Oracle® Enterprise Single Sign-on Universal Authentication Manager

User Guide

Release 11.1.1.5.0

E21031-01

March 2011

Oracle Enterprise Single Sign-on Universal Authentication Manager, User Guide, Release 11.1.1.5.0

E21031-01

Table of Contents

About ESSO-UAM 4

- Using This Guide 4

Getting Started with ESSO-UAM 5

Settings 7

- Fingerprint Settings 7
- BioAPI Settings 7
- Proximity Card Settings 7
- Smart Card Settings 8
- Windows Password 8
- Availability of Settings Depending on Client Mode 9
- Logon Method Enabled Policy 9

Working in Enterprise Mode or Local Mode 11

- Enterprise Client Mode 11
- Local Client Mode 11

Shortcut Keys 12

Authenticating 13

- Log On to Windows with ESSO-UAM 13
- Re-authenticating to ESSO-UAM 15
- Using ESSO-UAM Credentials to Lock a Workstation 16

Enrolling Credentials 17

- Prompted Enrollment 17
- Manual Enrollment 18
- Enrolling Additional Cards and Re-enrolling 20
- Changing an ESSO-UAM PIN 22

Fingerprint Logon Method 23

- Enrolling a Fingerprint at Windows Logon 23
- Enrolling a Fingerprint when Launching the ESSO-UAM Client 25
- Enrolling a Fingerprint Manually 29

BioAPI Logon Method 30

- Enrolling BioAPI at Windows Logon 30
- Enrolling BioAPI when Launching the ESSO-UAM Client 31
- Enrolling BioAPI Manually 33

Proximity Card Logon Method 34

- Enrolling a Proximity Card at Windows Logon 34
- Enrolling a Proximity Card when Launching the ESSO-UAM Client 35
- Enrolling a Proximity Card Manually 38
- Changing an ESSO-UAM PIN 39

Smart Card Logon Method 41

- Enrolling a Smart Card at Windows Logon 41
- Enrolling a Smart Card when Launching the ESSO-UAM Client 42
- Enrolling a Smart Card Manually 45

Integration with ESSO-LM 46

- Configuring ESSO-UAM as the Primary Logon Method with the First-Time Use Wizard 46
- Configuring ESSO-UAM as the Primary Logon Method Using Logon Manager 48
- Authenticating With ESSO-UAM When Prompted by ESSO-LM 49

About ESSO-UAM

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 ESSO-UAM system also enhances enterprise security beyond traditional password authentication by providing two-factor authentication methods. ESSO-UAM enables users to rapidly and securely enroll credentials that will be used to identify and authenticate them.

At its core, ESSO-UAM 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, ESSO-UAM offers four built-in and configurable authentication methods: smart cards, passive proximity cards, biometric fingerprint, and BioAPI compatible biometric. Native Windows Passwords are also supported.

Client Application

The ESSO-UAM Client Application is an intuitive interface that allows you to easily enroll credentials for your logon methods. There are 2 panels from which you can perform all actions for your logon methods:

- Logon Methods
- Settings

Authentication

The ESSO-UAM Log On 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 the Log On to ESSO-UAM section.

Using This Guide

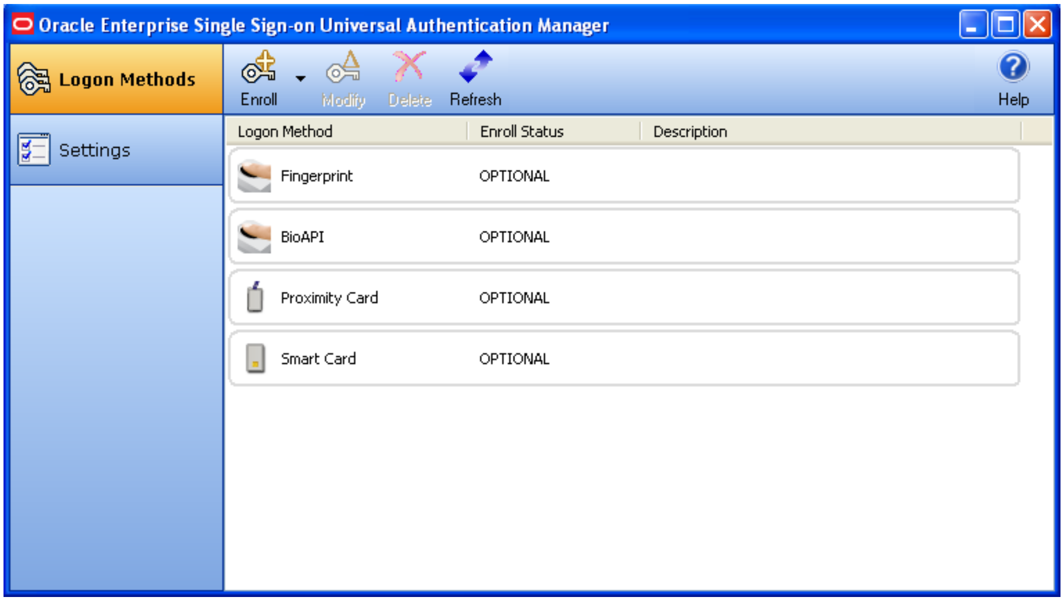
This user guide is intended for anyone using ESSO-UAM to manage enrollments for logon methods. You should be familiar with Windows conventions and with the enrollment procedures for the logon methods you'll use with ESSO-UAM.

Getting Started with ESSO-UAM

To start ESSO-UAM:

1. Click **Start**, then **Programs**.
2. Point to **Oracle**, then **ESSO-UAM**.
3. Click **ESSO-UAM**.

ESSO-UAM opens.


Oracle Enterprise Single Sign-on Universal Authentication Manager
Logon Methods
Settings
Enroll
Modify
Delete
Refresh
Help

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

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:

- View status of enrolled credentials
- Change an ESSO-UAM PIN associated with a proximity card
- View properties of enrolled credentials
- Refresh your account to synchronize changes made by your administrator
- Access the help system

The Logon Methods available with this release are:

- Fingerprint Logon Method
- BioAPI Logon Method
- Proximity Card Logon Method
- Smart Card Logon Method

The controls on this panel are:

Enroll	Enroll	Use this button to enroll a new credential. When you click **Enroll**, a drop-down list appears; from this menu, select the logon method you wish to use.

Modify	Modify	Select a logon method and then click **Modify** to open a screen showing the properties for the credential you have enrolled. 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	Use this button to delete an enrolled credential. If you do not have permission to delete the enrolled credential, you will receive an error message stating so.
Refresh	Refresh	Use this button to synchronize with the ESSO-UAM repository and update any policy settings that were changed by your administrator (in enterprise client mode).

Settings

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 ESSO-UAM is configured by your administrator:

- Fingerprint
- BioAPI
- Proximity Card
- Smart Card
- 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:

Number of fingers	Specifies the number of finger samples you are required to enroll. This policy requires you to enroll exactly the specified number of finger samples during enrollment. Default is 1. Maximum is 10.
Logon Method Enabled	Controls if an installed authenticator is enabled or disabled. This policy setting enhances security by controlling the specific logon methods you are allowed to use. The **Logon Method Enabled** setting is only displayed if you are working in Local Client mode. In Enterprise Client mode, this setting is not displayed.

BioAPI Settings

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

Logon Method Enabled	Controls if an installed authenticator is enabled or disabled. This policy setting enhances security by controlling the specific logon methods you are allowed to use. The **Logon Method Enabled** setting is only displayed if you are working in Local Client mode. In Enterprise Client mode, this setting is not displayed.

Proximity Card Settings

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

PIN Required	Determines whether you must submit a PIN for your card in order to be authenticated. Options are **Yes** (default setting) or **No**.
PIN Minimum Length	The minimum allowed length for the proximity card PIN. Possible values are 4-16 characters (default setting is 4 characters).

PIN Allowed Characters	Determines what characters you can use in your proximity card PIN. Options are **numeric only**, **alphanumeric**, or **any characters**(default setting).
Logon Method Enabled	Controls if an installed authenticator is enabled or disabled. This policy setting enhances security by controlling the specific logon methods you are allowed to use. Options are **Yes** (default setting) or **No**. The **Logon Method Enabled** setting is only displayed if you are working in Local Client mode. In Enterprise Client mode, this setting is not displayed.
Removal Action	Controls how ESSO-UAM behaves when you "tap out" your proximity card (tap your card against the reader a second time during a session). Options are: • No Action • Lock workstation (locks the workstation; you must re-authenticate to return to your session if **PIN Required** is set to **Yes**) (default setting) • Force Logoff (automatically logs you off the workstation)

Smart Card Settings

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

PIN Required	Determines whether you must submit a PIN for your card in order to be authenticated. Options are **Yes** (default setting) or **No**.
Logon Method Enabled	Controls if an installed authenticator is enabled or disabled. This policy setting enhances security by controlling the specific logon methods you are allowed to use. Options are **Yes** (default setting) or **No**. The **Logon Method Enabled** setting is only displayed if you are working in Local Client mode. In Enterprise Client mode, this setting is not displayed.
Removal Action	Controls how ESSO-UAM behaves when you remove your smart card. Options are: • No Action • Lock workstation (locks the workstation; you must re-authenticate to return to your session if **PIN Required** is set to **Yes**) (default setting) • Force Logoff (automatically logs you off the workstation)

Windows Password

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

Logon Method Enabled	Controls if an installed authenticator is enabled or disabled. This policy setting enhances security by controlling the specific logon methods you are allowed to use. The **Logon Method Enabled** setting is only displayed if you are working in Local Client mode. In Enterprise Client mode, this setting is not displayed.

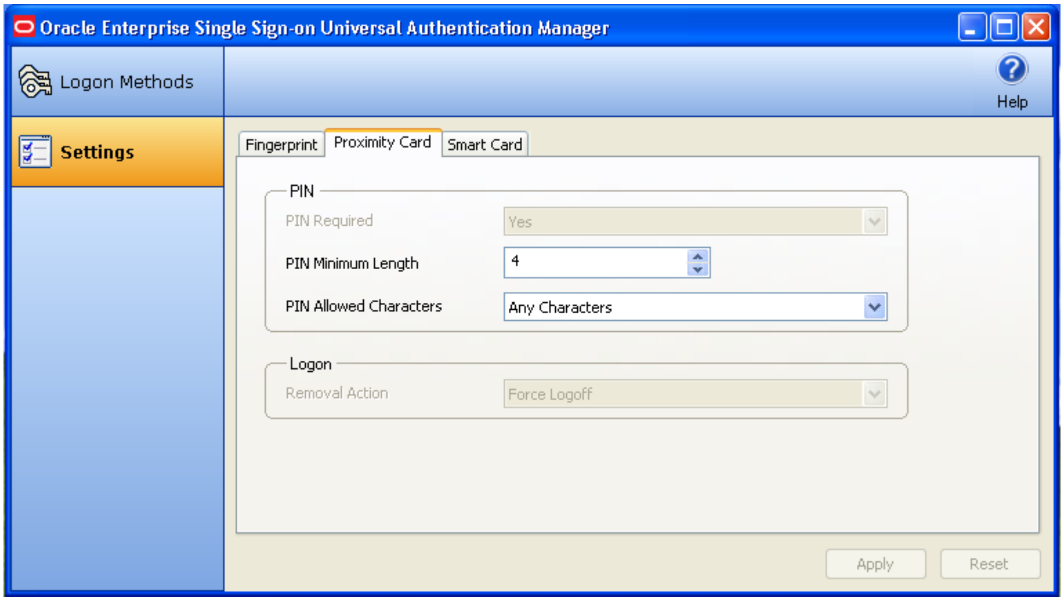
Availability of Settings Depending on Client Mode

If you are working in Enterprise Client 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:

- PIN is required upon enrollment (using the **PIN Required** setting).
- when a smart card is removed, you are automatically logged off the workstation (using the **Force Logoff** setting).

In this scenario, the **PIN Required** and **Force Logoff** settings will be visible to you, but they will be disabled; you will not be able to change them.



Oracle Enterprise Single Sign-on Universal Authentication Manager

PIN

PIN Required: Yes

PIN Minimum Length: 4

PIN Allowed Characters: Any Characters

Logon

Removal Action: Force Logoff

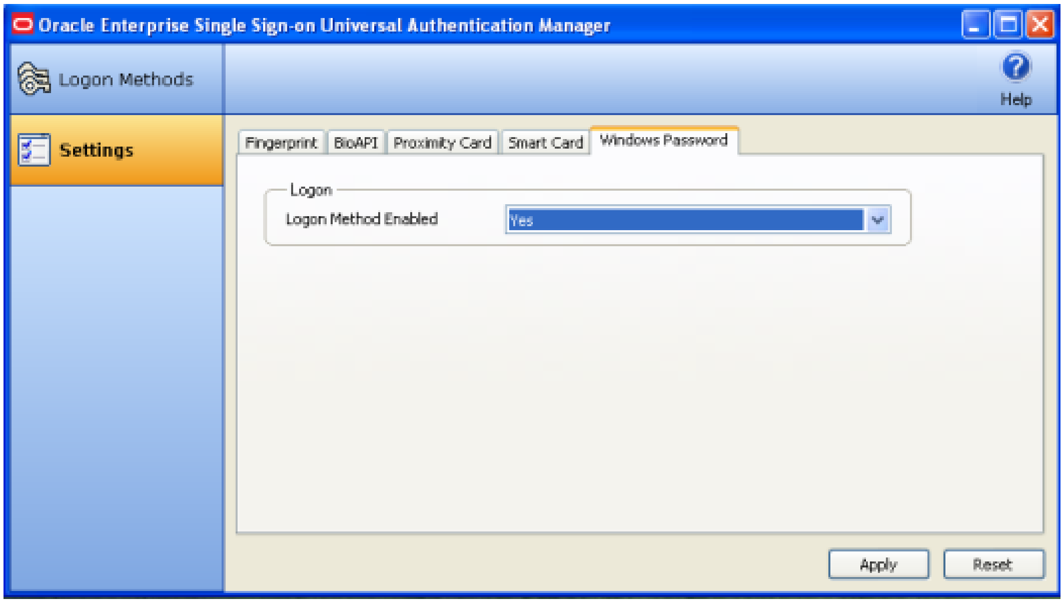
For details on Enterprise Client Mode, see Working in Enterprise Mode or Local Mode.

Logon Method Enabled Policy

The Logon Method Enabled policy allows administrators or users to disable an installed ESSO-UAM authenticator.

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

- In Enterprise Client Mode, the Logon Method Enabled policy setting is an Administrative policy only. This means that the policy will never appear in the ESSO-UAM Client Application settings.
- In 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 ESSO-UAM Client Application:



Logon

Logon Method Enabled: Yes

Windows Password Exception

ESSO-UAM 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 ESSO-UAM 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 ESSO-UAM Client Application 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 Client Mode, the logon method appears in the ESSO-UAM Client Application Settings tab. All policy settings are disabled, and the Logon Method Enabled policy setting is not displayed.
- In Local Client Mode, the logon method appears in the ESSO-UAM Client Application 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.

Working in Enterprise Mode or Local Mode

When you install ESSO-UAM, the InstallShield Wizard asks you to choose the Client Mode you wish to use.

Enterprise Client Mode

If you choose Enterprise Client mode, you will be accessing a network and a database that stores settings for your account. In this mode, you will be able to view settings that you can configure yourself, as well as settings that you cannot change but that are configured by your administrator. Your administrator can also make changes to policy settings that apply to you, but that you cannot configure. To update your account with changes made by your administrator, click **Refresh**.

Local Client Mode

If you choose to work in Local Client Mode, ESSO-UAM will not connect to a network in order to retrieve your settings; instead, ESSO-UAM 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 ESSO-UAM 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.

Shortcut Keys

You can use the following keyboard shortcuts in ESSO-UAM:

- 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)

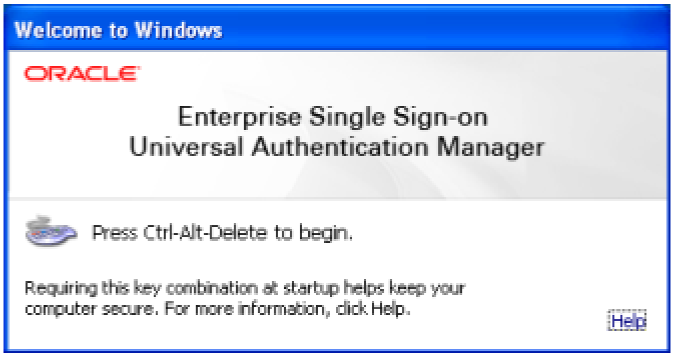
Authenticating

The ESSO-UAM Log On and Re-authentication dialogs allow 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. This section describes all the different ways to authenticate, as well as lock a workstation:

- Log On to Windows with ESSO-UAM
    - Logging on with Biometrics
    - Logging on with Smart Cards and Proximity Cards
    - Logging on with Windows Password
- Re-authenticating to ESSO-UAM
- Using ESSO-UAM Credentials to Lock a Workstation

Log On to Windows with ESSO-UAM

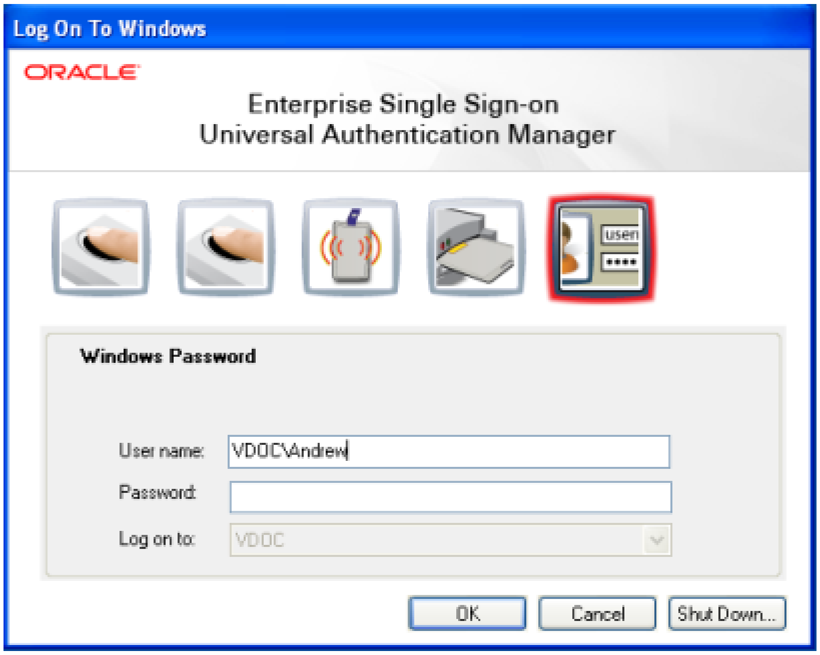
Once you have ESSO-UAM installed on your system, the Windows Log On dialog is replaced with the ESSO-UAM logon dialog.



Press Ctrl-Alt-Delete to begin.

Requiring this key combination at startup helps keep your computer secure. For more information, click Help.

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



User name: VDOC\Andrew

Password:

Log on to: VDOC

The ESSO-UAM Log On dialog appears. This dialog allows you to log onto your system with any of the installed and enrolled logon methods, or your Windows password.

Upon initial log on to ESSO-UAM, use your Windows Password (if this is an option). You can then launch the ESSO-UAM 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 revert to using your Windows password for logon (if enabled).

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

This Log On dialog box always defaults to the last used logon method, so if Fingerprint is used to logon, it will be pre-selected at next logon.

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

Logging on with Biometrics

The biometric logon methods, Fingerprint and BioAPI, must be manually selected from the log on dialog.

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

1. At the logon screen, select one of the biometric icons.
2. ESSO-UAM prompts you to present your biometric sample (for example, place your fingerprint on the reader).
3. ESSO-UAM validates the biometric sample and logs you onto 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:

- The biometric sample you try to use for logon is not enrolled as a ESSO-UAM 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 Smart Card and Proximity Cards

Unlike Fingerprint and BioAPI Logon Methods, Smart Card and Proximity Card logons are event-driven by token insertion and removal.

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

1. At the logon screen, insert or tap an enrolled card on the card reader. ESSO-UAM 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 of proximity card icon, ESSO-UAM prompts you to tap or insert your card.
3. If a PIN is required with your card, enter your PIN when prompted. ESSO-UAM validates the PIN and logs you onto 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:

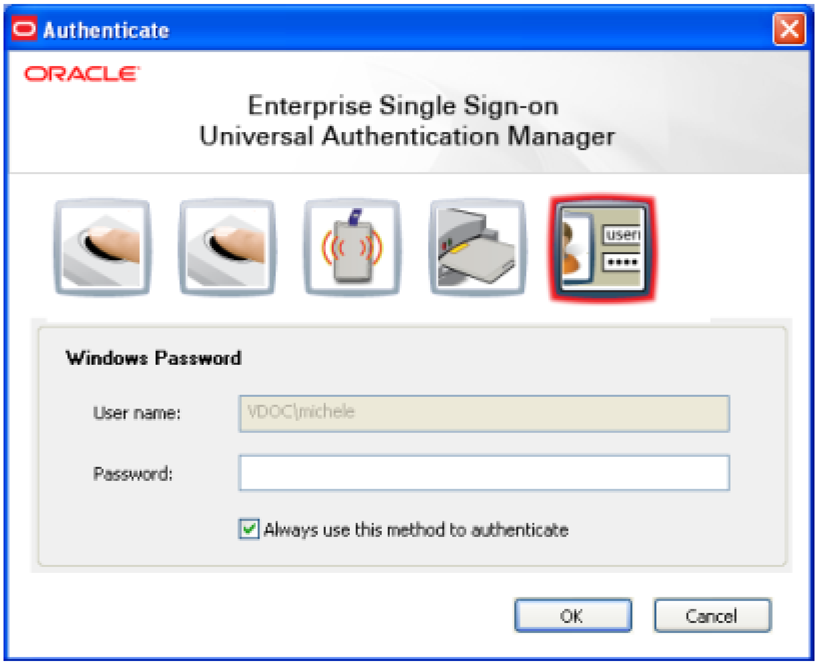
- A PIN is required and you enter an invalid PIN. In this case, try entering your PIN again, or click **Cancel** to return to the logon screen.
- The card you try to use for logon is not enrolled as a ESSO-UAM logon method. If the card is not detected, nothing will occur. If the card is detected but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

Logging on with 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 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 ESSO-UAM

The ESSO-UAM 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, BioAPI, Proximity Card, Smart Card and Windows Password.



Windows Password

User name: VDOC\michele

Password:

☑ Always use this method to authenticate

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.

Using ESSO-UAM Credentials to Lock a Workstation

Using credentials to lock a work station can only be done using proximity cards and smart cards. This feature does not work with fingerprint and BioAPI logon methods.

From the Settings page, you can configure ESSO-UAM 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 ESSO-UAM, 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 ESSO-UAM Client Application or the re-authentication dialog is open.

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

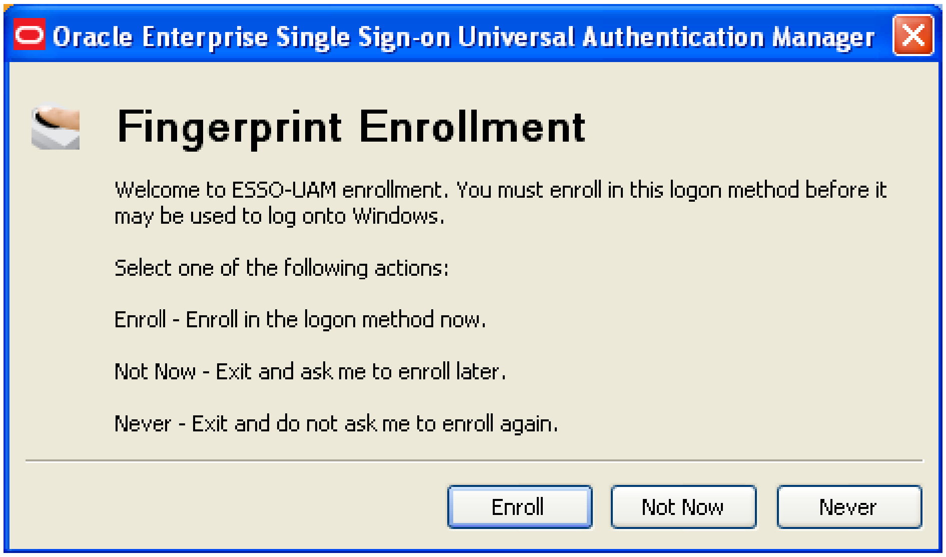
Enrolling Credentials

Credentials can be enrolled manually, or you may be prompted to enroll credentials during Windows logon, or upon launching the ESSO-UAM Client Application. Your administrator may also set a grace period for enrollment. This section describes all the different ways to enroll:

- Prompted
- Prompted with Grace Period
- Manual

Prompted Enrollment

After ESSO-UAM 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. For example:



Oracle Enterprise Single Sign-on Universal Authentication Manager

Fingerprint Enrollment

Welcome to ESSO-UAM enrollment. You must enroll in this logon method before it may be used to log onto Windows.

Select one of the following actions:

Enroll - Enroll in the logon method now.

Not Now - Exit and ask me to enroll later.

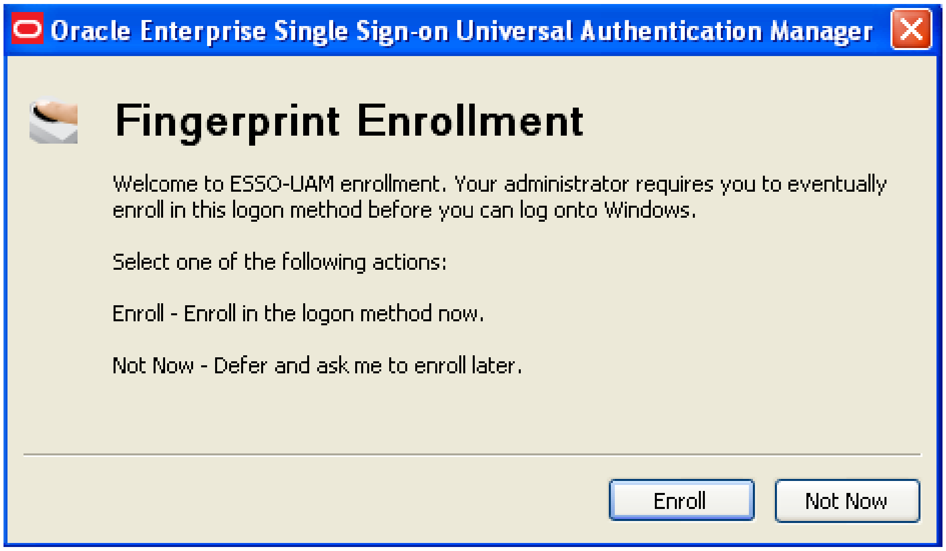
Never - Exit and do not ask me to enroll again.

If multiple logon methods are installed, you will be consecutively prompted to enroll each logon method. When prompted to enroll in each logon method, you may choose from the following options (depending upon how your system is configured for each logon method):

- **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 in this logon method before you can log onto Windows:



Oracle Enterprise Single Sign-on Universal Authentication Manager

Fingerprint Enrollment

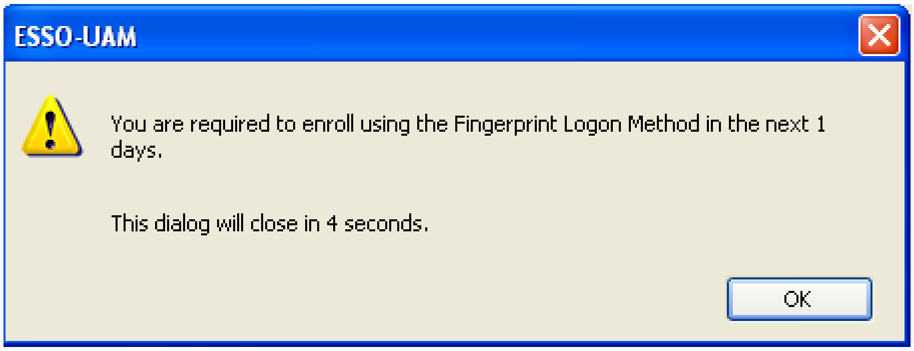
Welcome to ESSO-UAM enrollment. Your administrator requires you to eventually enroll in this logon method before you can log onto Windows.

Select one of the following actions:

Enroll - Enroll in the logon method now.

Not Now - Defer and ask me to enroll later.

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



ESSO-UAM

You are required to enroll using the Fingerprint Logon Method in the next 1 days.

This dialog will close in 4 seconds.

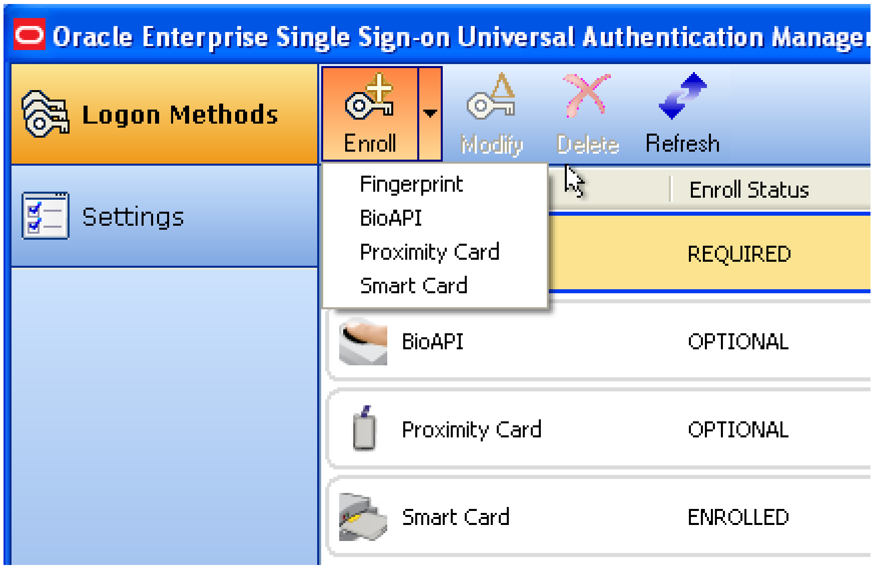
You must enroll in this logon method within the configured number of days. Once the Grace Period has ended, you will be required to enroll in this logon method before logging onto Windows.

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 ESSO-UAM Client Application.

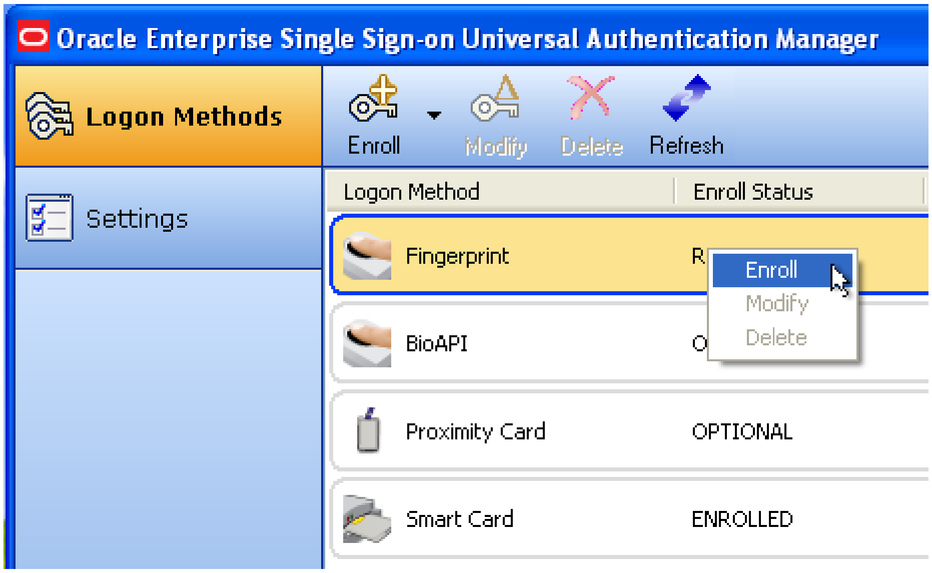
If you choose not to enroll in a logon method when you log on to Windows, you can launch ESSO-UAM and manually enroll in a logon method using one of the following enrollment procedures:

- 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. If the card requires a PIN, you will be prompted to enter your 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.)

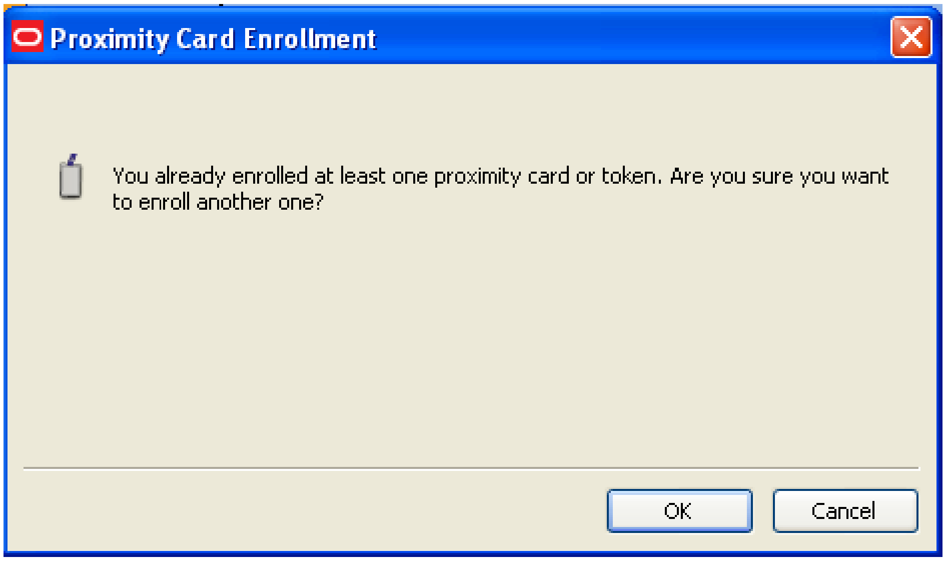
Enrolling Additional Cards and Re-enrolling

When you use cards and tokens, you can enroll multiple credentials. When you use biometrics, you can re-enroll your credentials and replace your existing ones.

Enrolling Additional Cards

When a smart card, proximity card, or token method is detected, it will display 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.

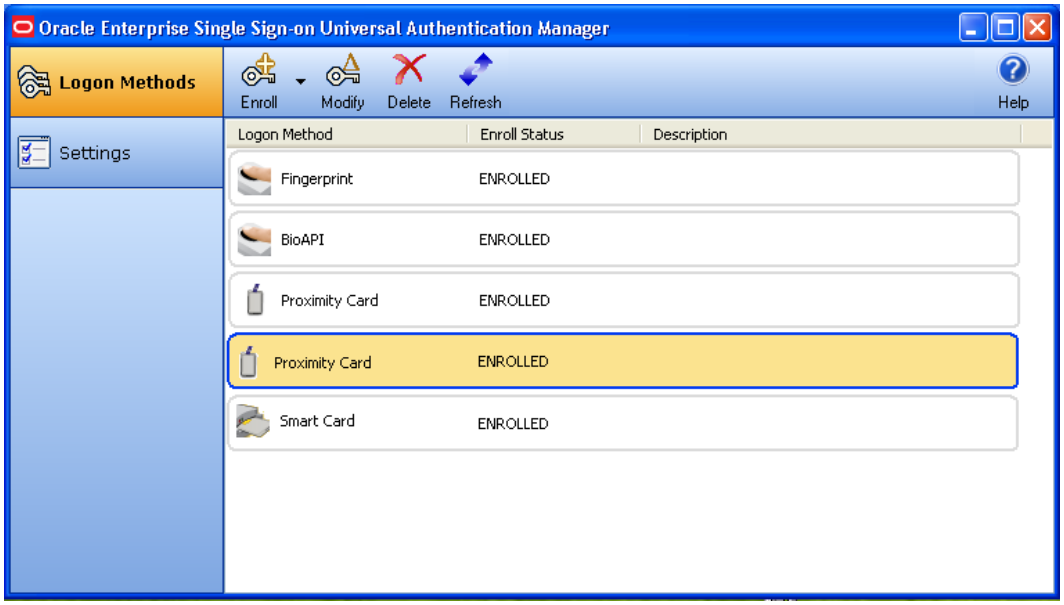
If you have enrolled at least one card or token, and want to enroll and additional one, click the **Enroll** button and choose either Proximity Card or Smart Card from the drop-down list that appears. ESSO-UAM displays a message stating that you have already enrolled one card and asks you to confirm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



You already enrolled at least one proximity card or token. Are you sure 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 complete, ESSO-UAM displays a message confirming that you have successfully enrolled the second card.

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

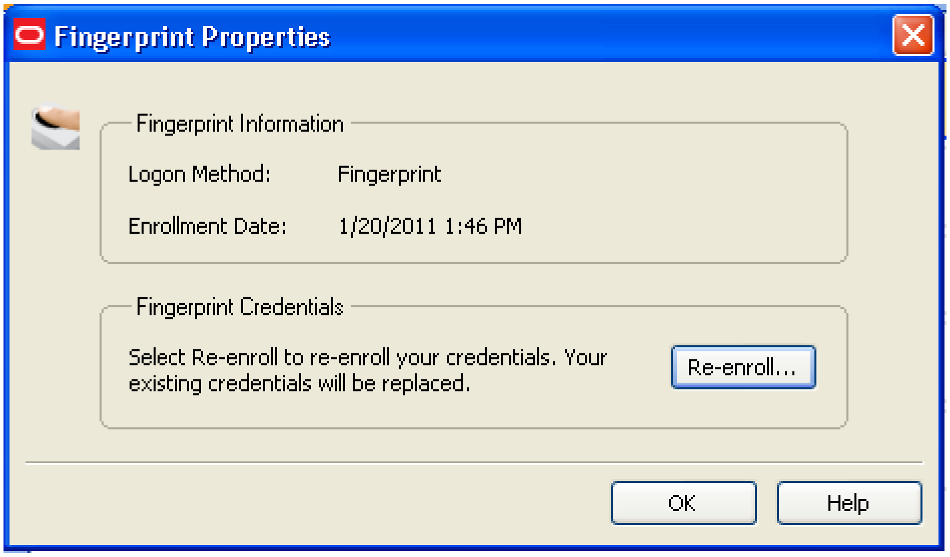

Oracle Enterprise Single Sign-on Universal Authentication Manager
Logon Methods
Settings
Enroll
Modify
Delete
Refresh
Help

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

Re-enrolling Credentials

When a fingerprint or BioAPI logon method is enrolled, it will display 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 can not 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**.



Fingerprint Information

Logon Method: Fingerprint

Enrollment Date: 1/20/2011 1:46 PM

Fingerprint Credentials

Select Re-enroll to re-enroll your credentials. Your existing credentials will be replaced.

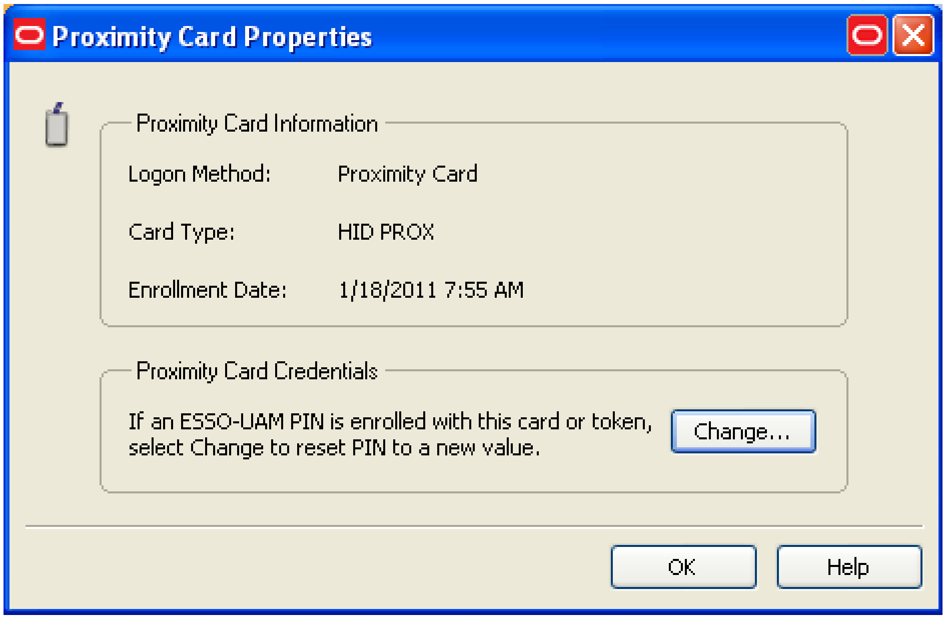
Select **Re-enroll** to re-enroll your credentials.

ESSO-UAM displays a message stating that you have already enrolled in this logon method and informs you that re-enrolling will replace your existing enrollment. Click **OK** to continue with enrollment or click **Cancel** to cancel enrollment. If you click **OK**, follow the on-screen instructions to re-enroll. When complete, ESSO-UAM displays a message confirming that you have successfully enrolled your credentials.

Changing an ESSO-UAM PIN

If your ESSO-UAM proximity card is enrolled with an associated PIN and you wish to change the PIN:

1. Select the row for the proximity card.
2. Click **Modify** in the toolbar at the top of the screen or right-click in the row and select **Modify** from the drop-down menu. The dialog box that opens displays the properties of the proximity card as well as a **Change…** button. Click **Change…** to change the PIN for the card.



Proximity Card Properties

Proximity Card Information

Logon Method: Proximity Card

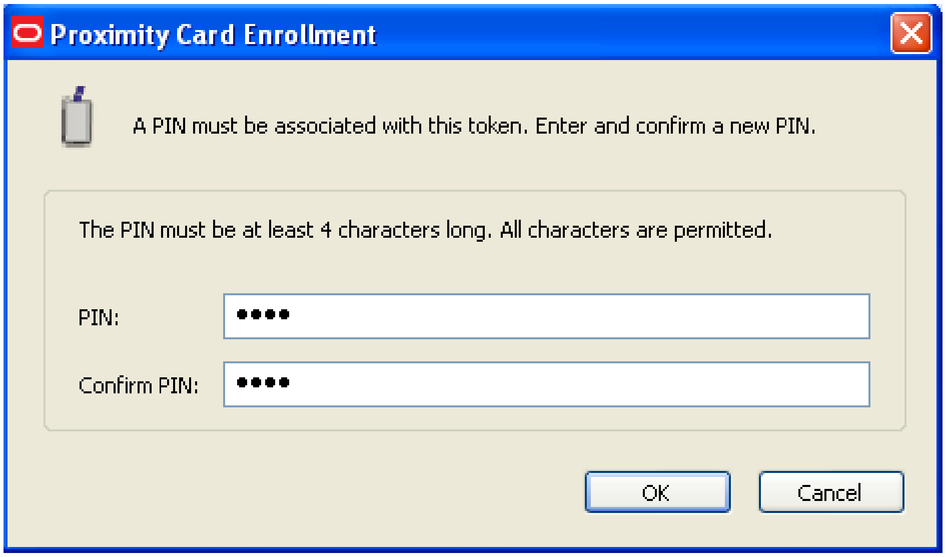
Card Type: HID PROX

Enrollment Date: 1/18/2011 7:55 AM

Proximity Card Credentials

If an ESSO-UAM PIN is enrolled with this card or token, select Change to reset PIN to a new value.

3. Tap your card on the reader or authenticate with an enrolled logon method to proceed.
4. Provide the current PIN for the card.
5. When prompted, enter and confirm a new PIN.



Proximity Card Enrollment

A PIN must be associated with this token. Enter and confirm a new PIN.

The PIN must be at least 4 characters long. All characters are permitted.

PIN: ••••

Confirm PIN: ••••

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

Fingerprint Logon Method

ESSO-UAM enables you to enroll and use third party USB biometric fingerprint readers and readers embedded in laptops as an authentication mechanism to ESSO-UAM.

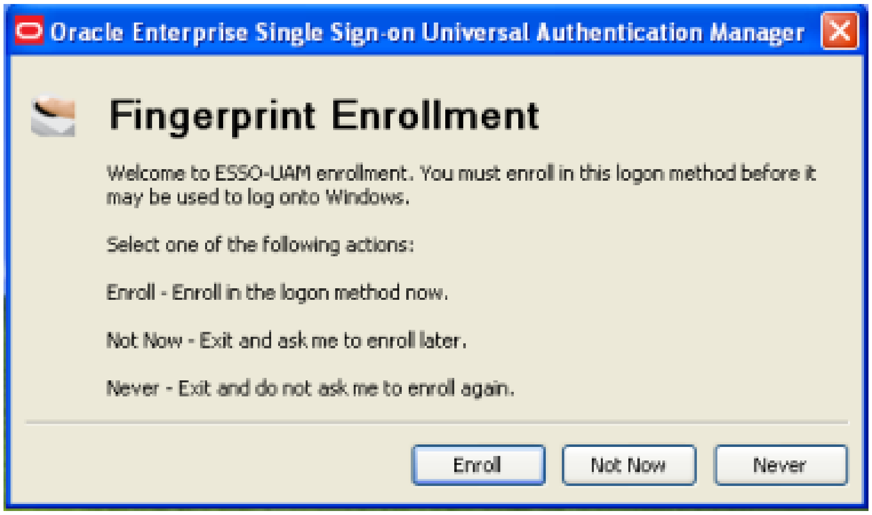
> This logon method requires BIO-key BioAPI BSP to be installed. If this is not installed, you will get an error message. Contact your system administrator for assistance.

The following topics are discussed:

- Enrolling a Fingerprint at Windows Logon
- Enrolling a Fingerprint when Launching the ESSO-UAM Client
- Enrolling a Fingerprint Manually

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 see the following prompt:



Oracle Enterprise Single Sign-on Universal Authentication Manager

Fingerprint Enrollment

Welcome to ESSO-UAM enrollment. You must enroll in this logon method before it may be used to log onto Windows.

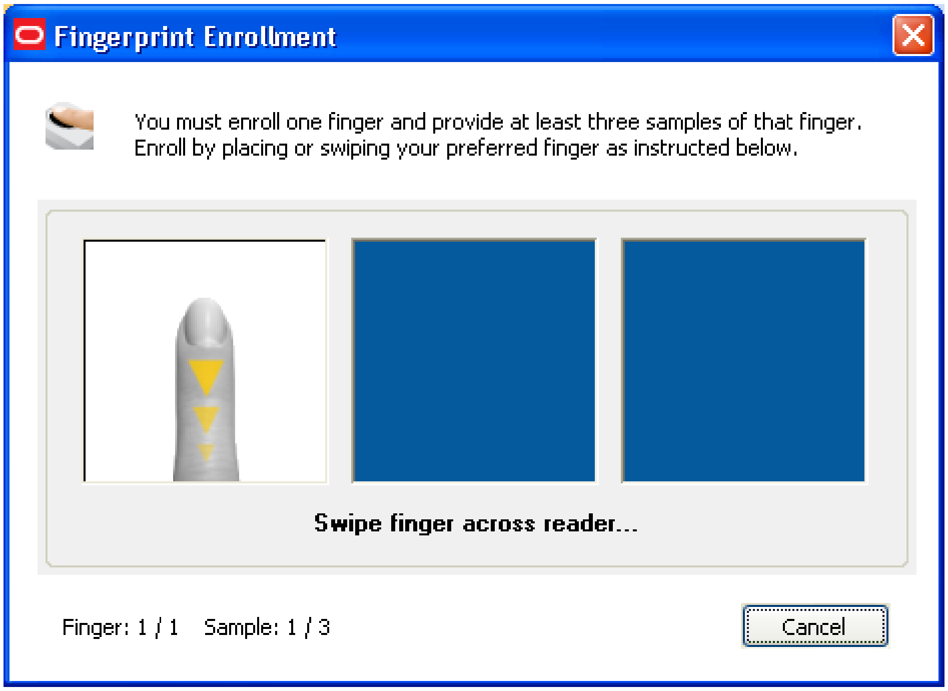
Select one of the following actions:

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.

1. Click **Enroll** to enroll a fingerprint. You are prompted to enroll at least one fingerprint sample. The number of fingerprint samples is configured by your administrator. Enroll by placing or swiping your preferred finger.



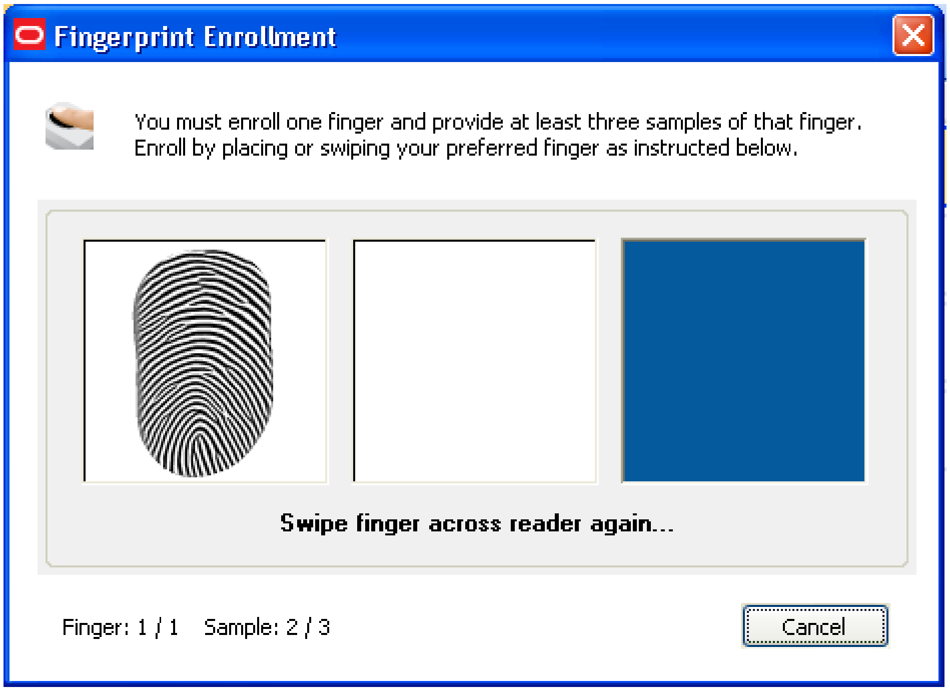
Fingerprint Enrollment

You must enroll one finger and provide at least three samples of that finger. Enroll by placing or swiping your preferred finger as instructed below.

Swipe finger across reader...

Finger: 1 / 1 Sample: 1 / 3

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



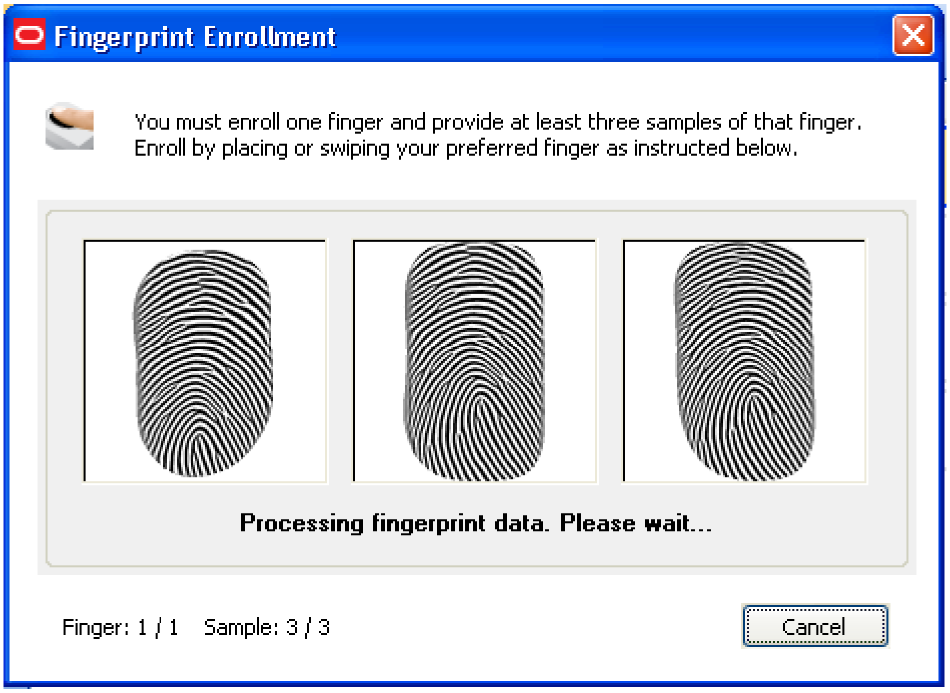
Fingerprint Enrollment

You must enroll one finger and provide at least three samples of that finger. Enroll by placing or swiping your preferred finger as instructed below.

Swipe finger across reader again...

Finger: 1 / 1 Sample: 2 / 3

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

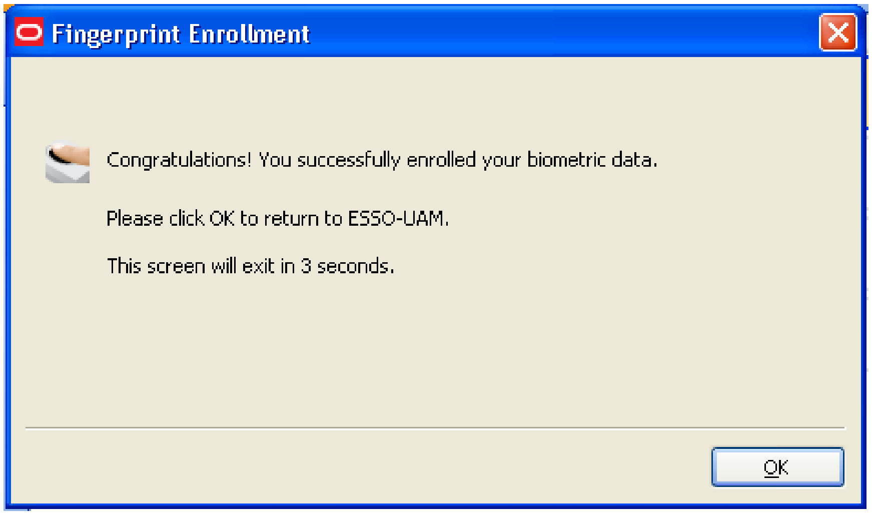


You must enroll one finger and provide at least three samples of that finger. Enroll by placing or swiping your preferred finger as instructed below.

Processing fingerprint data. Please wait...

Finger: 1 / 1 Sample: 3 / 3

4. 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 ESSO-UAM logon methods are installed, you may be prompted to enroll in additional methods.



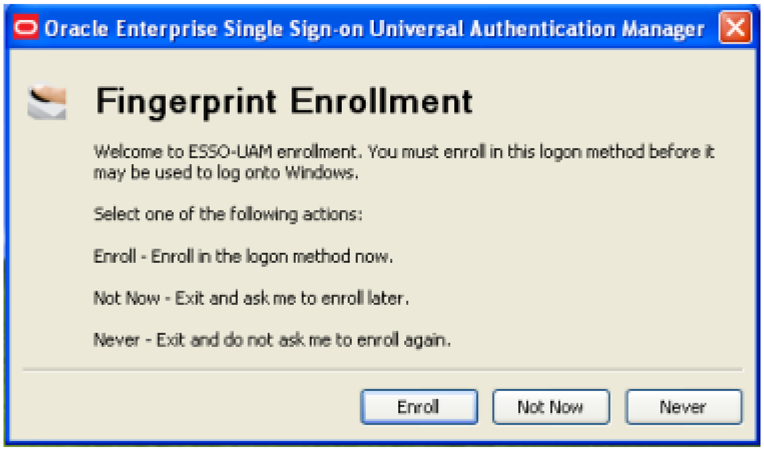
Congratulations! You successfully enrolled your biometric data.

Please click OK to return to ESSO-UAM.

This screen will exit in 3 seconds.

Enrolling a Fingerprint when Launching the ESSO-UAM Client

When you launch the ESSO-UAM client, 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 see the following prompt:



Oracle Enterprise Single Sign-on Universal Authentication Manager

Fingerprint Enrollment

Welcome to ESSO-UAM enrollment. You must enroll in this logon method before it may be used to log onto Windows.

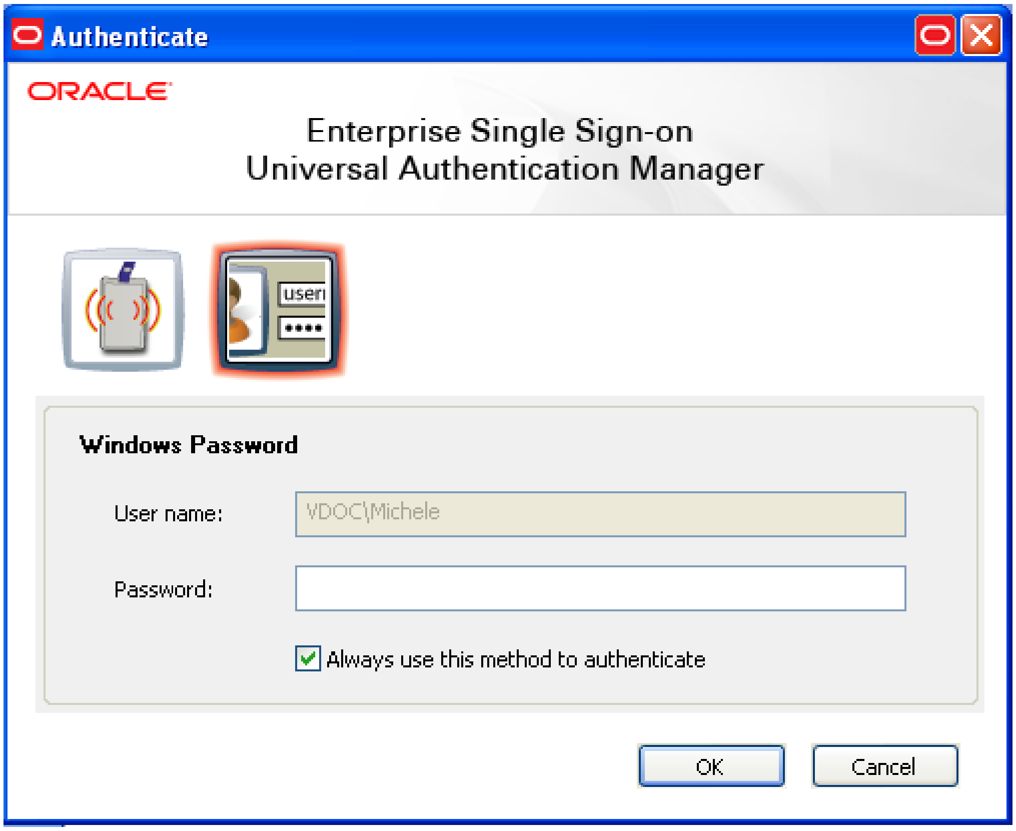
Select one of the following actions:

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.

1. Click **Enroll** to enroll a fingerprint. You are prompted to authenticate to continue. 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).



Authenticate

ORACLE

Enterprise Single Sign-on
Universal Authentication Manager

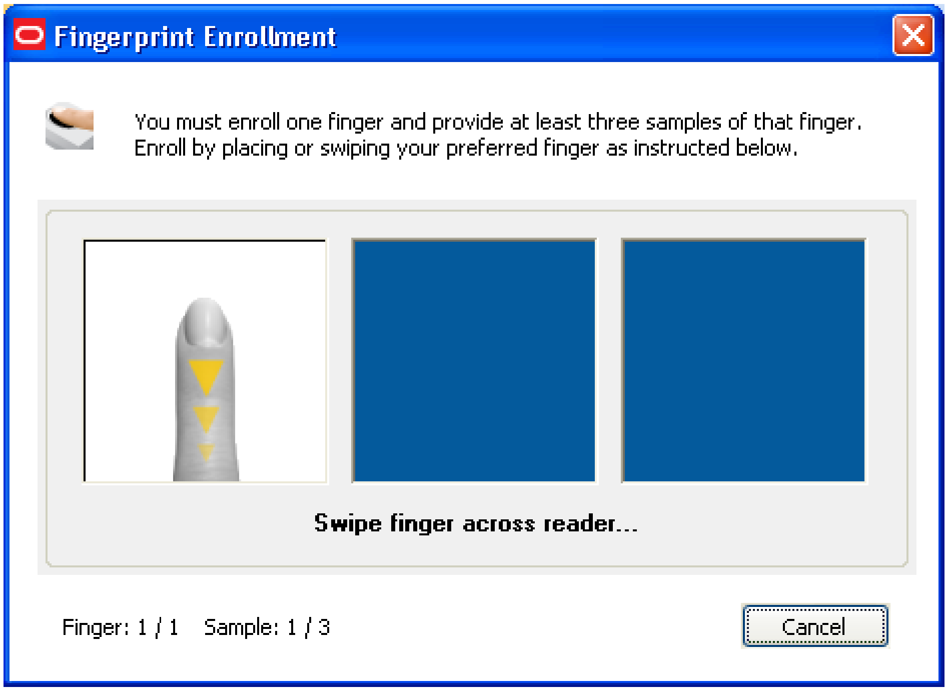
Windows Password

User name: VDOC\Michele

Password:

☑ Always use this method to authenticate

2. After you authenticate, you are prompted to enroll at least one fingerprint sample. The number of fingerprint samples is configured by your administrator. Enroll by placing or swiping your preferred finger.



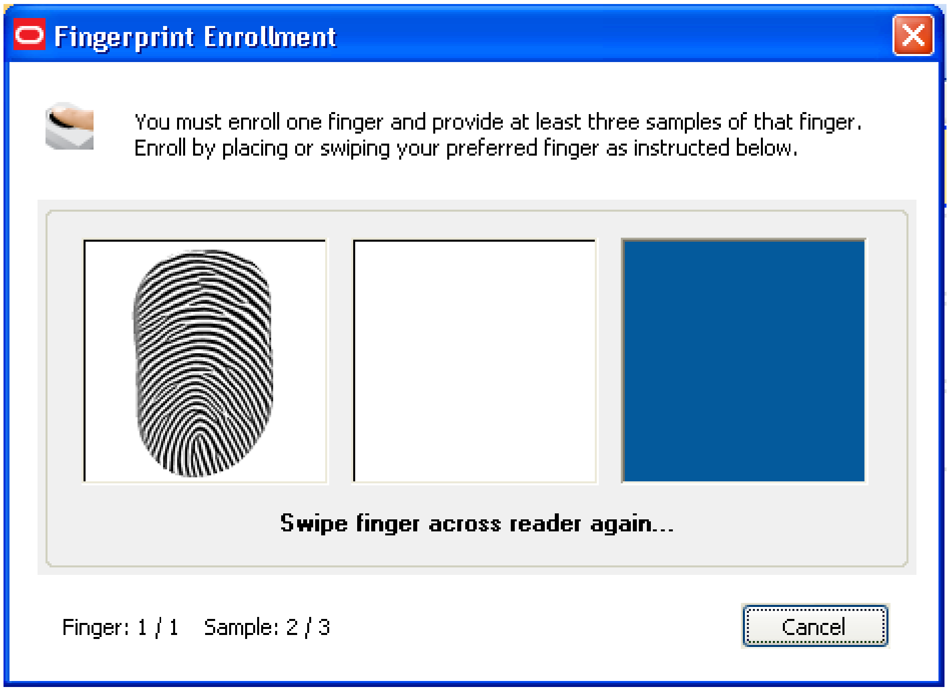
Fingerprint Enrollment

You must enroll one finger and provide at least three samples of that finger. Enroll by placing or swiping your preferred finger as instructed below.

Swipe finger across reader...

Finger: 1 / 1 Sample: 1 / 3

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



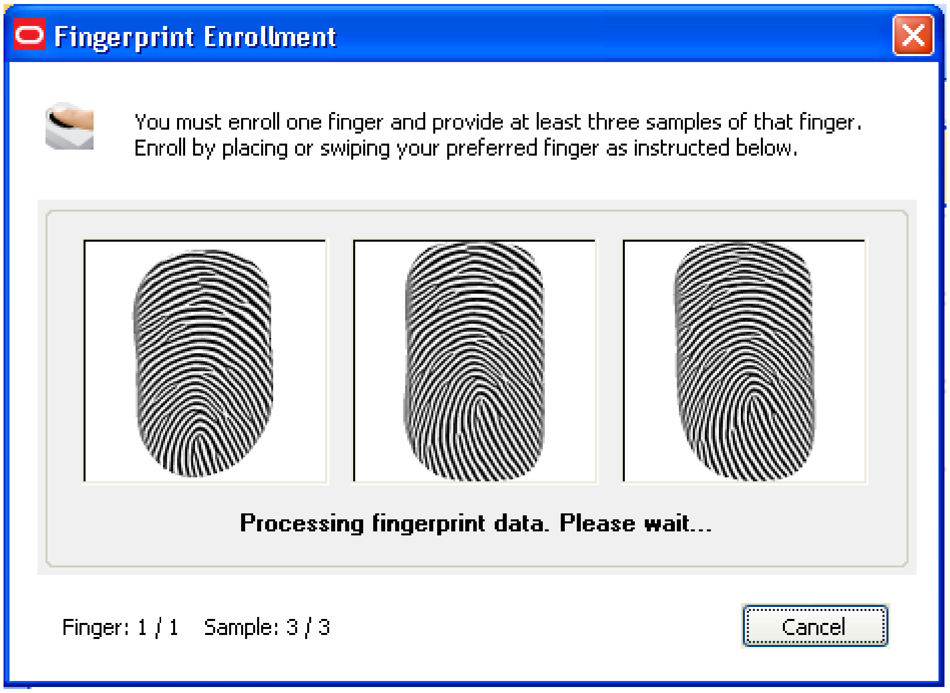
Fingerprint Enrollment

You must enroll one finger and provide at least three samples of that finger. Enroll by placing or swiping your preferred finger as instructed below.

Swipe finger across reader again...

Finger: 1 / 1 Sample: 2 / 3

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



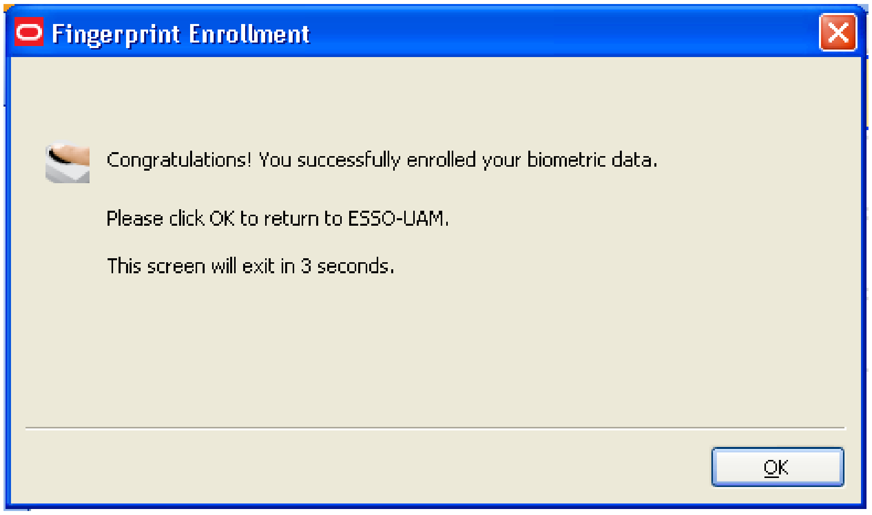
Fingerprint Enrollment

You must enroll one finger and provide at least three samples of that finger. Enroll by placing or swiping your preferred finger as instructed below.

Processing fingerprint data. Please wait...

Finger: 1 / 1 Sample: 3 / 3

5. When enrollment is complete, a message confirms that your biometric data is enrolled. Click **OK** to return to ESSO-UAM.



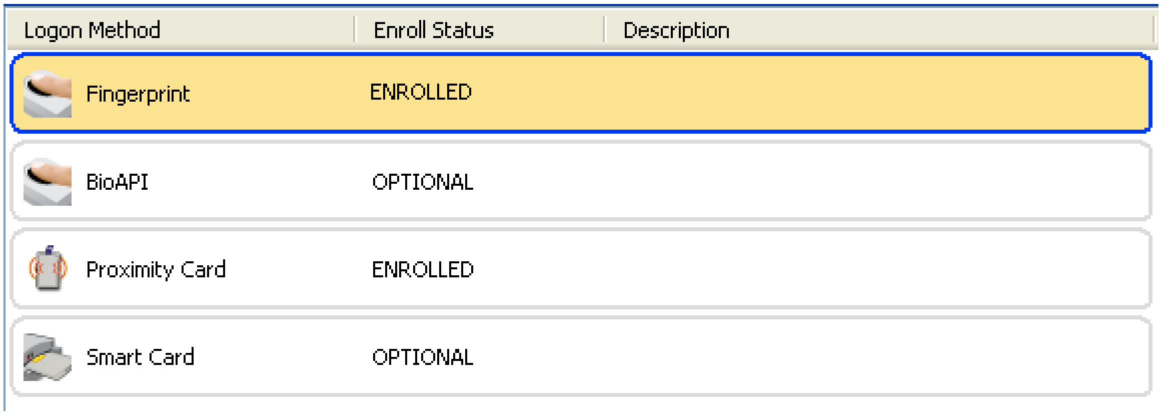
Fingerprint Enrollment

Congratulations! You successfully enrolled your biometric data.

Please click OK to return to ESSO-UAM.

This screen will exit in 3 seconds.

6. The Enroll Status column shows a status of ENROLLED.



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

Enrolling a Fingerprint Manually

To enroll a fingerprint manually:

1. Launch the ESSO-UAM client.
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. When prompted to authenticate, authenticate with an enrolled method.
4. Follow the steps to enroll your biometric data (see detailed instructions in previous section).
5. A message confirms that you have successfully enrolled your biometric data. The Enroll Status column shows a status of ENROLLED.

BioAPI Logon Method

ESSO-UAM enables you to enroll and use any third part BioAPI-compliant Biometric Service Provider (BSP) module as an authentication mechanism to ESSO-UAM. In addition to fingerprint biometrics, this logon method may also support other biometric technologies that offer a BSP such as palm, facial, and iris recognition solutions.

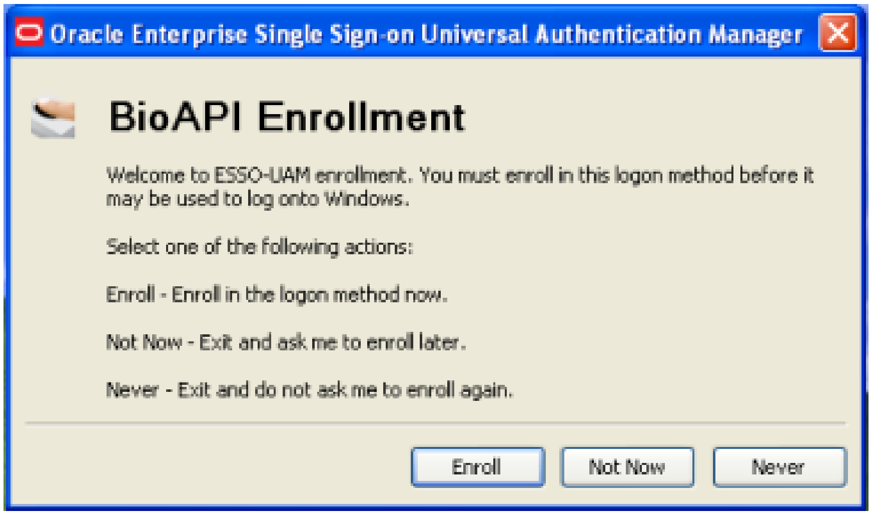
> This logon method requires a supported biometric reader device and BioAPI compatible BSP middleware. If the BioAPI BSP is not installed and properly configured with a compatible biometric reader device, you will get an error. Contact your system administrator for assistance.

The following topics are discussed:

- Enrolling BioAPI at Windows Logon
- Enrolling BioAPI when Launching the ESSO-UAM Client
- Enrolling BioAPI Manually

Enrolling BioAPI 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 BioAPI, you will see the following prompt:



Oracle Enterprise Single Sign-on Universal Authentication Manager

BioAPI Enrollment

Welcome to ESSO-UAM enrollment. You must enroll in this logon method before it may be used to log onto Windows.

Select one of the following actions:

Enroll - Enroll in the logon method now.

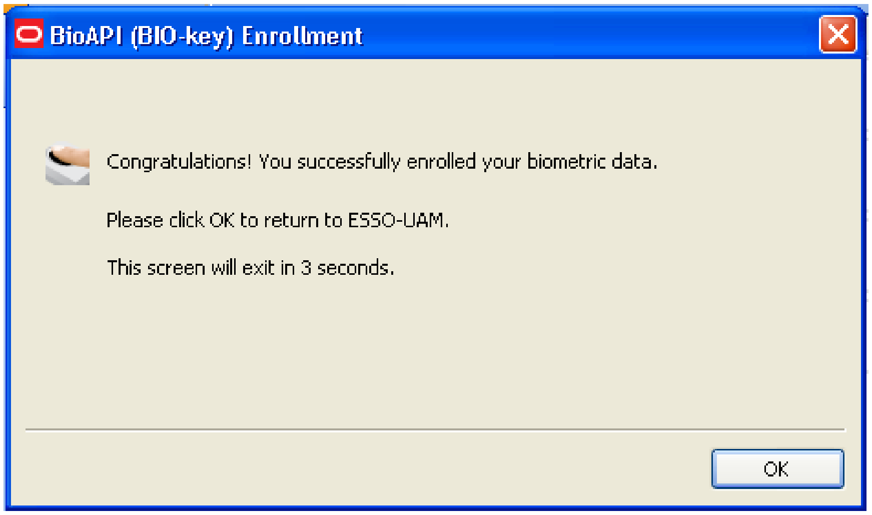
Not Now - Exit and ask me to enroll later.

Never - Exit and do not ask me to enroll again.

1. Click **Enroll**. The Enrollment Wizard launches. Click **Next** to begin the enrollment process.
2. Follow the on-screen instructions to enroll your biometric samples.

> For the BioAPI Logon Method, each third party BSP provider will have different enrollment steps to follow.

3. 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 ESSO-UAM logon methods are installed, you may be prompted to enroll in additional methods.



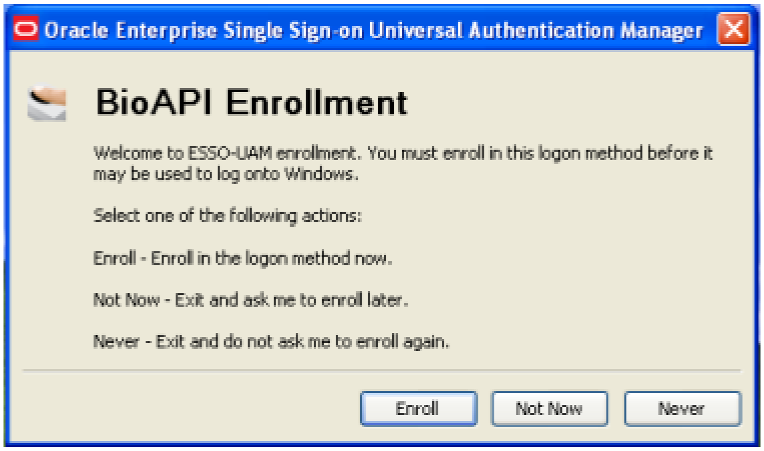
Congratulations! You successfully enrolled your biometric data.

Please click OK to return to ESSO-UAM.

This screen will exit in 3 seconds.

Enrolling BioAPI when Launching the ESSO-UAM Client

When you launch the ESSO-UAM client, you are automatically prompted to enroll installed logon methods (if they are not already enrolled). If one of those methods is BioAPI, you will see the following prompt:


Oracle Enterprise Single Sign-on Universal Authentication Manager
BioAPI Enrollment
Enroll
Not Now
Never

Welcome to ESSO-UAM enrollment. You must enroll in this logon method before it may be used to log onto Windows.

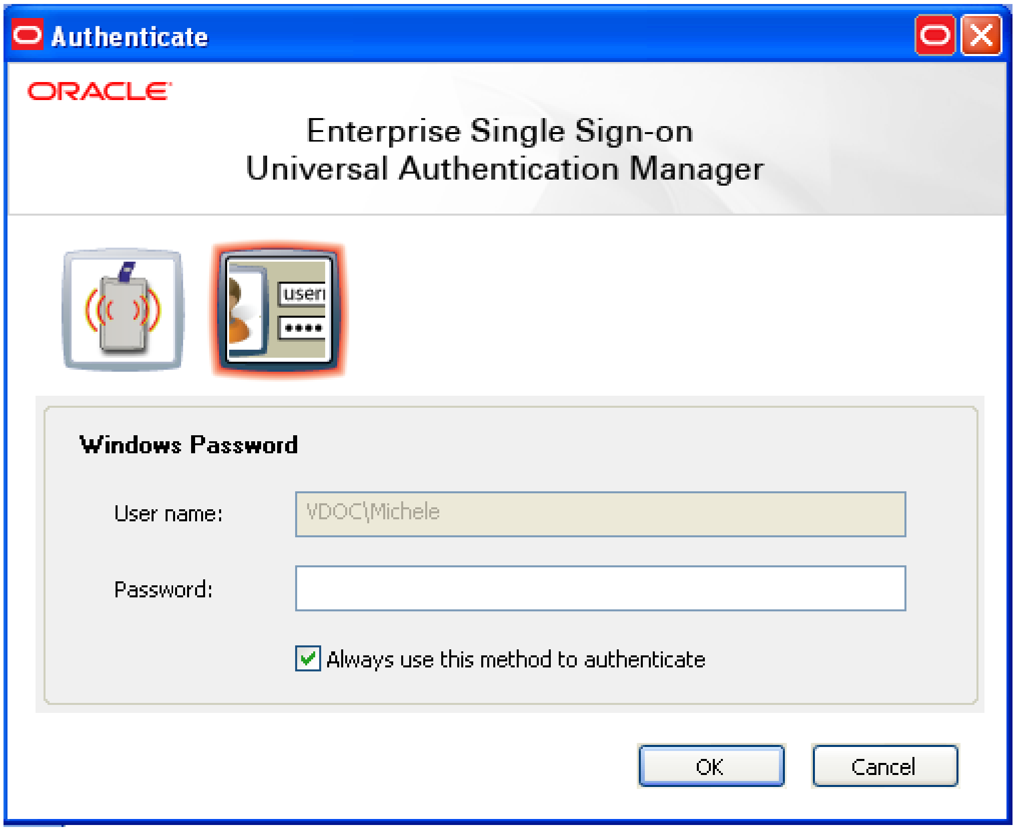
Select one of the following actions:

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.

1. Click **Enroll** . You are prompted to authenticate to continue. 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).



Windows Password

User name: VDOC\Michele

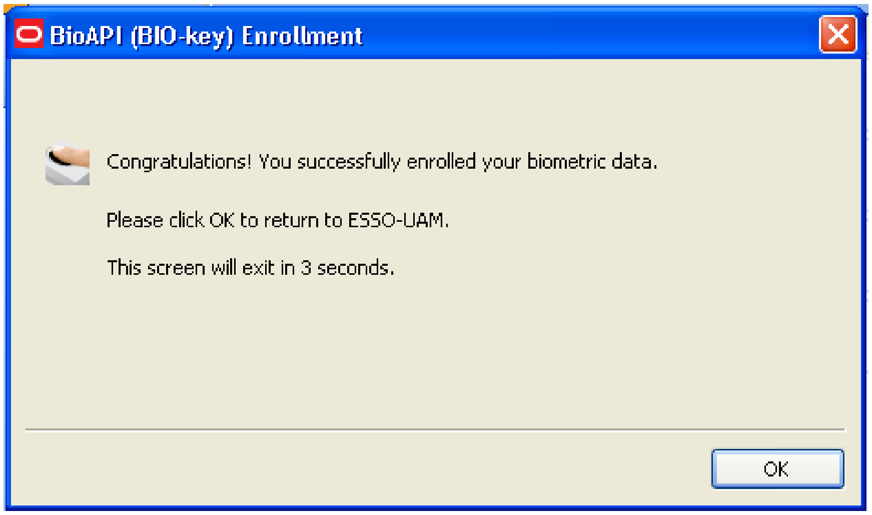
Password:

☑ Always use this method to authenticate

2. Follow the on-screen instructions to enroll your biometric samples.

> For the BioAPI Logon Method, each third party BSP provider will have different enrollment steps to follow.

3. When enrollment is complete, a message confirms that your biometric data is enrolled. Click **OK** to return to ESSO-UAM.

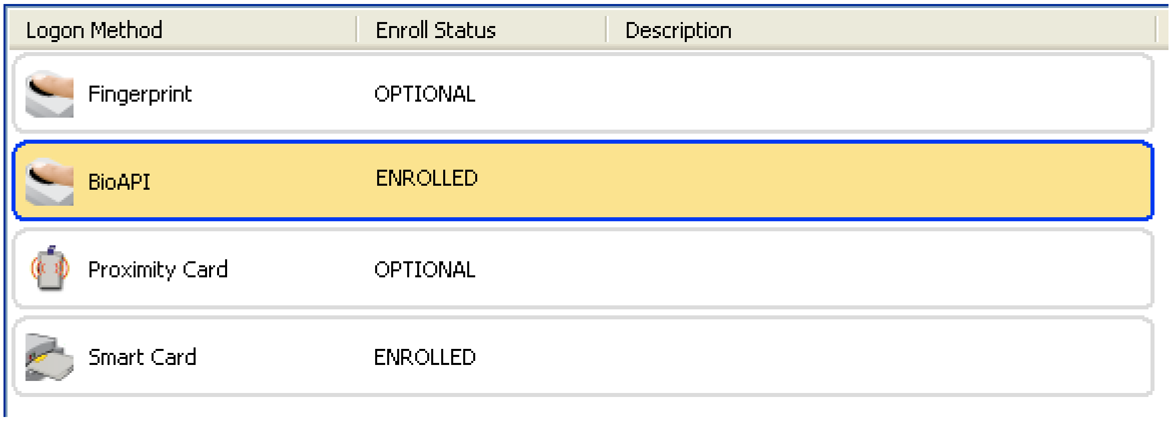


Congratulations! You successfully enrolled your biometric data.

Please click OK to return to ESSO-UAM.

This screen will exit in 3 seconds.

4. The Enroll Status column shows a status of ENROLLED.



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

Enrolling BioAPI Manually

To enroll BioAPI manually:

1. Launch the ESSO-UAM client.
2. Click **Enroll** in the Logon Methods toolbar and select **BioAPI** from the drop-down list; or right-click in the highlighted BioAPI row and select **Enroll**; or double click in the BioAPI row.
3. When prompted to authenticate, authenticate with an enrolled method.
4. Follow the on-screen instructions to enroll your biometric samples.
5. A message confirms that you have successfully enrolled your biometric data. The Enroll Status column shows a status of ENROLLED.

Proximity Card Logon Method

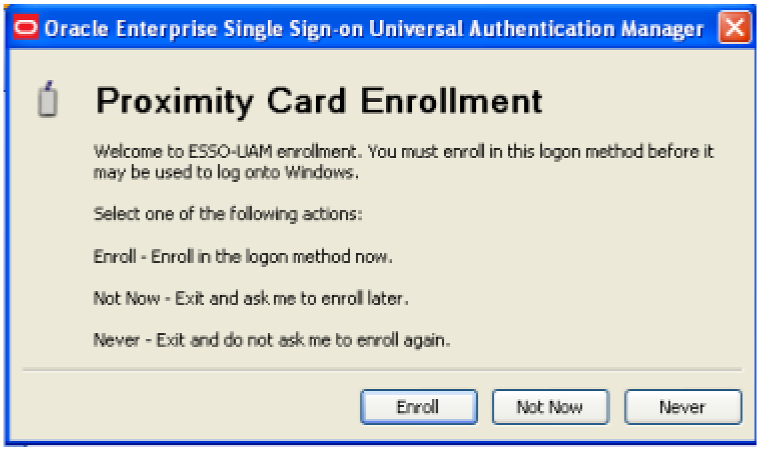
A passive proximity card or token is an identity object (such as a workplace ID badge) containing a circuit that a card-reading device can detect and decipher. When you place a proximity card close to a card reader, the reader detects the token's presence and recognizes identifying information that is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

- Enrolling a Proximity Card at Windows Logon
- Enrolling a Proximity Card when Launching the ESSO-UAM Client
- Enrolling a Proximity Card Manually
- Changing an ESSO-UAM PIN

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 see the following prompt:



Oracle Enterprise Single Sign-on Universal Authentication Manager

Proximity Card Enrollment

Welcome to ESSO-UAM enrollment. You must enroll in this logon method before it may be used to log onto Windows.

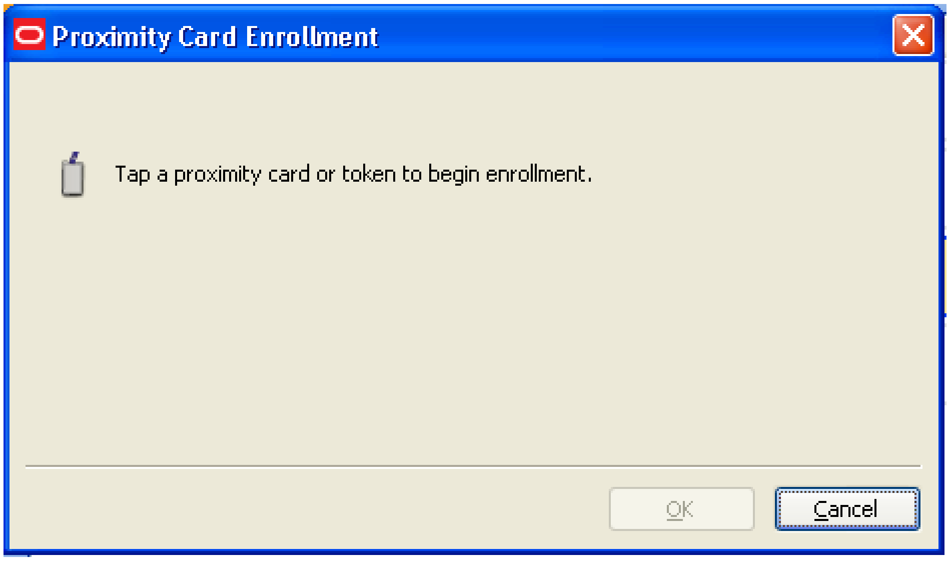
Select one of the following actions:

Enroll - Enroll in the logon method now.

Not Now - Exit and ask me to enroll later.

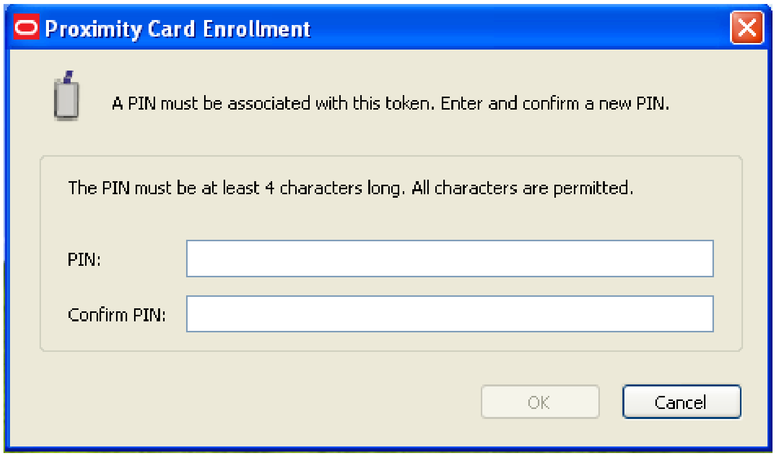
Never - Exit and do not ask me to enroll again.

1. Click **Enroll** to enroll a proximity card. You are prompted to tap your card.



Tap a proximity card or token to begin enrollment.

2. Tap the card. If your system is configured to require a PIN with a proximity card, you will be prompted to enroll a PIN that will be linked with the card.



Proximity Card Enrollment

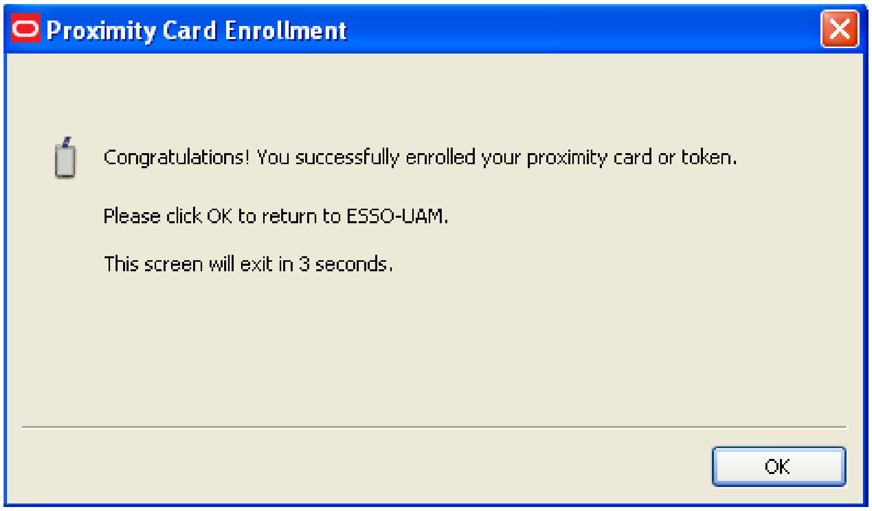
A PIN must be associated with this token. Enter and confirm a new PIN.

The PIN must be at least 4 characters long. All characters are permitted.

PIN:

Confirm PIN:

3. Enter and confirm the PIN and click **OK**.
4. When enrollment is complete, a message confirms that your card is enrolled. Click **OK** to exit and resume log on to Windows. If other ESSO-UAM logon methods are installed, you may be prompted to enroll in additional methods.



Proximity Card Enrollment

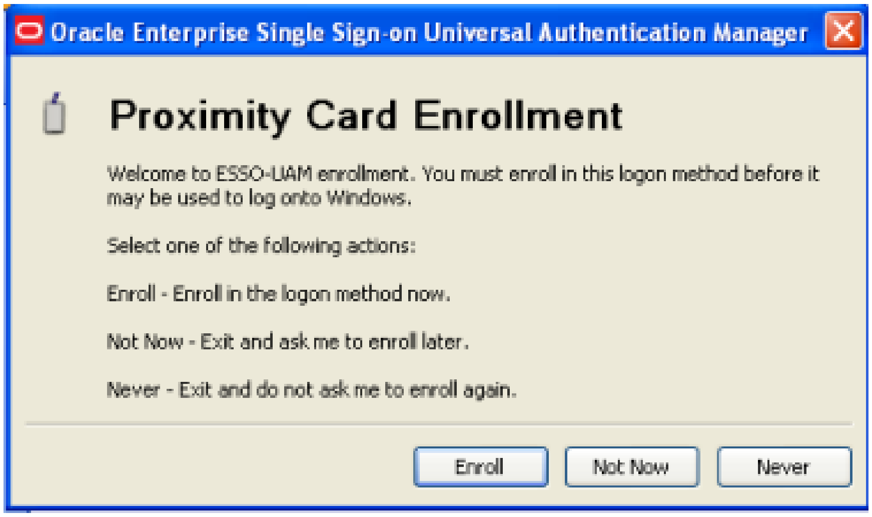
Congratulations! You successfully enrolled your proximity card or token.

Please click OK to return to ESSO-UAM.

This screen will exit in 3 seconds.

Enrolling a Proximity Card when Launching the ESSO-UAM Client

When you launch the ESSO-UAM client, you are automatically prompted to enroll installed logon methods. If one of those methods is a proximity card, you will see the following prompt:



Oracle Enterprise Single Sign-on Universal Authentication Manager

Proximity Card Enrollment

Welcome to ESSO-UAM enrollment. You must enroll in this logon method before it may be used to log onto Windows.

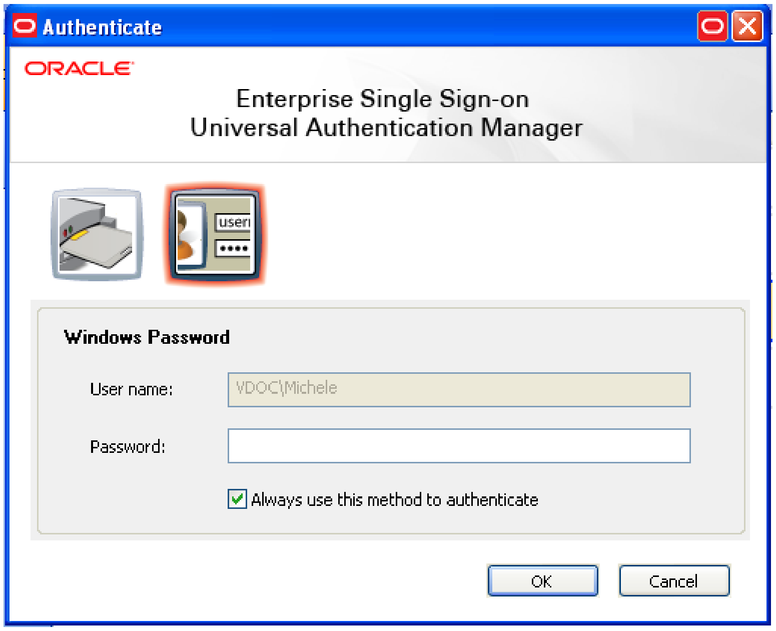
Select one of the following actions:

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.

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 (in the screen sample below, you can select to authenticate with either a Windows password or smart card)



Authenticate

ORACLE

Enterprise Single Sign-on
Universal Authentication Manager

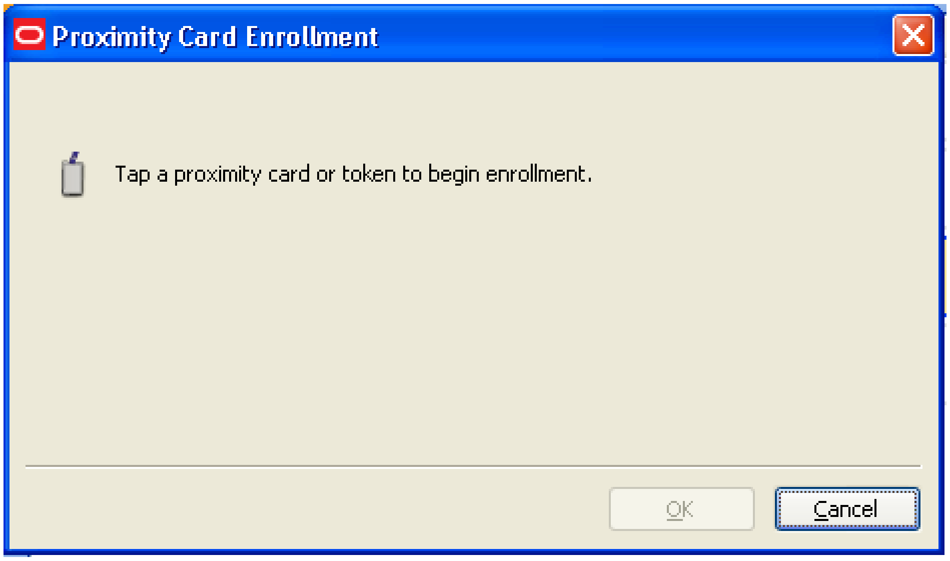
Windows Password

User name: VDOC\Michele

Password:

☑ Always use this method to authenticate

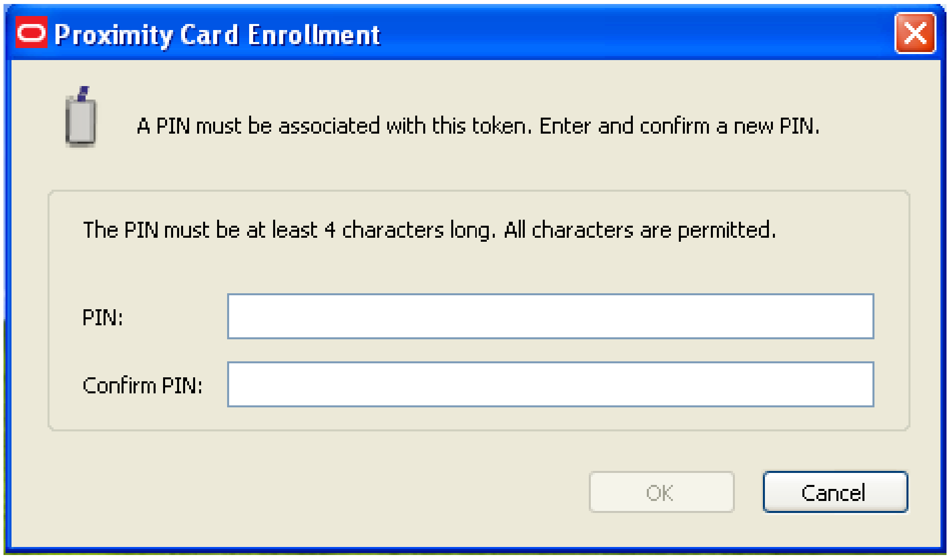
2. After you authenticate, you are prompted to tap your proximity card on the card reader.



Proximity Card Enrollment

Tap a proximity card or token to begin enrollment.

3. Tap the card. If your system is configured to require a PIN with a proximity card, you will be prompted to enroll a PIN that will be linked with the card.



Proximity Card Enrollment

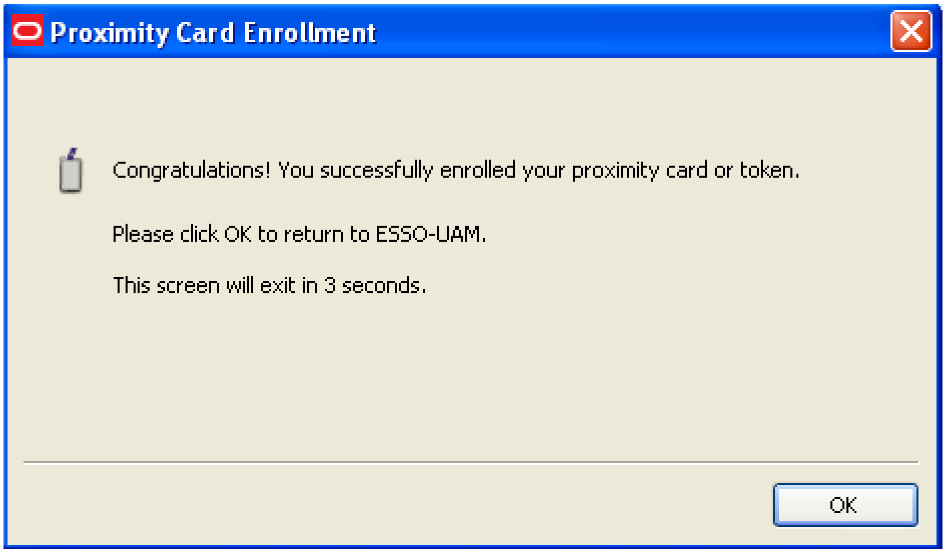
A PIN must be associated with this token. Enter and confirm a new PIN.

The PIN must be at least 4 characters long. All characters are permitted.

PIN:

Confirm PIN:

4. Enter and confirm the PIN and click **OK**.
5. A message confirms that you have successfully enrolled your card. Click **OK** to return to ESSO-UAM.

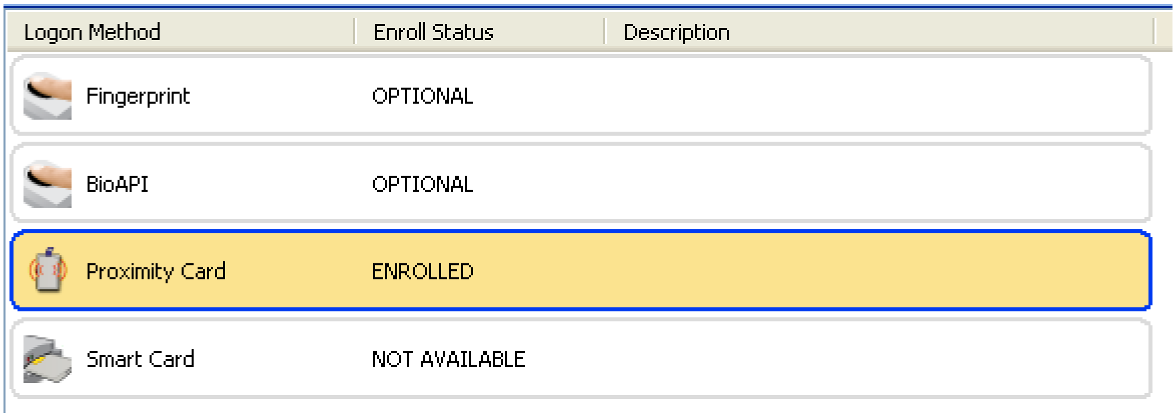


Congratulations! You successfully enrolled your proximity card or token.

Please click OK to return to ESSO-UAM.

This screen will exit in 3 seconds.

6. The Enroll Status column shows a status of ENROLLED.



Logon Method	Enroll Status	Description
Fingerprint	OPTIONAL	
BioAPI	OPTIONAL	
Proximity Card	ENROLLED	
Smart Card	NOT AVAILABLE	

Enrolling a Proximity Card Manually

To enroll a proximity card manually:

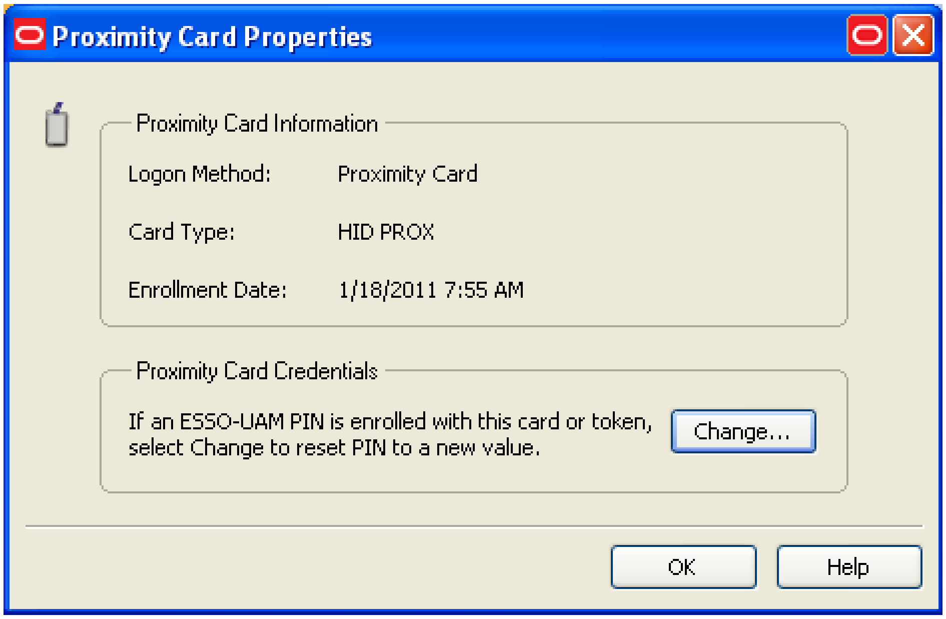
1. Launch the ESSO-UAM client.
2. Click **Enroll** in the Logon Methods toolbar and select **Proximity Card** from the drop-down list; or right-click in the highlighted proximity card row and select **Enroll**; or double click in the proximity card row.
3. When prompted to authenticate, authenticate with an enrolled method.
4. Tap your proximity card when prompted.
5. If your system is configured to require a PIN with a proximity card, you will be prompted to enroll a PIN that will be linked with the card. When prompted, type and re-type the PIN. (see detailed instructions in previous section).
6. A message confirms that you have successfully enrolled your card. Click **OK** to return to ESSO-UAM. The Enroll Status column on the interface 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.

Changing an ESSO-UAM PIN

If your ESSO-UAM proximity card is enrolled with an associated PIN and you wish to change the PIN:

1. Launch the ESSO-UAM client.
2. Select the enrolled proximity card from the Logon Methods screen.
3. Click **Modify** in the toolbar at the top of the screen or right-click the highlighted card and select **Modify** from the pop-up menu. The screen that opens displays the properties of the proximity card as well as a **Change...** button. Click **Change...** to change the PIN for the card.



Proximity Card Properties

Proximity Card Information

Logon Method: Proximity Card

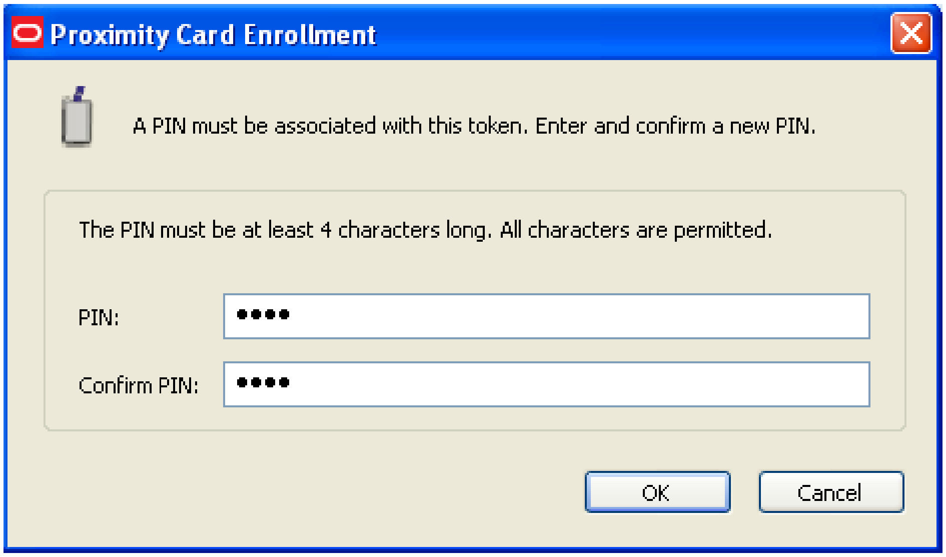
Card Type: HID PROX

Enrollment Date: 1/18/2011 7:55 AM

Proximity Card Credentials

If an ESSO-UAM PIN is enrolled with this card or token, select Change to reset PIN to a new value.

4. When prompted to authenticate, authenticate with an enrolled method.
5. When prompted, tap the card.
6. When prompted, enter and confirm a new PIN.



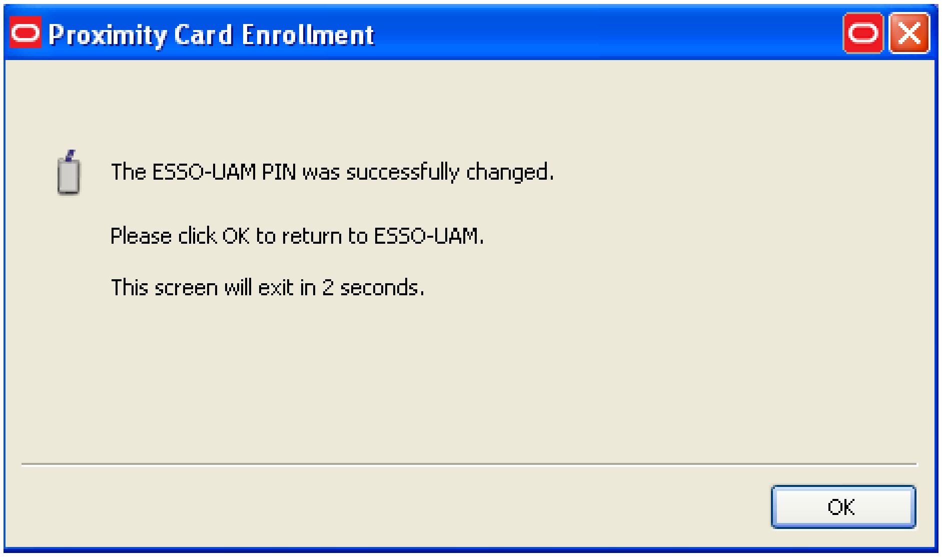
A PIN must be associated with this token. Enter and confirm a new PIN.

The PIN must be at least 4 characters long. All characters are permitted.

PIN: ••••

Confirm PIN: ••••

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



The ESSO-UAM PIN was successfully changed.

Please click OK to return to ESSO-UAM.

This screen will exit in 2 seconds.

Smart Card Logon Method

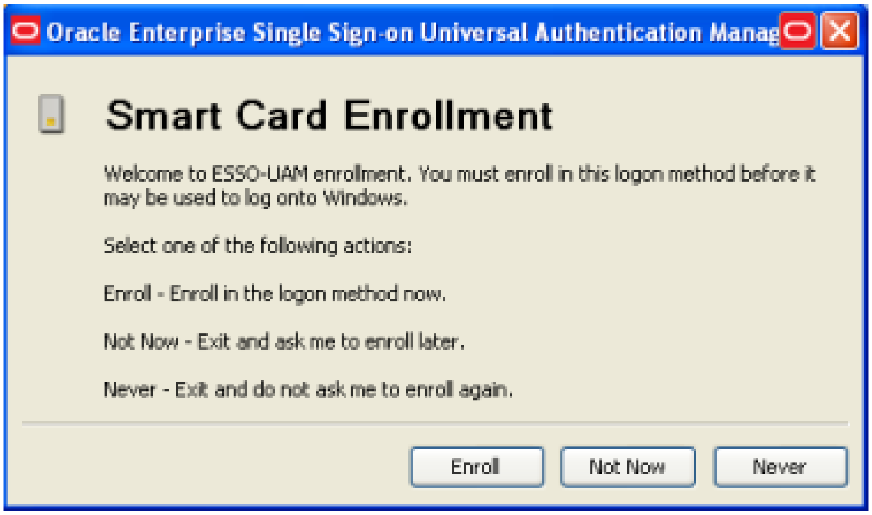
A smart card is a credit card-sized token containing a chip or embedded circuits that can store and process data securely. Information stored on a smart card can also be used for identification and authentication. ESSO-UAM enables you to enroll and use smart cards for logon and authentication without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

The following topics are discussed:

- Enrolling a Smart Card at Windows Logon
- Enrolling a Smart Card when Launching the ESSO-UAM Client
- Enrolling a Smart Card Manually

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 see the following prompt:



Oracle Enterprise Single Sign-on Universal Authentication Manag

Smart Card Enrollment

Welcome to ESSO-UAM enrollment. You must enroll in this logon method before it may be used to log onto Windows.

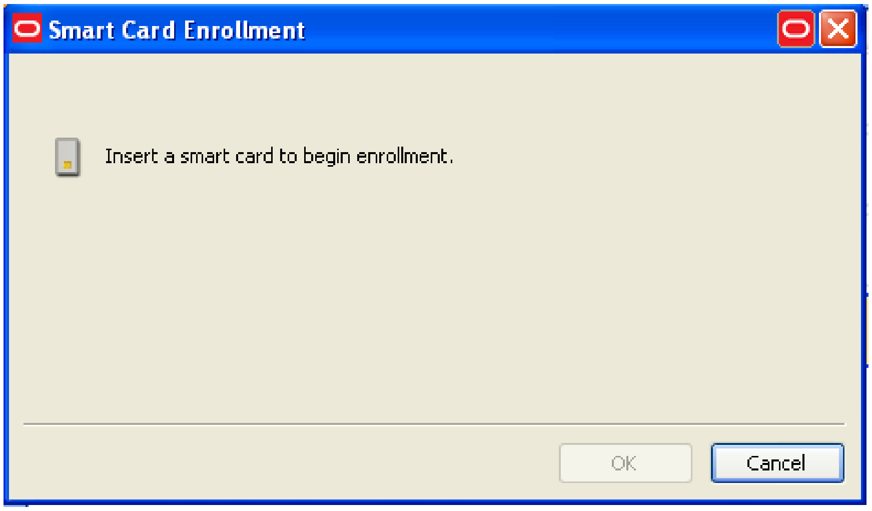
Select one of the following actions:

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.

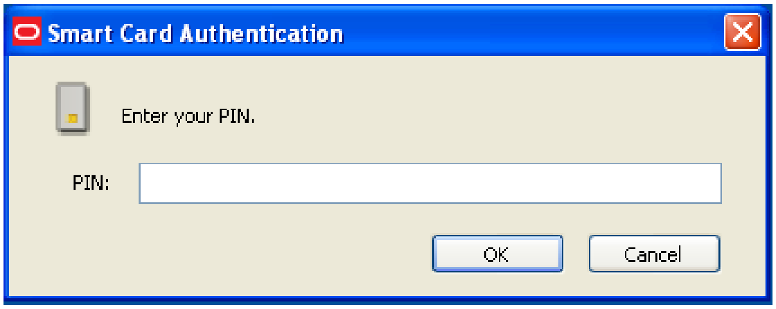
1. Click **Enroll** to enroll a smart card. You are prompted to insert your card.



Smart Card Enrollment

Insert a smart card to begin enrollment.

2. Insert the card. If your system is configured to require a PIN with a smart card, you are prompted to enter the PIN associated with the card.

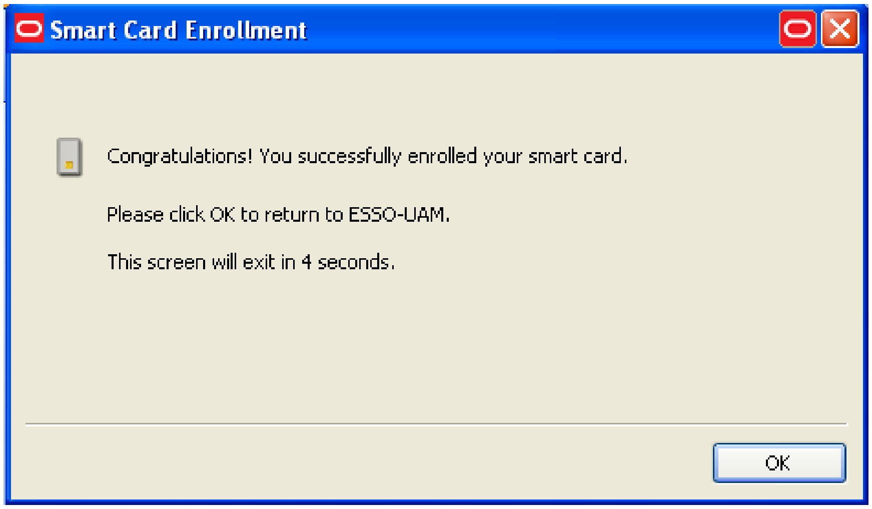


Smart Card Authentication

Enter your PIN.

PIN:

3. Enter the PIN and click **OK**.
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 log on to Windows. If other ESSO-UAM logon methods are installed, you may be prompted to enroll in additional methods.



Smart Card Enrollment

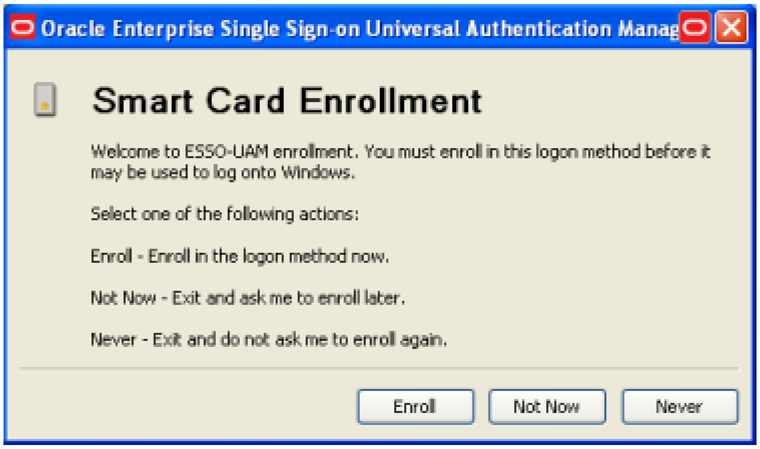
Congratulations! You successfully enrolled your smart card.

Please click OK to return to ESSO-UAM.

This screen will exit in 4 seconds.

Enrolling a Smart Card when Launching the ESSO-UAM Client

When you launch the ESSO-UAM client, 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 see the following prompt:



Oracle Enterprise Single Sign-on Universal Authentication Manag

Smart Card Enrollment

Welcome to ESSO-UAM enrollment. You must enroll in this logon method before it may be used to log onto Windows.

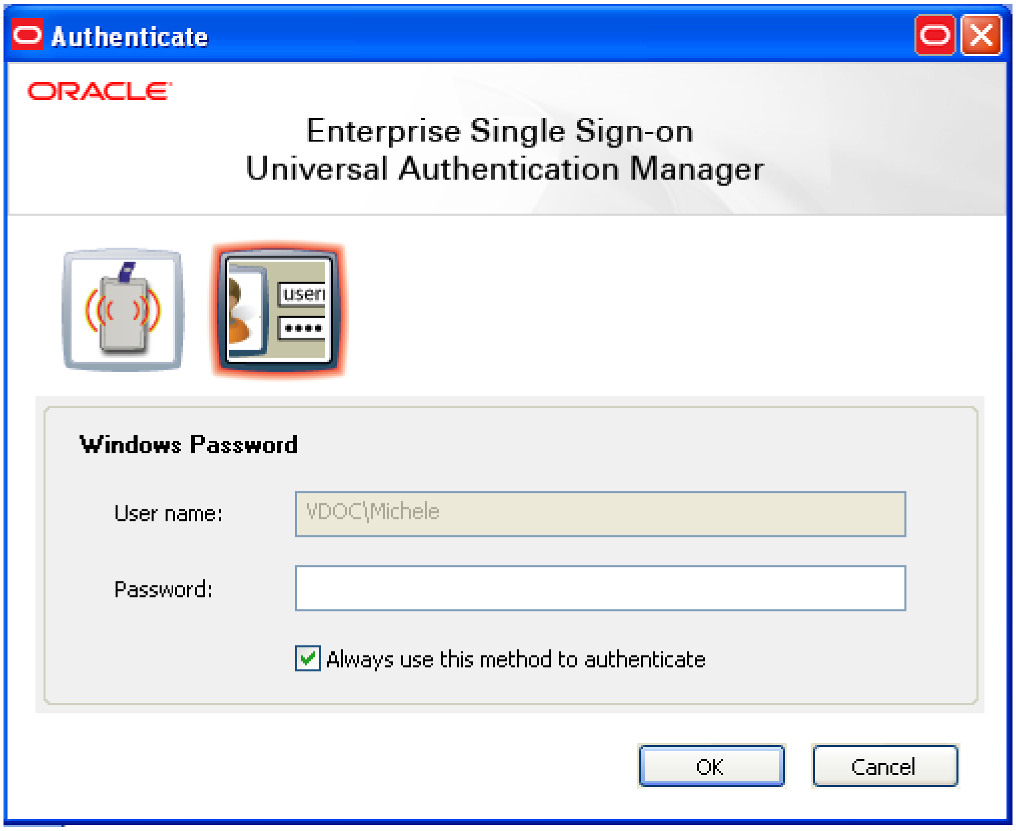
Select one of the following actions:

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.

1. Click **Enroll** to enroll a smart card. You are prompted to authenticate to continue. 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).



Authenticate

ORACLE

Enterprise Single Sign-on
Universal Authentication Manager

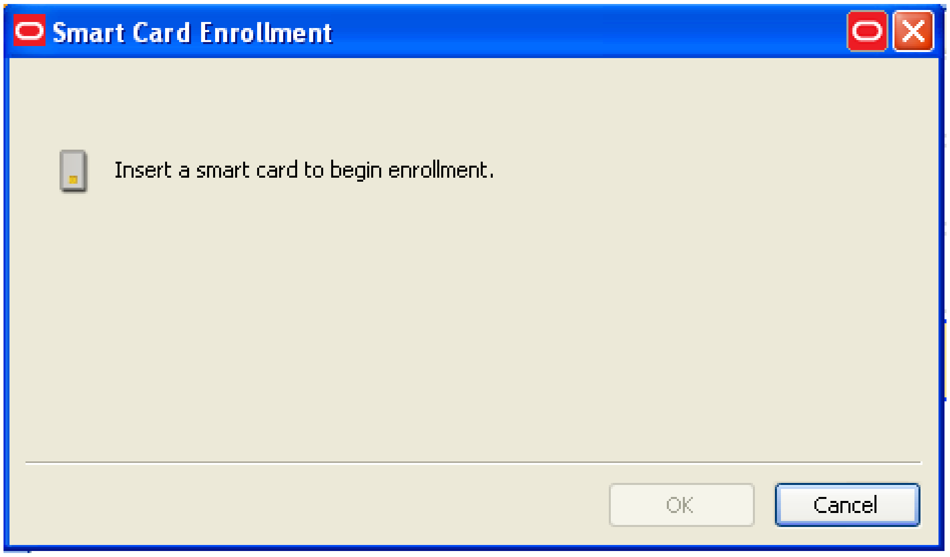
Windows Password

User name: VDOC\Michele

Password:

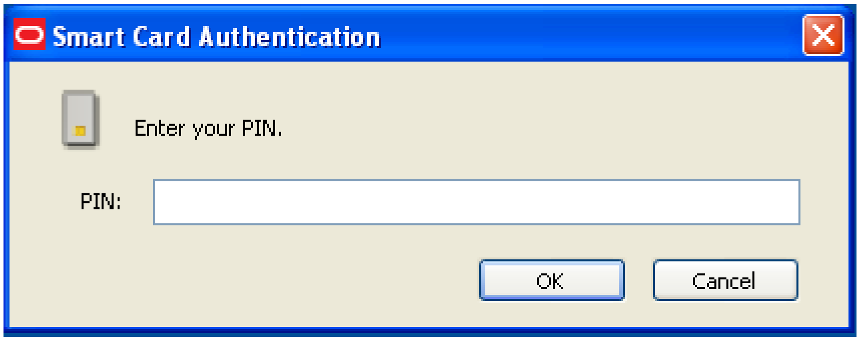
☑ Always use this method to authenticate

2. After you authenticate, you are prompted to insert your smart card into the card reader. If you insert your card first without entering your Windows password, a message states that the card is not currently enrolled.



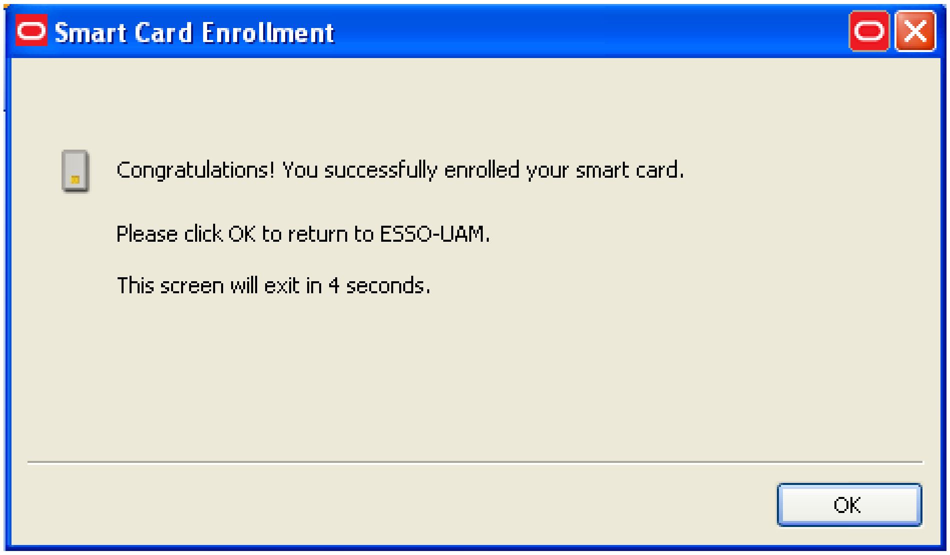
Insert a smart card to begin enrollment.

3. Insert the card. If your system is configured to require a PIN with a smart card, you are prompted to enter the PIN associated with the card.



Enter your PIN.

4. Enter the PIN and click **OK**.
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 ESSO-UAM.

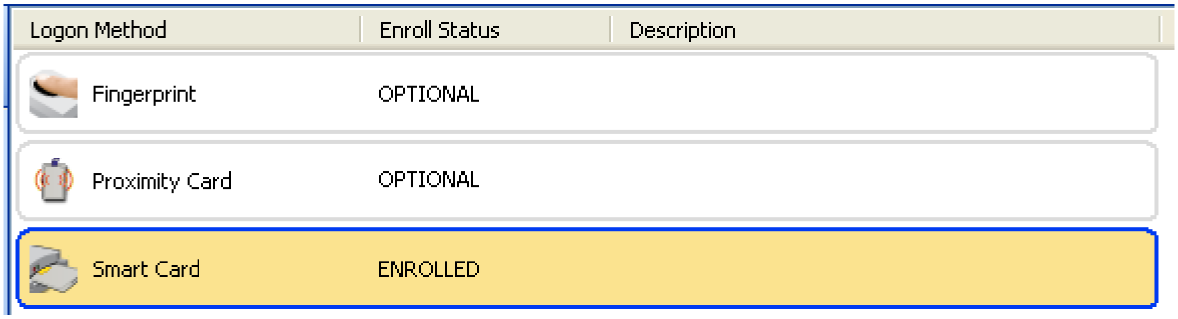


Congratulations! You successfully enrolled your smart card.

Please click OK to return to ESSO-UAM.

This screen will exit in 4 seconds.

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 the ESSO-UAM client.
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. When prompted to authenticate, authenticate with an enrolled method.
5. If your system is configured to require a PIN for your smart card, you will be prompted to enter it. Enter the PIN. (see detailed instructions in previous section).
6. Click **OK** to return to ESSO-UAM. A message confirms that you have successfully enrolled your card. The Enroll Status column shows a status of ENROLLED.

Integration with ESSO-LM

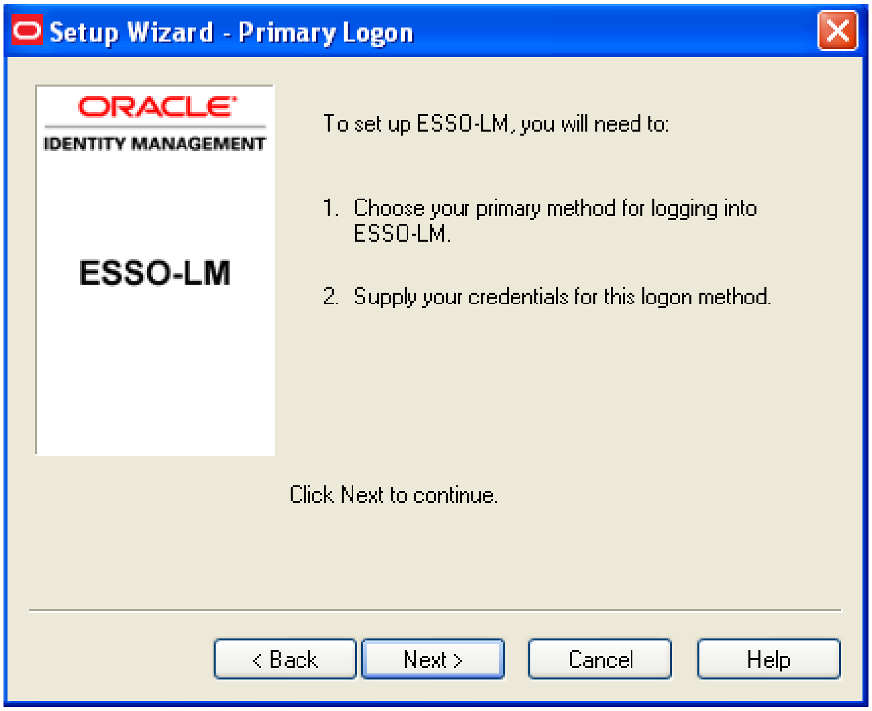
ESSO-UAM can operate as a stand-alone application and also integrate seamlessly with ESSO-LM. If your administrator has enabled and installed the ESSO-UAM authenticator during a ESSO-UAM custom installation, the ESSO-UAM authenticator will be added to the list of ESSO-LM logon methods. If you wish to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

> ESSO-UAM authenticator must be installed before you can configure ESSO-UAM as the primary logon method for ESSO-LM. For details on installing the necessary integration components, see the *ESSO-UAM Install and Setup Guide*.

Configuring ESSO-UAM as the Primary Logon Method with the First-Time Use Wizard

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

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



Setup Wizard - Primary Logon

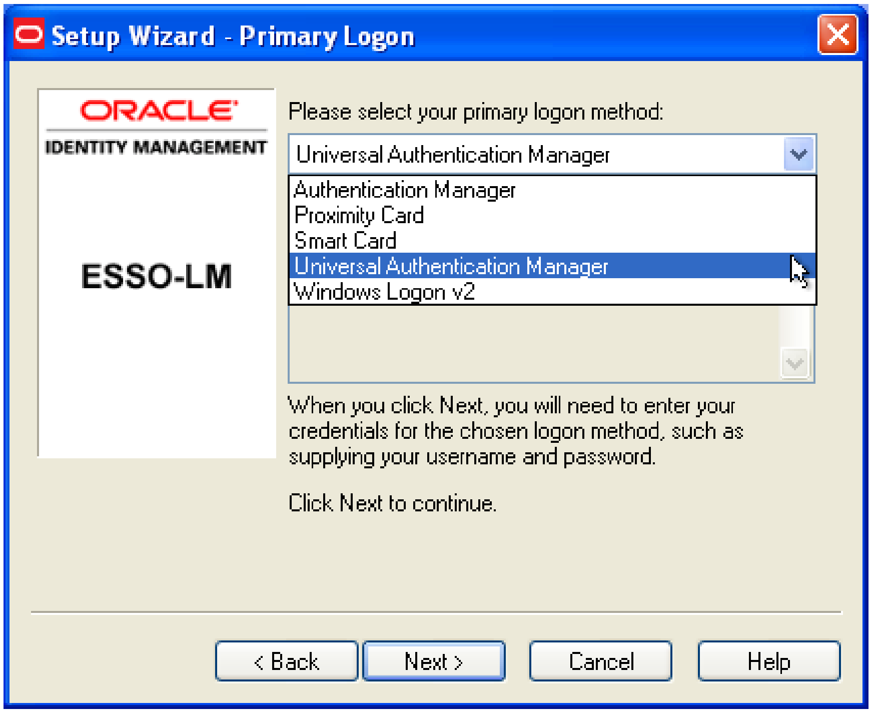
To set up ESSO-LM, you will need to:

1. Choose your primary method for logging into ESSO-LM.

2. Supply your credentials for this logon method.

Click Next to continue.

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

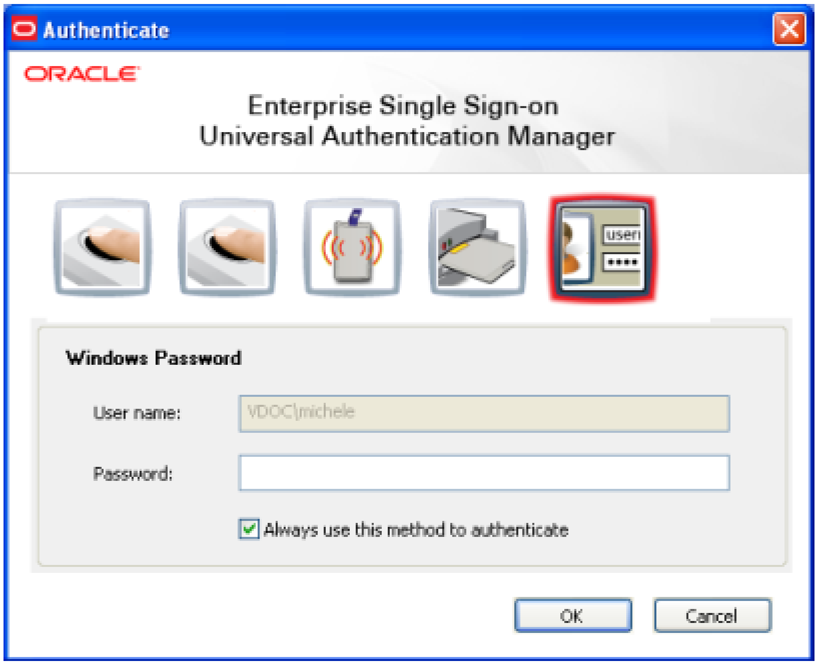


Please select your primary logon method: Universal Authentication Manager

When you click Next, you will need to enter your credentials for the chosen logon method, such as supplying your username and password.

Click Next to continue.

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



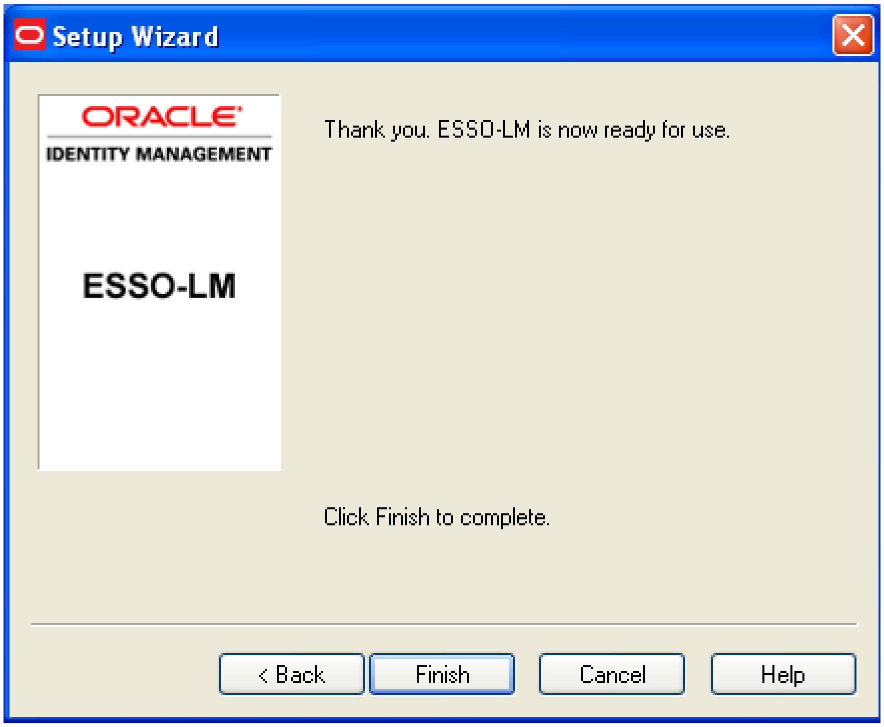
Windows Password

User name: VDOC\michele

Password:

☑ Always use this method to authenticate

5. ESSO-LM displays a message informing you that it is ready for use. ESSO-UAM is now configured as your primary logon method. Click **Finish** to complete the wizard.



Setup Wizard

ORACLE IDENTITY MANAGEMENT

ESSO-LM

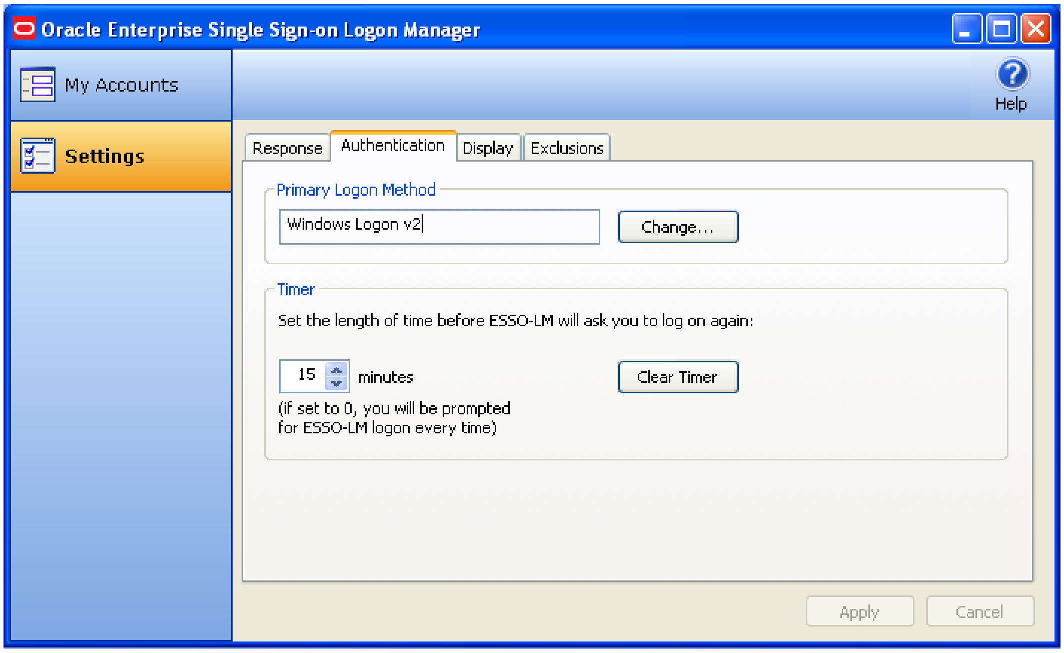
Thank you. ESSO-LM is now ready for use.

Click Finish to complete.

Configuring ESSO-UAM as the Primary Logon Method Using Logon Manager

To configure ESSO-UAM as the primary logon method for ESSO-LM:

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



Oracle Enterprise Single Sign-on Logon Manager

Primary Logon Method

Windows Logon v2

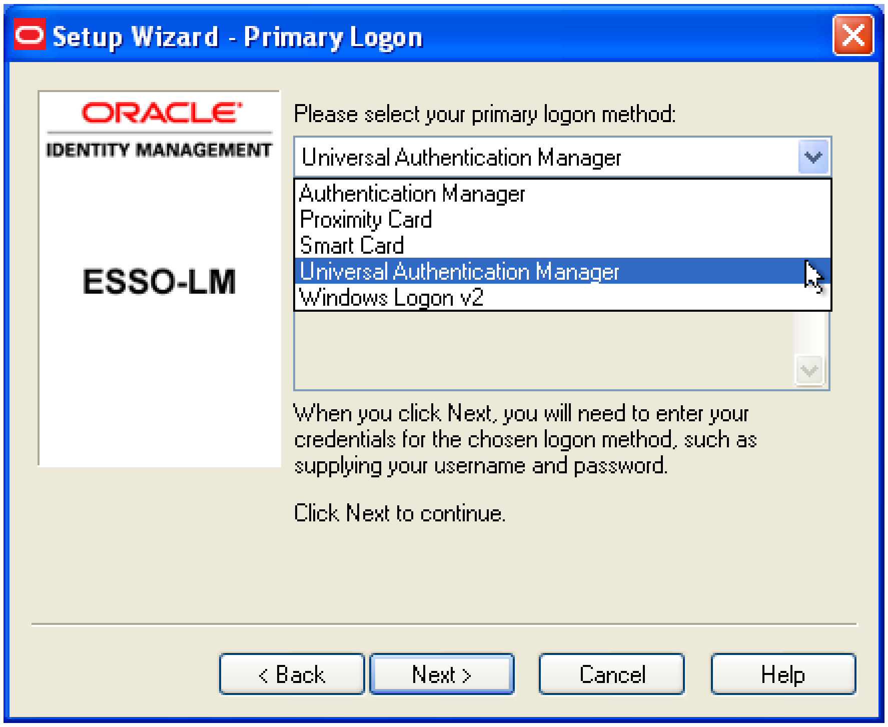
Timer

Set the length of time before ESSO-LM will ask you to log on again:

15 minutes

(if set to 0, you will be prompted for ESSO-LM logon every time)

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**.


Setup Wizard - Primary Logon
ORACLE
IDENTITY MANAGEMENT
ESSO-LM
Please select your primary logon method:
Universal Authentication Manager
Authentication Manager
Proximity Card
Smart Card
Universal Authentication Manager
Windows Logon v2
< Back
Next >
Cancel
Help

When you click Next, you will need to enter your credentials for the chosen logon method, such as supplying your username and password.

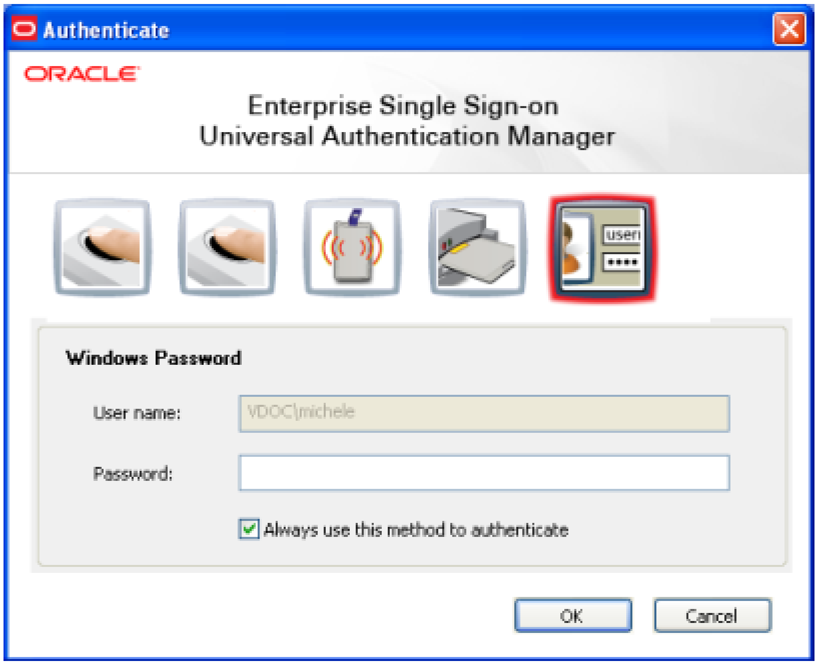
Click Next to continue.

6. The ESSO-UAM authentication dialog is displayed; enter your Windows password or authenticate to ESSO-UAM to enroll.

Authenticating With ESSO-UAM When Prompted by ESSO-LM

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

When authentication is required, you are prompted by the ESSO-UAM 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 ESSO-UAM. For example, if you last authenticated to ESSO-UAM with your Windows password, the screen will appear as follows:



Windows Password

User name: VDOC\michele

Password:

☑ Always use this method to authenticate

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