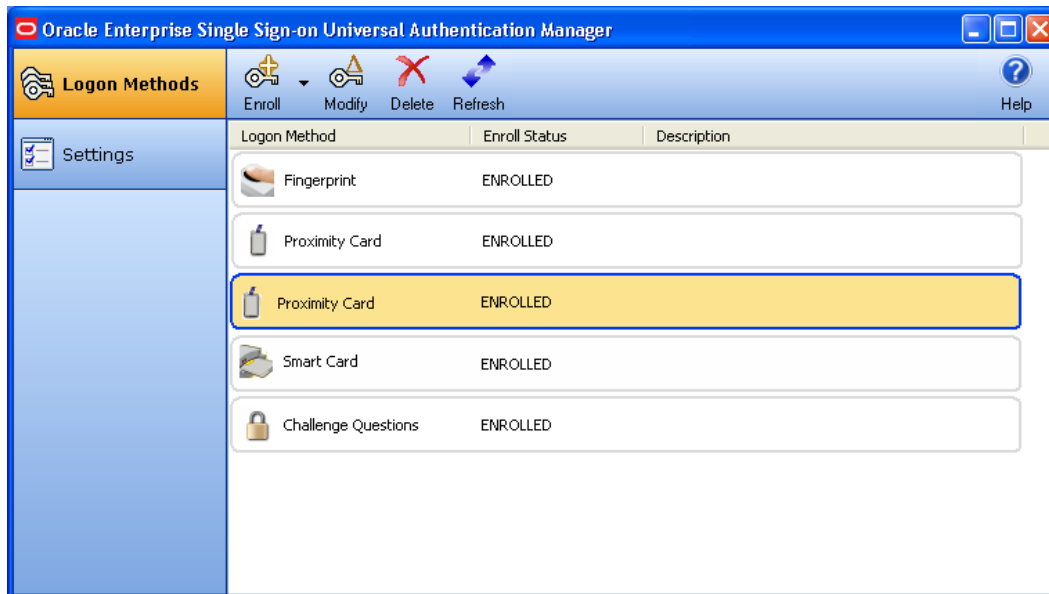
When a smart card or proximity card is detected, Universal Authentication Manager displays a single row of information, including a status of either **OPTIONAL** or **REQUIRED**. When you enroll the first card or token, the enrolled credential will activate the existing row and display a status of **ENROLLED**.

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



Click **OK** to continue with enrollment or click **Cancel** to cancel enrollment. If you click **OK**, follow the on-screen instructions to enroll an additional card. You will be asked to tap or insert your card to begin enrollment and then asked to enter your PIN. When the card has been enrolled, Universal Authentication Manager displays a message confirming successful enrollment.

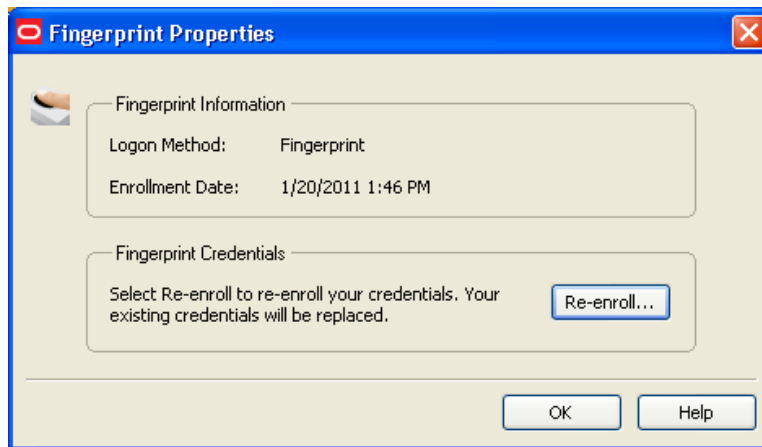
The Enroll Status column now shows two rows of card credentials, each with a status of **Enrolled**.



Re-Enrolling Credentials

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


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




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

Deleting Credentials

To delete credentials:


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

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

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

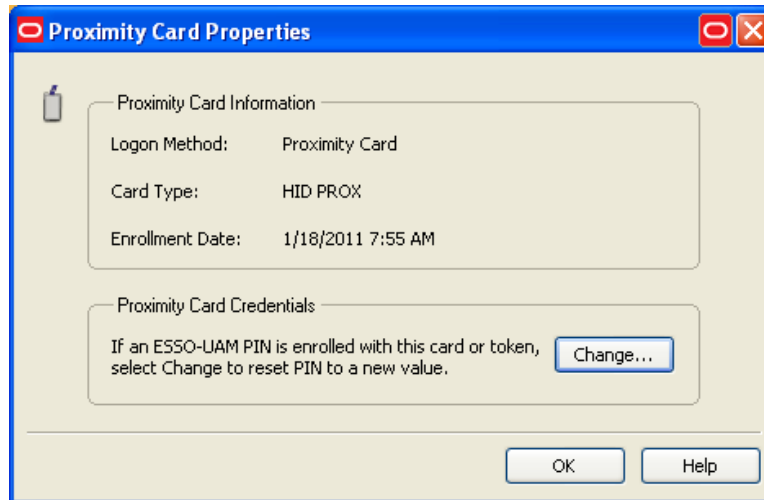
Changing Your Universal Authentication Manager PIN

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

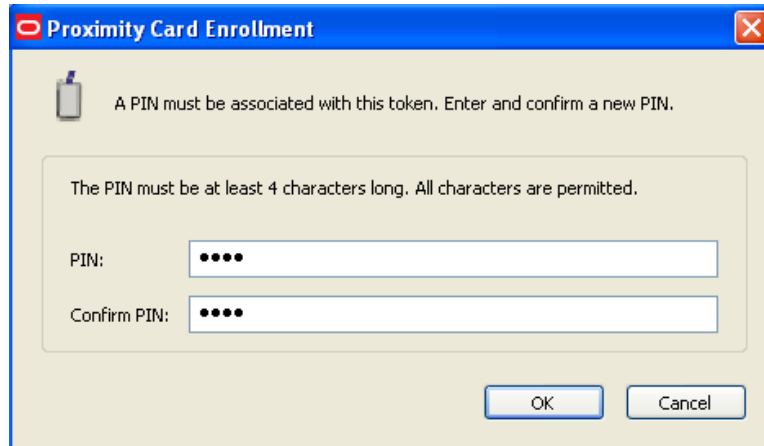
 When using a smart card, the card's own PIN cannot be changed. Only a Universal Authentication Manager PIN associated with the smart card can be changed. For more information, see [Configuring Universal Authentication Manager](#).

To change the Universal Authentication Manager PIN for a fingerprint enrollment, follow the steps in [Re-enrolling Credentials](#).

1. Select the desired logon method.
2. Click **Modify** in the toolbar at the top of the window.
3. In the properties dialog that appears, click **Change....**



4. Insert or tap your card into or on the reader, or authenticate with an enrolled logon method to proceed.
5. Enter the current PIN.
6. When prompted, enter and confirm a new PIN.



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

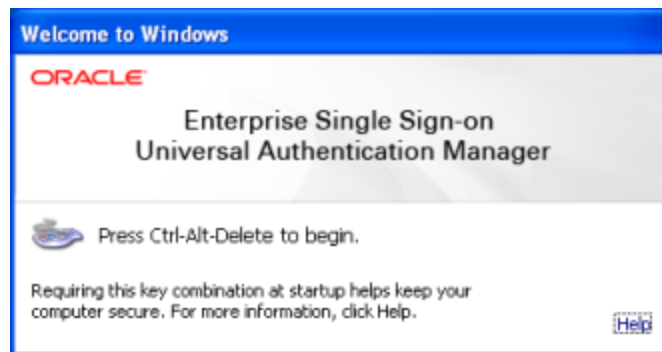
Authenticating

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

- Logging on to Windows with Universal Authentication Manager using:
 - Your Fingerprint
 - Smart Card or Proximity Card
 - Challenge Questions
 - Windows Password
- Re-authenticating to Universal Authentication Manager
- Locking a Workstation

Logging On to Windows with Universal Authentication Manager

When Universal Authentication Manager is installed on your system, the Windows logon dialog is replaced with the Universal Authentication Manager logon dialog.



Press **Ctrl-Alt-Delete** to begin.



The Universal Authentication Manager logon dialog appears. This dialog allows you to log on to your system with any of the installed and enrolled logon methods, or your Windows password.

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



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

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

This logon dialog always defaults to the last used logon method, so if Fingerprint is used to log on, it will be preselected at next logon.

You can select your logon method from the horizontal bar of icons, which from left to right represent: Fingerprint, Proximity Card, Smart Card, Challenge Questions, and Windows Password. The available logon methods will depend upon what your administrator has installed.

Logging On with Your Fingerprint

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

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

1. At the logon screen, select the **Fingerprint** icon.
2. Enter your Windows user name and click **OK**.
3. If you have enrolled a PIN, Universal Authentication Manager prompts you to enter it.
4. Universal Authentication Manager prompts you to present your fingerprint sample (for example, place or slide your finger on your reader).
5. Universal Authentication Manager validates the fingerprint sample and logs you on to Windows.

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

You may have to retry logon or unlock if:

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

Logging On with a Smart Card or Proximity Card

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



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

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

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

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

You may have to retry logon or unlock if:

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

Logging On with Challenge Questions

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

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

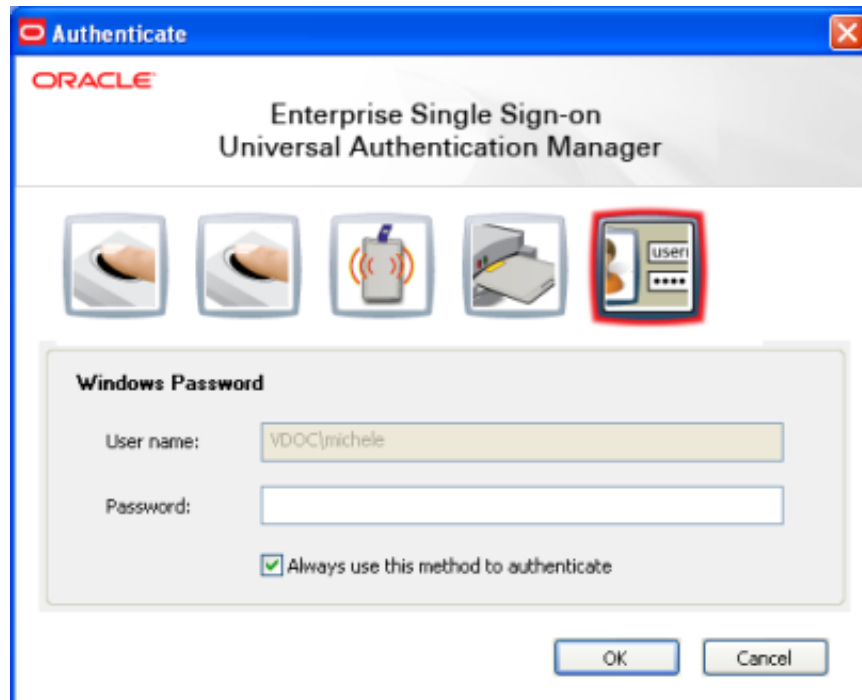
1. At the logon screen, click the **Challenge Questions** icon.
2. Enter your Windows user name and click **OK**.
3. In the dialog that appears, read the challenge question and provide your answer, then click **Next**. If you don't know the answer to the question and have enrolled extra questions to fall back on, click **Skip**. (If you have not enrolled extra questions, skipping a required question will result in a failed logon since you will not be able to satisfy the weight requirement set by the administrator.) When you have correctly answered enough questions to complete the logon, Universal Authentication Manager logs you on to Windows.

Logging On with the Windows Password

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

Re-Authenticating to Universal Authentication Manager

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



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

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

The Re-Authentication dialog box:

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

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

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