Oracle© EnterpriseSingle Sign-on Authentication Manager

Installation and Setup Guide

Release 11.1.1.2.0

E15706-02

November 2010

ORACLE®

Oracle Enterprise Single Sign-on Authentication Manager Installation and Setup Guide, Release 11.1.1.2.0

E15706-02

Table of Contents

Abbreviations and Terminology

Following is a list of commonly-used abbreviations and terminology.

Abbreviation or Terminology	Full Name
Administrative Console	ESSO-LM Administrative Console
Agent	ESSO-LM Manager
FTU	First Time Use Wizard
ESSO-AM	Oracle Enterprise Single Sign-on Authentication Manager
ESSO-PG	Oracle Enterprise Single Sign-on Provisioning Gateway
ESSO-KM	Oracle Enterprise Single Sign-on Kiosk Manager
ESSO-LM	Oracle Enterprise Single Sign-on
ESSO-PR	Oracle Enterprise Single Sign-on Password Reset

Oracle Enterprise Single Sign-on Authentication Manager versus Authentication Manager

"Oracle Enterprise Single Sign-on Authentication Manager" (ESSO-AM) the product and "Authentication Manager" the feature are two separate functionalities that are similar in name, but different in utility.

ESSO-AM is the product, which adds strong authenticator functionality to ESSO-LM.

Authentication Manager is a feature of ESSO-LM that adds the capability to enable multiple logon methods to authenticate the user. These logon methods can be the standard ESSO-LM supported logon methods such as LDAP and Windows Logon, or the ESSO-AM strong authenticators such as smart cards, proximity devices, and RSA SecurID tokens.

Authenticator versus Primary Logon Method

An authenticator is a plug-in module to ESSO-LM. The Primary Logon Method is the authenticator you have selected to use. You can have multiple installed authenticators but can only have one Primary Logon Method.

About ESSO-AM

ESSO-AM, an add-on module to Oracle Enterprise Single Sign-on (ESSO-LM), enables organizations to seamlessly bridge strong authentication to all of their applications, including smart cards and Entrust authenticators. Users can employ different authenticators at different times and application access can be controlled based upon the authenticator used.

See the *ESSO-AM Release Notes* for the most up-to-date list of supported authentication devices.

ESSO-AM provides authentication support from a variety of strong authenticators for all authentication events: initial authentication, re-authentication, and forced authentication.

Multiple authenticator support and graded authentication are features of ESSO-LM that extend their functionality to ESSO-AM installed authenticators. See the ESSO-LM documentation for more information on using these features with the ESSO-AM authenticators.

ESSO-AM files and components are installed directly into the ESSO-LM directory. A separate ESSO-AM directory does not exist. Because ESSO-AM is an add-on module to ESSO-LM, the ESSO-AM help is part of the ESSO-LM help file.

Installation Overview

ESSO-AM is installed as an add-on component to ESSO-LM, therefore ESSO-LM must be installed first. ESSO-LM automatically recognizes ESSO-AM once it is installed.

The following procedures must be completed in order to successfully install ESSO-AM:

1. Install ESSO-LM.
2. Install the ESSO-AM.
3. Optionally, configure settings in the ESSO-LM Administrative Console.
4. Adjust any applicable authenticator configuration settings. See the Authenticator Configuration Settings section of this document.

If upgrading from earlier versions of ESSO-AM, refer to the Upgrade Notes.

Inter-product Compatibility

ESSO-AM_11.1.1.2.0

- ESSO-LM version 11.1.1.2.0
- ESSO-KM version 11.1.1.2.0

Install ESSO-LM Agent and Administrative Console

The ESSO-LM Agent must be installed prior to installing ESSO-AM. The ESSO-LM Administrative Console should also be installed first. Refer to the *ESSO-LM Installation and Setup Guide* for instructions. See the Installation Overview for a list of supported versions.

If you want to use the Enrollment, Grade, and Order functionality of ESSO-LM for the ESSO-AM authenticators, the **Authentication Manager** feature must be installed.

If the ESSO-LM Agent is already installed, go to **Control Panel** > **Add/Remove Programs** > **ESSO-LM** and click **Change**. Modify the installation to install the **Authentication Manager**.

To use the SoftID helper included with ESSO-AM, Authentication Manager must be installed and selected as your primary logon method.

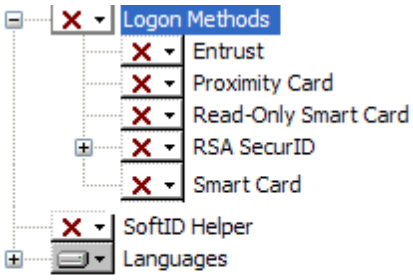
For more information, see the *ESSO-LM Installation and Setup Guide*.

Install ESSO-AM Agent

If you are upgrading from earlier versions of ESSO-AM, refer to the Upgrade Notes.

To install and configure the ESSO-AM Agent:

1. Close all programs.
2. Place the installation CD in your CD-ROM drive (or start the installation from a shared network drive).
3. In the \AM folder, double-click the setup file. Wait while the installer loads.
4. The **Welcome** dialog box opens. Click **Next**.
5. The Custom Setup dialog box prompts you to select the features to install. Select the ones you want by clicking the red [**x**] next to the feature and clicking **This feature will be installed on local hard drive**. See screen shot below.
6. When you have selected all necessary, click **Next**.
7. ESSO-AM is ready to be installed. Click **Install**.
8. When the installation is complete, click **Finish**.



ESSO-AM features include:

- **Logon Methods**: Choose the logon method by clicking the [+] next to **Logon Methods**. Entrust, Proximity Card, Read-Only Smart Card, RSA SecurID, and Smart Card logon methods are available. See the Authenticator Configuration Settings section in this document for instructions on adjusting any specific settings for your logon method to work with ESSO-AM.

- Click the [+] next to **RSA SecurID** to install support for **Local Authentication Toolkit (LAT)**. If you are installing RSA LAT, see the RSA SecurID configuration page.

- **SoftID Helper**: Select to install SoftID support. See the Configuring the SoftID Helper section for more information on using this feature.

- **Languages**: If you will be using localized language support to display ESSO-AM in other languages, click the [+] next to **Languages** and select the language pack.

Configure Settings in ESSO-LM

After ESSO-AM is installed, it automatically integrates with the ESSO-LM Agent and Administrative Console. Many ESSO-LM features extend their functionality to the ESSO-AM authenticators. These settings are described in this section.

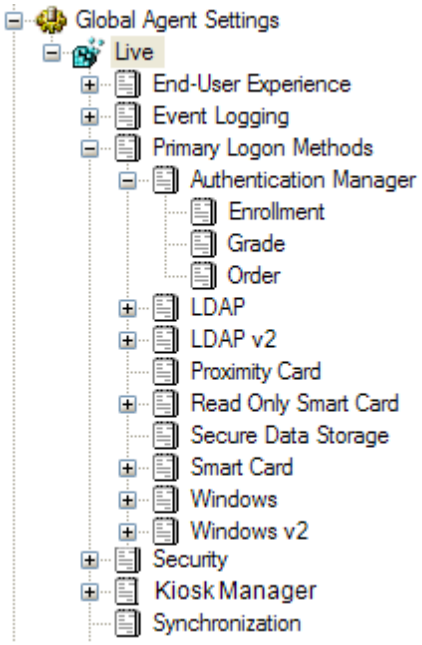
To configure these settings:

1. Click **Start** > **Programs** > **Oracle** > **ESSO-LM** > **ESSO-LM** Console. The Administrative Console opens.

2. Right-click the **Global Agent Settings** icon to display a shortcut menu, point to **Import** and click **From Live HKLM**.
3. After the list has been imported, expand **Live**, expand **Primary Logon Methods**, and then expand **Authentication Manager**.

4. There are three ESSO-LM features available to configure for ESSO-AM: Enrollment, Grade, and Order.

5. Configure the authenticator as needed.



A potential security problem exists with graded authentication and multiple primary logon methods.

If multiple authenticators are set up with different grades, a user with a lower grade authenticator has the ability to change his primary logon method from multiple authentication to single authentication, thereby giving himself access to logons that require higher grades.

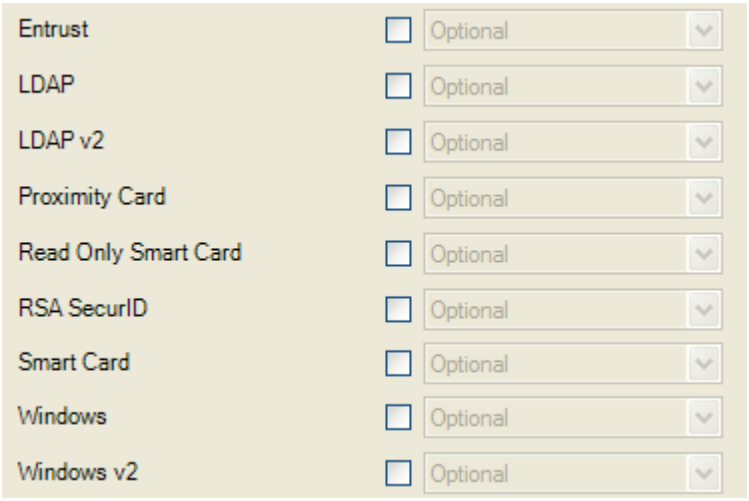
This potential issue can be avoided through settings in the ESSO-LM Administrative Console.

Expand **Global Agent Settings** > **Live** > **End User Experience** > **Setup Wizard**. Set the **Selected Primary Logon** (Registry Location: AUI: Selected) setting to **Authentication Manager**. As long as this is selected, the user can no longer change the primary logon method.

Configuring Authentication Manager: Enrollment

The enrollment settings allow the administrator to configure the primary logon methods to be used with the Authentication Manager.

To access the enrollment settings, click **Global Agent Settings** > **Live** > **Primary Logon Methods** > **Authentication Manager** > **Enrollment**.



The settings on this page determine whether a user will be required to set up a specific logon method during the First Time Use (FTU) Wizard, if Authentication Manager is chosen as the primary logon method.

For each primary logon method, the following options are available:

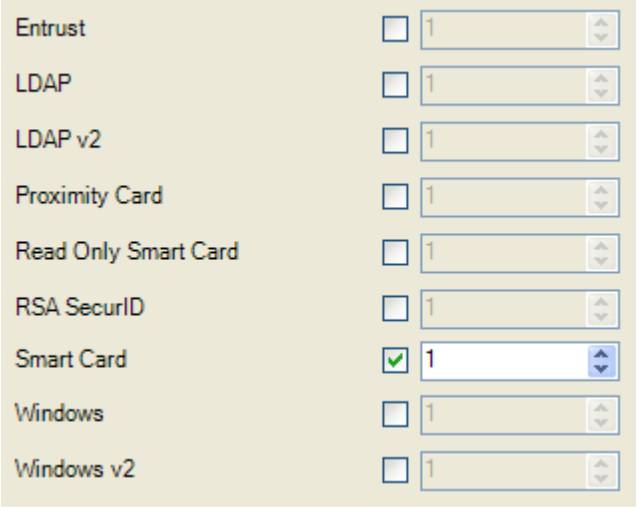
- **Optional**: User has the option to configure this logon, or to skip it. If the user defers the logon request, ESSO-LM will not ask again.
- **Incremental**: User has the option to configure this logon, or to skip it. If the user defers the logon request, ESSO-LM will ask for credentials each time the application starts.
- **Required**: User is required to configure this logon. If this logon is not configured, the user will not be able to complete enrollment.
- **Disabled**: This logon method is not presented to the user during the FTU wizard.

Configuring Authentication Manager: Grade

The grade settings specify an authentication grade for each primary logon method, if Authentication Manager is chosen as the primary logon method..

Set a number grade value (>=1) for each logon method.

To access the grade settings, click **Global Agent Settings** > **Live** > **Primary Logon Methods** > **Authentication Manager** > **Grade**.



Authentication Grades are numeric values. An authentication grade automatically defaults to grade level 1 if authentication grading is turned on and no grade level is specified. The higher the grade level specified, the stronger the authentication level that is being requested.

You can arbitrarily configure the grading scale. For example, an expected normal scenario would be a scale of 1 to 3, but you have the flexibility to make this 1 to 5 or 1 to n, as you require. To be consistent, any grade lower than 1 will be converted to 1.

ESSO-AM supports the authentication grades by mapping the grades to the authentication methods used.

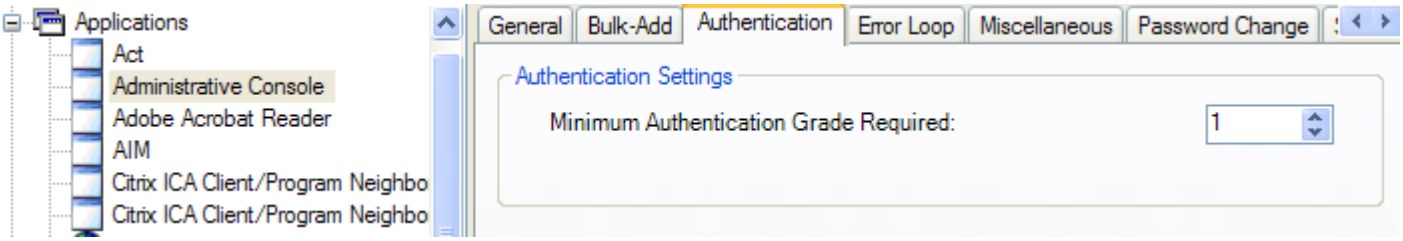
If a user tries to access credentials using an authenticator that is assigned a grade level that is too low, he or she will need to authenticate at a higher grade and only gain access if successful. If the user cannot authenticate at a higher grade they will not gain access.

To set the authenticator grade for specific applications, use the Authenticator Level Grade setting. This is located in the application configuration settings.

Configuring Application-Level Authentication Grades

Authentication Tab (for selected application)

To access the application-level settings, click **Applications** > *Select any application* > **Authentication**.



Use the Authentication tab to set the **Minimum Authentication Grade Required** for the selected application. The user's primary logon method used must have an Authentication Grade equal to or higher than this value in order for ESSO-LM to log the user on to the selected application. If the end user's primary logon method has an authentication grade lower than the minimum set for this application, access to the selected application will not be successful.

Select or type the numeric value of the lowest authentication grade that the end user's primary logon method can be. The default is 1.

Authentication Grades are numeric values. An authentication grade will automatically default to grade level 1 if authentication grading is turned on and no grade level is specified. The higher the grade level specified, the stronger the authentication level that is being requested.

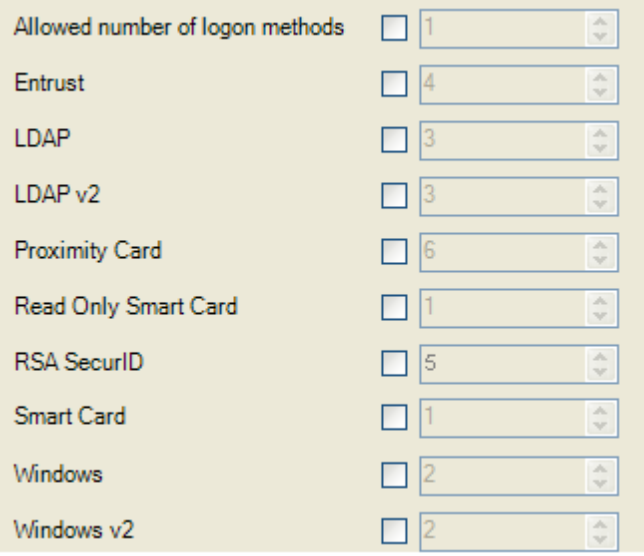
You can arbitrarily configure the grading scale. For example, an expected normal scenario would be a scale of 1 to 3, but you have the flexibility to make this 1 to 5 or 1 to n, as you require. To be consistent, any grade less than 1 will be converted to 1.

To set the authentication grade for primary logon methods, use the Authenticator Grade setting.

Configuring Authentication Manager: Order

The order settings specify the sequence that the installed logon methods will be presented to the end user during re-authentication scenarios, if Authentication Manager is chosen as the primary logon method.

To access the grade settings, click **Global Agent Settings** > **Live** > **Primary Logon Methods** > **Authentication Manager** > **Order**.



The **Allowed number of logon methods** setting allows you to set the maximum number of logon methods that will be presented to a user during authentication. After this number of logon methods has been presented, a **Choose Logon** dialog box opens. The user can then select their logon method from this dialog box.

For each primary logon method, select or type a number to indicate the logon method's position during a re-authentication scenario.

A "1" indicates the most preferred logon method.

Configuring the SoftID Helper

The SoftID Helper is an extension helper that adds SSO support for SecurID applications. This section describes how to install and configure the SoftID helper and enable RSA SecurID application templates.

Pre-requisites

ESSO-AM supports the following combinations of software and hardware tokens for SoftID applications:

- RSA SecurID Software Tokens
- RSA Authentication Client and RSA SecurID SID800 Hardware Authenticator
- Both software and hardware tokens - if both are installed on the machine, ESSO-AM looks for the hardware token first, and if it cannot find the hardware token, it defaults to the software token.

One of the above combinations must be installed before installing and using the SoftID Helper.

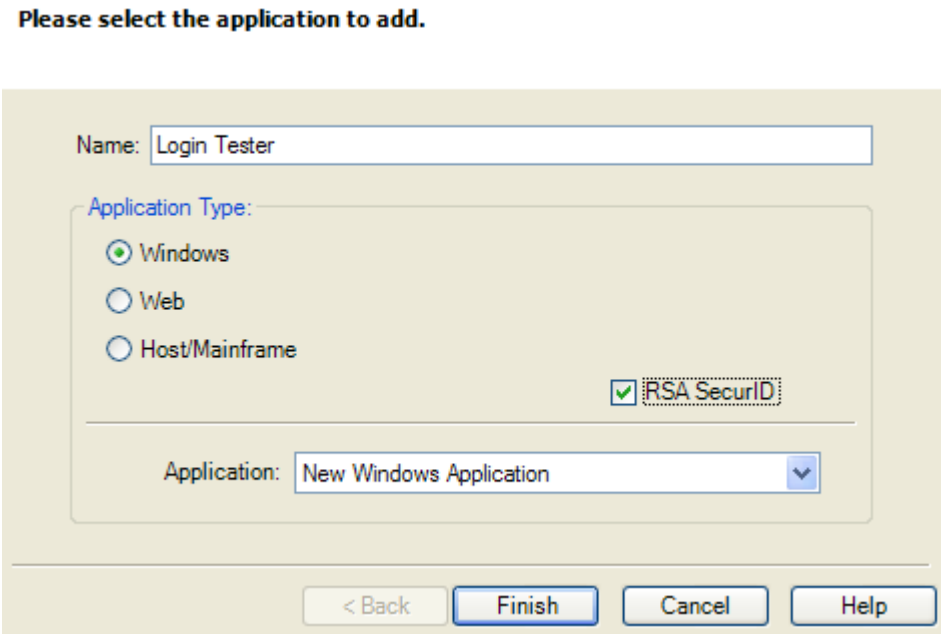
Install ESSO-LM and ESSO-AM

Install ESSO-LM with Authentication Manager and ESSO-AM with the SoftID helper. See each installation section for more information.

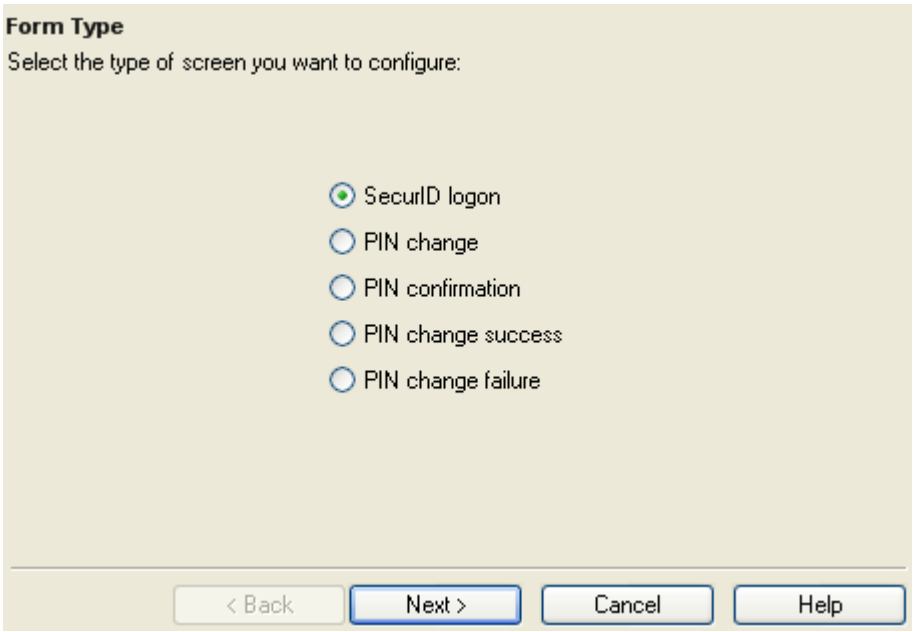
Configuring RSA SecurID Application Templates

This example walks through setting up a new RSA SecurID application for an application called Login Tester.

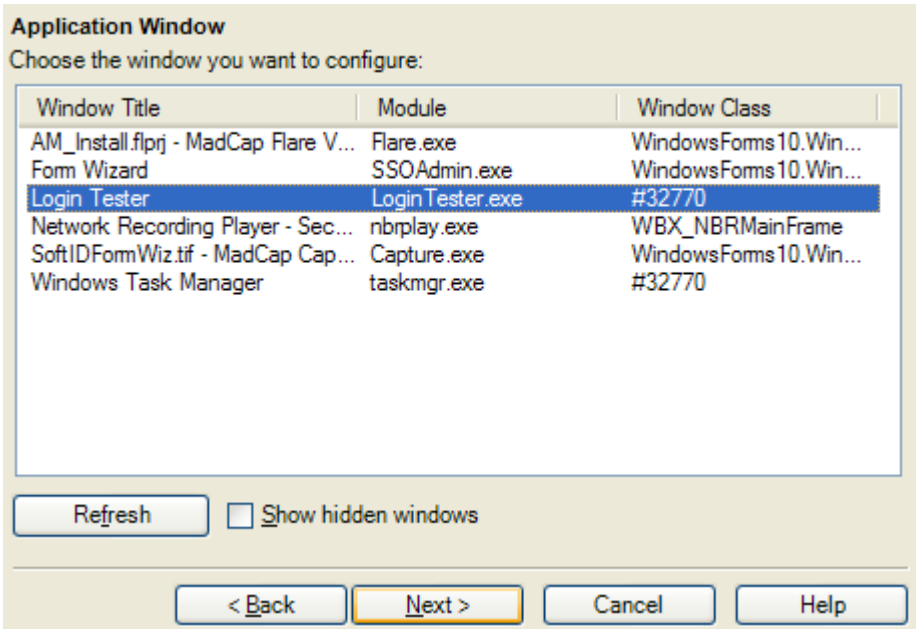
1. Open the ESSO-LM Administrative Console.
2. Open the Login Tester application logon screen.
3. Right-click **Applications** and select **New Windows Application**. The Add Application dialog appears.



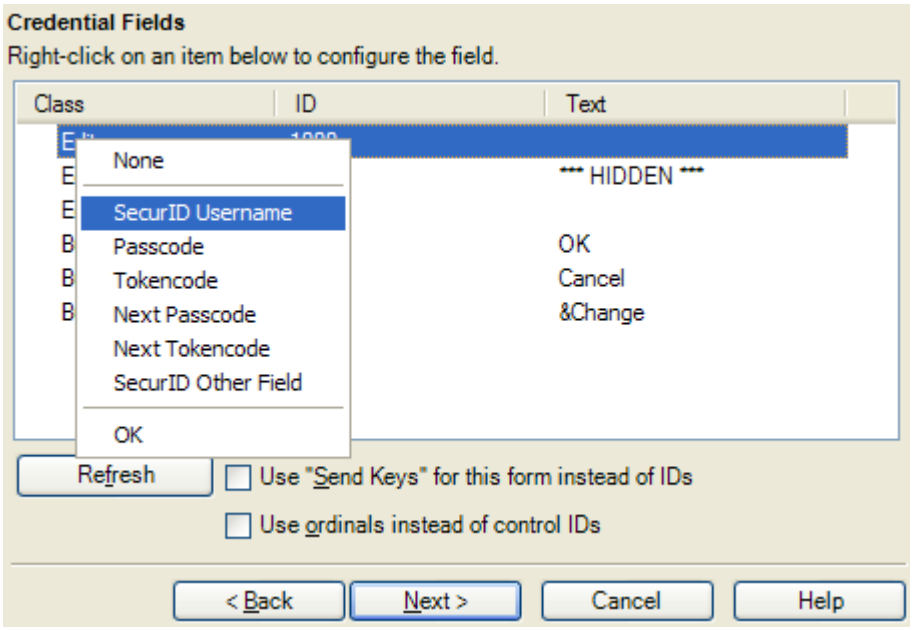
4. Enter the application **Name** and check the **RSA SecurID** check box. Click **Finish.** The Form Wizard appears.



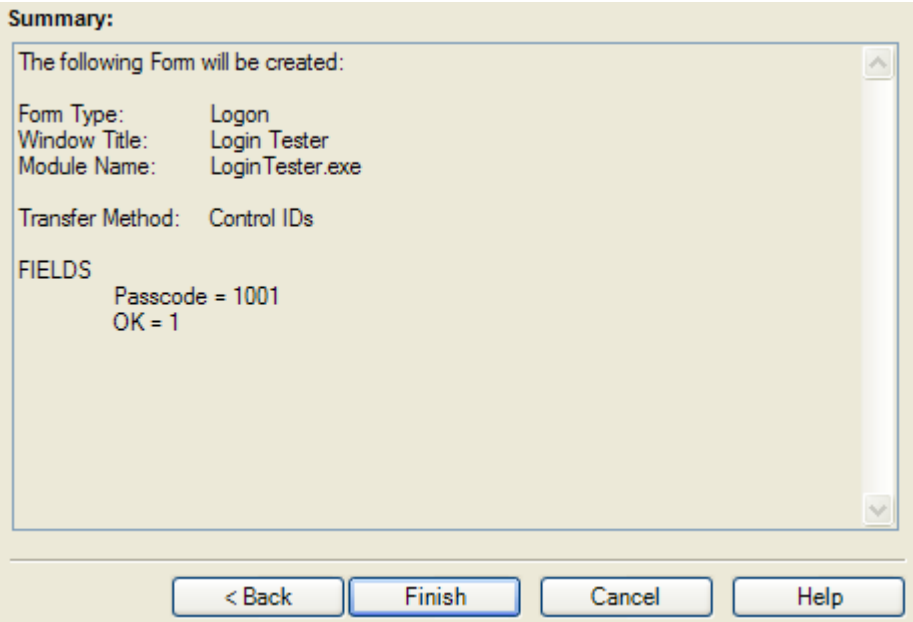
5. Select the **SecurID Login** button. Click **Next**. As long as the Login Tester application is open, the window title will appear in the next wizard panel.



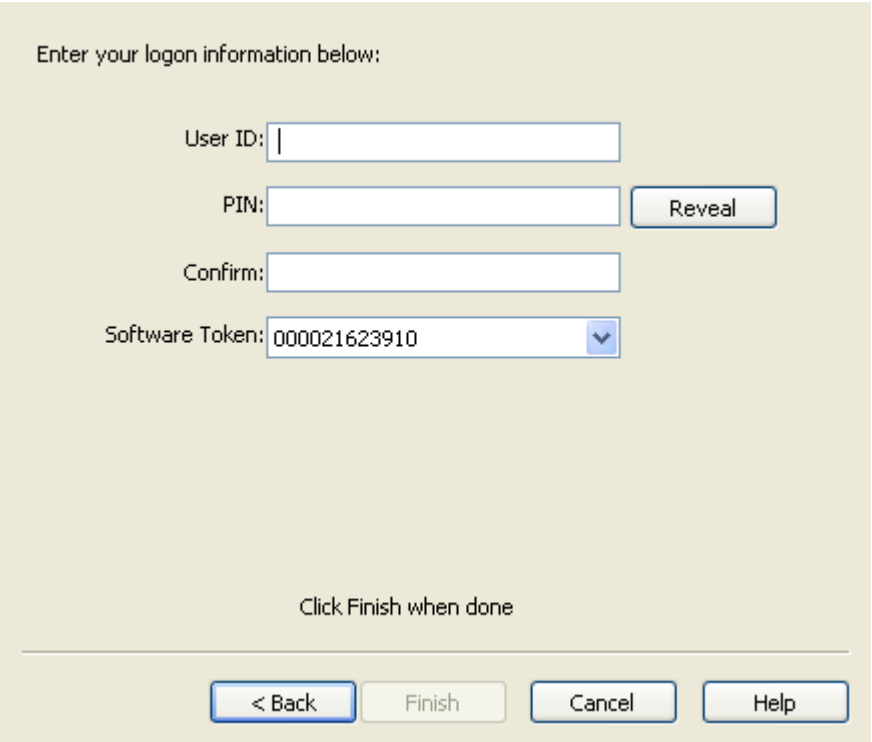
6. Select the Login Tester application Window title. Click **Next**.



7. On this dialog, you configure the **SecurID Username**, **Passcode**, and **OK** button fields as well as any other applicable fields for your application. Right-click on the class and select the fields. Click the **Help** button for more information on configuring the credential fields. Click **Next** when you are done. A Summary panel will appear.



8. Review the summary. Click **Finish** when done.
9. The Windows Logon Form appears. Change any other applicable settings and click **OK**.
10. Export the template to the Agent. See the ESSO-LM Administrative Console help file for more information on exporting applications.
11. When the Agent is started, the user will go through the FTU Wizard. They must select **Authentication Manager** as the primary logon method.
12. When the Login Tester application is started, the Agent will first ask the user if they want to add credentials for the application. If the user selects **Yes**, the Agent will prompt the user to enter their credentials into the New Logon for Login Tester dialog.



13. The user must enter the **User ID**, **PIN** and select the **Software Token**. The user's PIN is set up through the RSA middleware prior to use with ESSO-AM. ESSO-AM automatically populates the Software Token field as it detects the serial number of the available token.

14. Click **Finish** when done. The Agent will log the user onto the RSA SecurID application every time the application is started.

Authenticator Configuration Settings

This section lists any specific settings that can be enabled within an authenticator in order for the authenticator to work with ESSO-AM. It also describes all the ESSO-LM Administrative Console settings and any steps that must be taken to integrate with ESSO-KM. This section also lists any known issue or technical notes that apply to the specific authenticator.

If the authenticator you are using is not listed in this section, there are no specific settings that must be adjusted or relevant technical notes.

Select your authenticator, or view the ESSO-KM integration notes which apply to all authenticators:

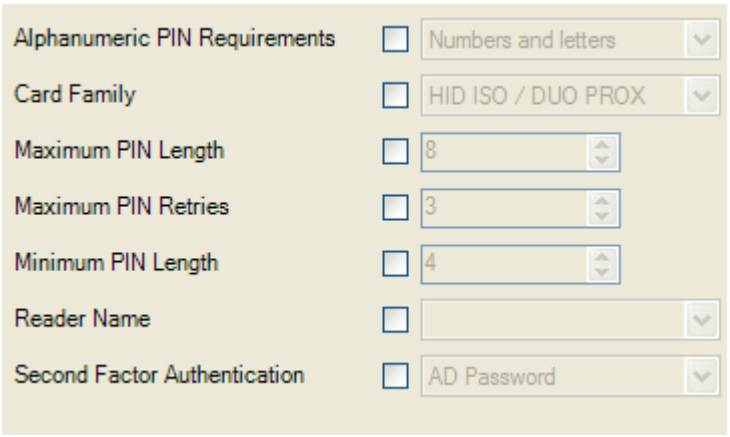
- Proximity Card
- Read Only Smart Card
- RSA SecurID
- Secure Data Storage
- Smart Card
- ESSO-KM Integration Notes

Proximity Card

If you are using Proximity Cards, advanced settings are available in the ESSO-LM Administrative Console. There are also steps that need to be taken when using Active Directory or Active Directory Application Mode (ADAM) and other technical notes about configuring and using this authenticator.

Administrative Console Settings

To access the proximity card settings, click **Global Agent Settings** > **Live** > **Primary Logon Methods** > **Proximity Card**.



Alphanumeric PIN Requirements	Configures the alphanumeric requirements of the user defined PIN. **Options:** • Numbers and letters (default) • Letters only • Numbers only
Card Family	The proximity card family type. **Options:** • HID ISO/DUO PROX (default) • iClass • Indala/EM
Maximum PIN Length	Configures the maximum length of the user defined PIN. Default is 8.
Maximum PIN Retries	Configures the number of correct PIN attempts before the authentication fails. Default is 3.
Minimum PIN Length	Configures the minimum length of the user defined PIN. Default is 4.
Reader Name	The name of the proximity card reader to use. **Options:** • Omnikey CardMan 5125 • Omnikey CardMan 5121 • Omnikey CardMan 5321 • RFIdeas
Second Factor Authentication	Configures whether to use the Active Directory Password or a user defined PIN for the second factor in authentication.

	Options: • AD Password (default) • User defined PIN  If User defined PIN is selected, and ESSO-KM is being used, Secure Data Storage must be enabled and configured in order for this setting to work.

Integrating with ESSO-KM

Support for storing and passing through the synchronization credentials with ESSO-KM and Proximity Card integration:

When the Proximity Card authenticator's second factor is set to "User Defined PIN", the user's synchronization credentials can optionally be stored by the authenticator by configuring the Secure Data Storage feature. If stored in this manner, the credentials are then silently passed through to ESSO-LM after a user initiates a ESSO-KM session by tapping their proximity card and entering the correct PIN. This feature prevents a double authentication when starting a ESSO-KM session whereby the user authenticates with their proximity card and PIN and then is subsequently prompted by ESSO-LM to provide their synchronization username and password.

Insufficient privileges for Guest User Accounts

Guest User accounts do not have sufficient privileges to perform operations required for successfully completing the ESSO-LM First Time Use wizard. Oracle recommends against using Guest Accounts as the kiosk account.

Active Directory Technical Notes

An Active Directory administrator must perform the following steps on the "CN=Users" container on the AD controller to grant read/write access to the Creator Owner user.

If the steps are not administered, users will not have sufficient rights to change their proximity card number. As a result, when a user enters the passphrase scenario to update their card information (lost card scenario), they get an error "Proximity card assigning failed."

1. Open Active Directory Users and Computers console on AD controller.
2. Right-click on the **Users** AD object (CN=Users).
3. Click **Properties** in pop-up menu.
4. Click the **Security** tab.
5. Click the **Add** button.
6. Under **Enter the object names to select**, type CREATOR OWNER.
7. Click the **Check Names** button to resolve the entry.
8. Click **OK**.
9. Under **Group or user names**: highlight **CREATOR OWNER**.
10. Click the **Advanced** button.
11. The Advanced Security Settings for Users window displays. Verify that **Allow inheritable permissions from the parent to propagate to this object and ...** checkbox is checked (set to TRUE).
12. Double-click the **CREATOR OWNER** user.
13. Set **Apply Onto** dropdown to **Child Objects** only.
14. Set the **Read All Properties** and **Write All Properties** checkboxes under **Allow** to checked (set to TRUE).
15. Apply all changes.

To use the proximity card authenticator with Active Directory, you must enable the storing of credentials under user objects:

1. Open the ESSO-LM Administrative Console.
2. Connect to the repository.
3. From the **Repository** menu, select **Enable Storing Credentials under User Objects** (AD only).

ADAM Technical Notes

An ADAM administrator must perform the following steps on the "OU=People" container on the ADAM server to grant read/write access to the users.

1. Open ADAM Tools Command Prompt on ADAM server.
2. Execute the following command to give users 'Read' permission to the **People** container and its sub objects:

```
dsacls.exe \\<hostname>:<port>\<adam container dn> /I:T /G <user/group/role DN>:GR
```

3. Execute the following command to give users 'Create Child' and 'Write Self' permissions to the **People** container and its sub objects:

```
dsacls.exe \\<hostname>:<port>\<adam container dn> /I:T /G <user/group/role
DN>:CCWS
```

OmniKey Proximity Card Reader Technical Note

When using the OmniKey family proximity card readers, it is recommended that the driver be installed through Windows updates.

Microsoft Visual C++ Technical Notes

Microsoft Visual C++ 2005 Redistributable Package (x86) is required for the Proximity Card authenticator. This can be downloaded from Microsoft's web site - http://www.microsoft.com/Downloads/details.aspx?FamilyID=32bc1bee-a3f9-4c13-9c99-220b62a191ee&displaylang=en.

Read-Only Smart Card

If you are using Read-Only Smart Cards, advanced settings are available in the ESSO-LM Administrative Console. There are also steps that need to be taken if integrating with ESSO-KM.

Administrative Console Settings

The read-only smart card settings control special-case options for read-only smart card authentication. These settings are not required.

To access the smart card settings, click **Global Agent Settings** > **Live** > **Primary Logon Methods** > **Read Only Smart Card** > **Advanced**.

Lock ESSO-KM on session removal	This setting configures whether ESSO-KM will lock a session when the session owner removes the smart card from the smart card reader. By default, this value is set to lock. If set to not lock, the ESSO-KM session will remain open when the smart card is removed. This setting is useful in a scenario where employees must have their smart cards displayed at all times, and therefore cannot leave it in a reader.
Passphrase	Enables the passphrase challenge for additional security. The passphrase can be supplied either by the user entering the passphrase in a dialog box (the default setting) or by the newest non-default encryption certificate on the card itself. The default setting requires users to provide a passphrase answer during First Time Use. Options: • Disable • Enable using a dialog box (default) • Enable using the card's certificate
PKCS#11 Library Path	Use this setting to configure the path to the smart card middleware file which implements the PKCS#11 standard. For sample paths, see the Smart Card Middleware Default Library Path Locations section later in this document. This entry is only required if smart cards are being used with ESSO-KM.
Reset Certificate Object Identifier	This is an optional setting. By default, the authenticator selects the most recent valid encryption certificate found on the card for the certificate-based passphrase feature. Use this setting to configure the object identifier that identifies the specific certificate to use for the passphrase feature. The authenticator searches the "Enhanced Key Usage" attribute of each certificate on the smart card for this Object Identifier. The **Passphrase** option must be set to **Enable using the card's certificate**.
Store Synchronization Credentials	Configure whether to store the user's synchronization repository credentials using Secure Data Storage. This setting should only be enabled when using Read-Only Smart Cards with ESSO-KM.

	Secure Data Storage must be enabled and configured in order for this setting to work. Options: • Do not store credentials (default) • Store credentials

Smart Card Initialization

Prior to use with ESSO-AM, read-only smart cards must be initialized and contain a valid PIN and PKI certificate. If the smart cards are also to be used with ESSO-KM, they must have a serial number.

ESSO-AM does not provide any smart card initialization, configuration, or administration services, so this step must be performed using a third-party Card Management System (CMS) or middleware administration utility compatible with your smart card.

Integrating with ESSO-KM

Support for storing and passing through the synchronization credentials with ESSO-KM and Read-Only Smart Card integration:

When using Read-Only Smart Card authenticator with ESSO-KM, the user's synchronization credentials can optionally be stored by setting **Store Synchronization Credentials** to **Store Credentials** and configuring the Secure Data Storage feature. If stored in this manner, the credentials are then silently passed through to ESSO-LM after a user initiates a ESSO-KM session by inserting their read-only smart card into the reader and entering the correct PIN. This feature prevents a double authentication when starting a ESSO-KM session whereby the user authenticates with their read-only smart card and PIN and then is subsequently prompted by ESSO-LM to provide their synchronization username and password.

Separate Authentication Prompts Appear for the ESSO-KM Session and ESSO-LM when Read-Only Smart Card is the Primary Logon Method:

In a ESSO-KM environment that uses read-only smart cards as the primary logon method, users are prompted to authenticate separately to ESSO-KM and ESSO-LM.

This occurs because a smart card authentication is only valid for the process that initiated it and cannot be shared between processes. This is a design characteristic of the smart card middleware and not Oracle software.

When the ESSO-KM session starts, ESSO-KM queries the smart card middleware for authentication and the user is prompted to authenticate via smart card and PIN. This authentication is valid for the ESSO-KM process only; therefore, when the ESSO-KM session is successfully created and ESSO-LM starts, the user is authenticated again, this time to ESSO-LM.

There is currently no workaround for this behavior.

RSA SecurID

If you are using RSA SecurID authenticator, there are steps that need to be taken if integrating with ESSO-KM and other technical notes about installing and using this authenticator.

Installing the RSA SecurID Method

Before installing the RSA SecurID authentication method, the RSA middleware must be installed and configured. There are two middleware options for the RSA SecurID authenticator:

- **RSA Local Authentication Client (LAC)** - if using RSA LAC, you must install the **RSA SecurID** Logon Method in the ESSO-AM installer.
- **RSA Local Authentication Toolkit (LAT)**- if using RSA LAT, you must install the **RSA SecurID** Logon Method as well as the **Local Authentication Toolkit**, if not previously installed, in the ESSO-AM installer. Installing RSA LAT will prompt you to reboot your machine so that it can start the service.

  After RSA LAT is installed, according to the RSA documentation on LAT, you must perform the following 2 steps:

1. You must get the `server.cer` file from your RSA Authentication Manager administrator and place it in the subdirectory of the main installation directory. For example: C:\Program Files\RSA Security\RSA Authentication Agent\Agenthost Autoreg Utility directory.
2. You must get the `sdconf.rec` file from your Authentication Manager administrator and place it in the system32 directory.

These notes are stated in RSA SecurID Local Authentication Toolkit document and also mentioned in *RSA Authentication Agent 6.1 for Microsoft Windows Installation and Administration Guide*.

Once RSA SecurID is installed, there are no specific settings that must be set in the ESSO-LM Administrative Console.

Integrating with ESSO-KM

When using the RSA SecurID authenticator with ESSO-KM,you have to enable and configure Secure Data Storage in the ESSO-LM Administrative Console.

RSA SecurID authenticator uses the user's PIN rather than the repository password for the prepopulation of the synchronization dialog. Secure Data Storage is used to securely save the PIN which then is associated with the repository credentials on the server. See the Secure Data Storage section below to set it up.

If using a version 6.x of ESSO-KM, you must also do the following:

1. Open the ESSO-LM Administrative Console.
2. Navigate to **Global Agent Settings** > **Kiosk Manager**. Set **Prepopulate on startup** to **Always Prepopulate**. Enabling this setting to **Always Prepopulate** ensures that the RSA SecurID authentication dialog appears rather than the repository synchronization dialog.

Support for storing and passing through the synchronization credentials with ESSO-KM and RSA SecurID integration:

When using RSA SecurID authenticator with ESSO-KM, the user's synchronization credentials can optionally be stored by the authenticator by configuring the Secure Data Storage feature. If stored in this manner, the credentials are then silently passed through to ESSO-LM after a user initiates a ESSO-KM session with a RSA SecurID token. This feature prevents a double authentication when starting a ESSO-KM session whereby the user authenticates with their PIN and Tokencode and then is subsequently prompted by ESSO-LM to provide their synchronization username and password.

Microsoft Visual C++ Technical Note

Microsoft Visual C++ 2005 Redistributable Package (x86) is required for the RSA SecurID authenticator. This can be downloaded from Microsoft's web site - http://www.microsoft.com/Downloads/details.aspx?FamilyID=32bc1bee-a3f9-4c13-9c99-220b62a191ee&displaylang=en.

PIN Mode Support Technical Note

Due to an incompatibility between RSA Local Authentication Toolkit and Visual Studio 2005, the RSA SecurID authenticator does not support New PIN Mode for SID700 and SID800. A support case has been opened with RSA (# C0842539).

Secure Data Storage

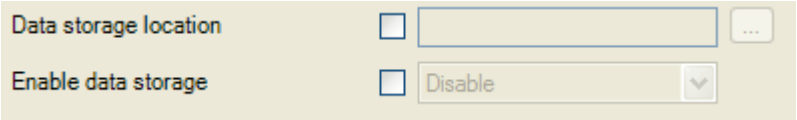
Secure data storage settings control the location for data storage. Secure data storage can be used for:

- The RSA SecurID authenticator in a ESSO-KM environment.
- The Proximity Card authenticator in a ESSO-KM environment when using "User Defined PIN" as second factor authentication.
- The Read-Only Smart Card authenticator in a ESSO-KM environment.

> Secure Data Storage is supported in Active Directory and Active Directory Application Mode only.

When using Secure Data Storage, you must log onto Windows using a domain user account.

To access the secure data storage settings, click **Global Agent Settings** > **Live** > **Primary Logon Methods** > **Secure Data Storage**.



Data storage location	Fully qualified path to the location in the repository where the data will be stored. Click the … to enter the location.
Enable data storage	Configures whether to securely store users synchronization credentials within the repository. Options: • Disable (default) • Enable

To enable secure data storage, perform the following:

1. Set **Enable Data Storage** to **Enable**.
2. Create a new Organizational Unit on the AD or ADAM repository that will serve as the location for data storage. The fully qualified distinguished name for this object should then be specified as the value of the **Data storage location** setting.
3. If using AD, grant FULL CONTROL permission to this Organizational Unit for Everyone. Apply this to **This object and all child objects**. For ADAM, grant General Access (GA) permission to this Organizational Unit and its sub objects for Everyone.
   `dsacls.exe \\<hostname>:<port>\<adam container dn> /I:T /G "Every-one":GA`

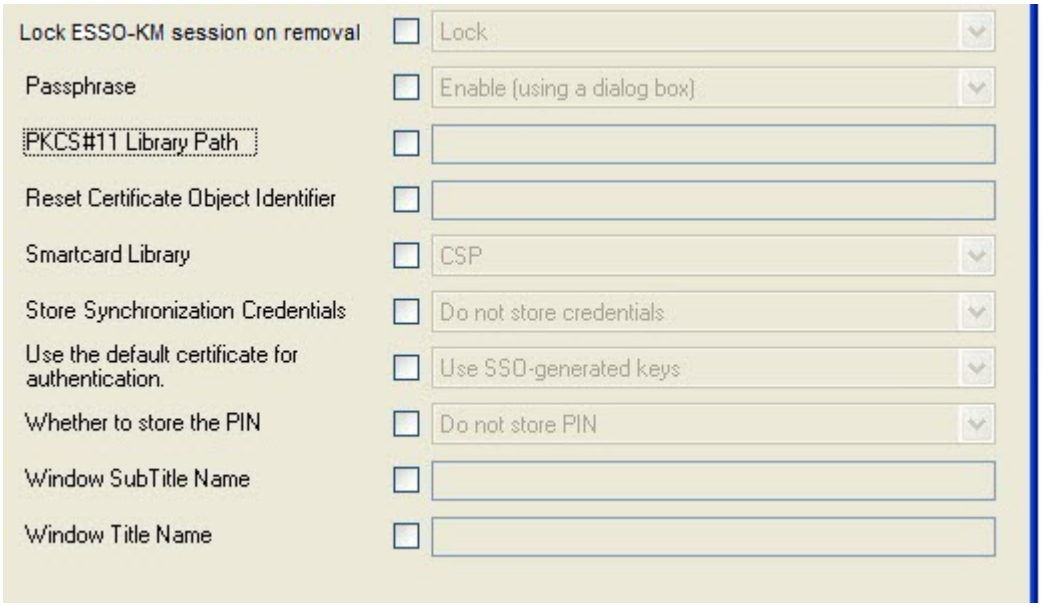
Smart Card

If you are using Smart Cards, advanced settings are available in the ESSO-LM Administrative Console. There are also steps that need to be taken if integrating with ESSO-KM and other technical notes about using this authenticator.

Administrative Console Settings

The smart card settings control special-case options for smart-card authentication. These settings are not required.

To access the smart card settings, click **Global Agent Settings** > **Live** > **Primary Logon Methods** > **Smart Card** > **Advanced**.



Lock ESSO-KM on session removal	This setting configures whether ESSO-KM will lock a session when the session owner removes the smart card from the smart card reader. By default, this value is set to lock. If set to not lock, the ESSO-KM session will remain open when the smart card is removed. This setting is useful in a scenario where employees must have their smart cards displayed at all times, and therefore cannot leave it in a reader.
Passphrase	Enables the passphrase challenge for additional security. The passphrase can be supplied either by the user entering the passphrase in a dialog box (the default setting) or by the newest non-default encryption certificate on the card itself. The default setting requires users to provide a passphrase answer during First Time Use. Options: • Disable • Enable using a dialog box (default) • Enable using the card's certificate
PKCS#11 Library Path	Use this setting to configure the path to the smart card middleware file which implements the PKCS#11 standard. For sample paths, see the Smart Card Middleware Default Library Path Locations section below. This entry is only required if the **Smartcard Library** setting below is set to **PKCS#11**, or if smart cards are being used with ESSO-KM.

Reset Certificate Object Identifier	This is an optional setting. By default, the authenticator selects the most recent valid encryption certificate found on the card for the certificate-based passphrase feature. Use this setting to configure the object identifier that identifies the specific certificate to use for the passphrase feature. The authenticator searches the "Enhanced Key Usage" attribute of each certificate on the smart card for this Object Identifier.  The **Passphrase** option must be set to **Enable using the card's certificate**.
Smart Card Library	Configures whether to use the Cryptographic Service Provider (CSP) or the PKCS #11 library to perform cryptographic operations on the smart card. If you set this to PKCS # 11, you must enter the library path above in the PKCS #11 Library Path. Options: • CSP • PKCS # 11  Only set this to PKCS #11 if using SafeSign/RaakSign middleware.
Store Synchronization Credentials	Configure whether to store the user's synchronization repository credentials on the card.  Set to **Store Credentials** if integrating with ESSO-KM. Options: • Do not store credentials (default) • Store credentials
Use the default certificate for authentication	Use the default logon certificate (provided by the administrator) on the card for authentication. If not enabled (the default), use (and create if necessary) the public or private keys in the SSO container on the card. Options: • Use SSO-generated keys (default) • Use the default logon certificate
Whether to store the PIN	Whether to store the smart card PIN (and thus the Agent prompts for the PIN) or to require that the smart-card drivers request the PIN. Options: • Do not store PIN (default) • Store PIN
Windows Title Name	Use this setting to customize the Window subtitle name for this authenticator. This entry is not required.
Windows Subtitle Name	Use this setting to customize the Window title name for this authenticator. This entry is not required.

Smart Card Initialization

Prior to use with ESSO-AM, smart cards must be initialized and contain a valid PIN. If ESSO-AM is configured to use smart card certificates, smart cards must contain a valid PKI certificate. If the smart cards are also to be used with ESSO-KM, they must have a serial number.

ESSO-AM does not provide any smart card initialization, configuration, or administration services, so this step must be performed using a third-party Card Management System (CMS) or middleware administration utility compatible with your smart card.

Integrating with ESSO-KM

The following information applies when using the Smart Card authenticator with ESSO-KM:

Support for storing and passing through the synchronization credentials with ESSO-KM and Smart Card integration: When using Smart Card authenticator with ESSO-KM, the user's synchronization credentials can optionally be stored on the smart card by the authenticator. If stored in this manner, the credentials are then silently passed through to ESSO-LM after a user initiates a ESSO-KM session by inserting their smart card into the reader and entering the correct PIN. This feature prevents a double authentication when starting a ESSO-KM session whereby the user authenticates with their smart card and PIN and then is subsequently prompted by ESSO-LM to provide their synchronization username and password.

.NET Smart Cards

Due to technical limitations with the .NET cards, when using .NET smart cards with ESSO-KM, inserting the smart card when ESSO-KM is locked always causes a new session to start. To unlock an existing session, click the **Unlock Existing Session** link.

Separate Authentication Prompts Appear for the ESSO-KM Session and ESSO-LM when Smart Card is the Primary Logon Method:

In a ESSO-KM environment that uses smart cards as the primary logon method, users are prompted to authenticate separately to ESSO-KM and ESSO-LM.

This occurs because a smart card authentication is only valid for the process that initiated it and cannot be shared between processes. This is a design characteristic of the smart card middleware and not Oracle software.

When the ESSO-KM session starts, ESSO-KM queries the smart card middleware for authentication and the user is prompted to authenticate via smart card and PIN. This authentication is valid for the ESSO-KM process only; therefore, when the ESSO-KM session is successfully created and ESSO-LM starts, the user is authenticated again, this time to ESSO-LM.

There is currently no workaround for this behavior.

HID Crescendo C200 and C700 smart cards

When using HID Crescendo C200 or C700 as smart cards with ESSO-KM, a smart card-only reader should be used. Using a dual function smart card and proximity card reader is unsupported. The HID Crescendo C200 mini-driver should be installed from Microsoft's update catalog - http://test.catalog.update.microsoft.com/v7/site/search.aspx?q=umdf.

Using SSO-generated Keys Technical Note

When the **Use default certificate for authentication configuration option** (located in the ESSO-LM Administrative Console **Global Agent Settings** > **Primary Logon Methods** > **Smart Card** > **Advanced**) is set to **Use SSO-generated keys**, users may be prompted to enter their PIN twice during the First Time Use (FTU) enrollment process.

This is normal and necessary in order to create the SSO keyset.

Subsequent authentications after FTU only prompt the user to enter their PIN once.

Smart Card Middleware

These technical notes are in reference to known issues and considerations with Smart Card middleware.

Gemplus Libraries 4.20 with ESSO-AM

Re-authentication events do not display the PIN dialog. When authenticating to ESSO-LM, the first authentication properly displays a PIN dialog and allows a successful authentication. Subsequent re-authentication events within a short period of time do not display the PIN dialog, preventing authentication from succeeding.

To work around this, restart the ESSO-LM process requesting authentication.

Netmaker Net iD 4.6 with ESSO-KM

When starting a new ESSO-KM session, the user's synchronization credentials are not read off the card. After entering their PIN, users must then manually enter their synchronization credentials to start the session.

RSA RAC 2.0 / Smartcard Middleware 2.0 with ESSO-KM

RSA Middleware reports that no smart cards are present when ESSO-KM is locked and a smart card is inserted into a reader. Sessions must be manually started. After ESSO-KM is unlocked, authentication to ESSO-LM with smart cards will work as expected.

Smart Card Middleware Default Library Path Locations

The following table provides the default installation paths for all supported smart card middleware. These are sample paths to enter in the PKCS #11 Library Path field located on the **Read Only Smart Card** > **Advanced** and **Smart Card** > **Advanced** panels:

Smart Card

RSA Authentication Client 2.0 / Smartcard Middleware 2.0	C:\Program Files\RSA Security\RSA Authentication Client\Pkcs11.dll
NetMaker Net iD 4.6	iidp11.dll
SafeSign/RaakSign Standard 2.3	aetpkss1.dll
HID C700 middleware	aetpkss1.dll
GemSafe Libraries 4.2.0	C:\Program Files\Gemplus\GemSafe Libraries\BIN\GCLIB.DLL
Schlumberger Cyberflex Access 4.5	C:\Program Files\Schlumberger\Smart Cards and Terminals\Cyberflex Access Kits\v4\slbCk.dll
Axalto Access Client Software 5.2	C:\Program Files\Axalto\Access Client\v5\xltCk.dll

Read-Only Smart Card

SafeSign Identity Client 2.2.0	aetpkss1.dll
Fujitsu mPollux DigiSign Client 1.3.2-34(1671)	C:\Program Files\Fujitsu Services\Fujitsu mPollux DigiSign Client\Cryptoki.dll

The files above that are just file names and not the fully qualified path reside in the system directory so the full path is not necessary.

Oracle Enterprise Single Sign-on Kiosk Manager Integration Notes

Domain Password Change

This issue occurs when using proximity devices, smart cards, and read only smart cards.

If user's domain password is changed, the next time the user tries to start a session on a kiosk with the device within the lifetime period of the old password, depending on their sync repository, the following occurs:

- **Active Directory:** An error message displays saying "Unable to connect to network ...".
- **ADAM:** ESSO-KM stops responding and requires a restart.

There are 2 workarounds to this issue:

1. Users can manually start a ESSO-KM session by authenticating with a username and new password within the password lifetime period.
2. Administrators can change the lifetime period of an old password to decrease the probability that this issue will occur. Please refer to Microsoft Help and Support for more details - http://support.microsoft.com/kb/906305.

Hardware Reassignment

If a hardware device, such as a smart card, is ever reassigned to another user, it is possible that ESSO-KM will logon as the original user. This occurs because ESSO-KM keeps a device-to-username mapping.

There is no work-around for this issue. It is strongly recommended that these devices not be reassigned to avoid this issue.

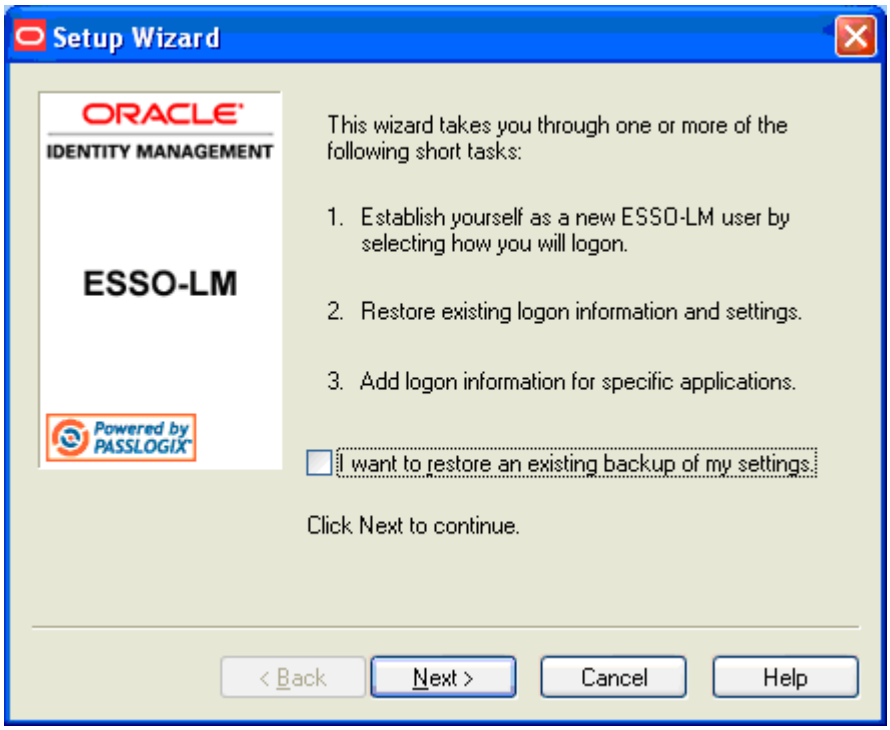
First Time Use Scenarios

In the setup phase, the user will go through the normal ESSO-LM First Time Use (FTU) wizard until the Select Primary Logon Method dialog box is displayed.

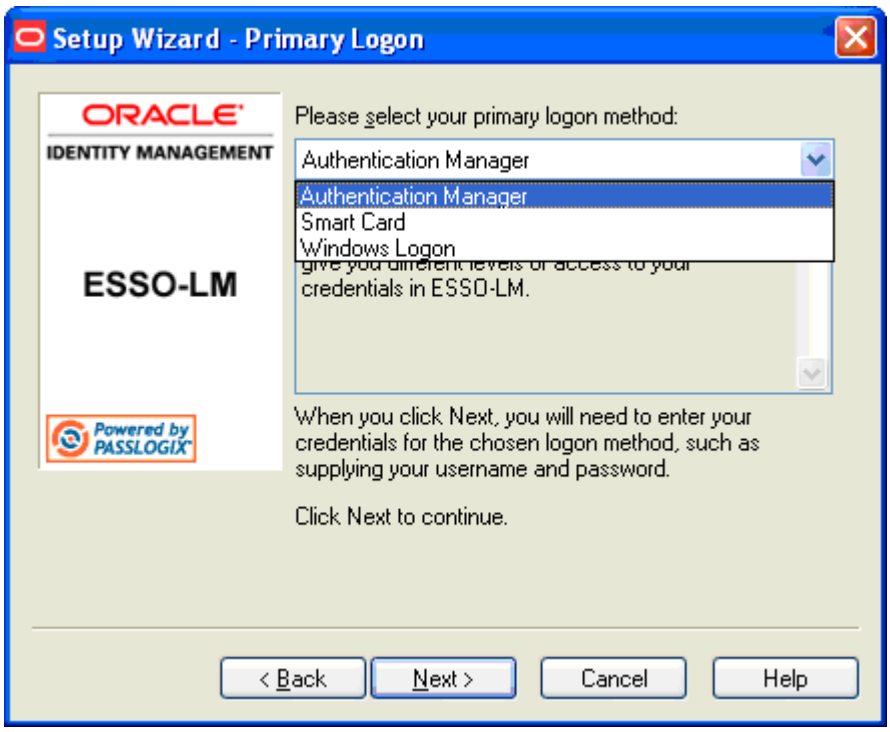
The behavior of this setup wizard is configured through the ESSO-LM Administrative Console.

Setup Flow Example

1. The first dialog box in the Setup Wizard dialog box lists the setup tasks necessary for the local installation of ESSO-LM. Click **Next** to begin setup.



2. The dialog box lists the setup tasks necessary for your local installation of ESSO-LM, choosing your primary logon method and supplying the credentials for that method. Click **Next**.
.
3. The Primary Logon dialog box prompts you to select a logon method. Select your desired primary logon method. Only methods that are currently installed will appear in the drop-down box. Click **Next**.



4. Enroll in your selected primary logon method. For example, if a smart card authenticator is installed, you will see the dialog below. Clicking **Cancel** for a required authenticator cancels the Setup Wizard.

5. Insert your smart card. You are prompted to enter your PIN. Click **OK**. A successful message appears. Click **OK**.
6. If the passphrase option is enabled, you might be prompted to enter a passphrase with a minimum answer length of eight characters. Enter an answer, confirm (re-enter) it, and click **OK**.
7. The Setup Wizard indicates that the process is complete and ESSO-LM is ready for use. Click **Finish** to complete.

Upgrade Notes

If you are performing an upgrade from an earlier version of ESSO-AM, install ESSO-AM according to the procedures contained in this document. ESSO-AM will preserve the behavior of previously enabled authenticators and automatically recognize the new authenticators.

If using ESSO-KM

If you have also installed ESSO-KM, you must take certain steps to ensure a successful upgrade.

1. Uninstall ESSO-KM. For more information, see the *ESSO-KM Installation and Setup Guide* for more information.
2. Install ESSO-AM 11.1.1.2.0.
3. Reinstall ESSO-KM.

If using Smart Cards

If you are using Smart Cards, you must take certain steps to ensure a successful upgrade.

- The Smart Card Authenticator now requires manually configuring the file path to the **PKCS #11 Library** when using PKCS#11 integration or using the authenticator with ESSO-KM.
- The Read-Only Smart Card Authenticator now requires manually configuring the file path to the **PKCS #11 Library** when using the authenticator with ESSO-KM.

Refer to the Smart Card Authenticator or Read-Only Smart Card Authenticator section for specific instructions on configuring this setting.

Uninstalling ESSO-AM

To uninstall ESSO-AM:

1. Close all programs.
2. Open the Control Panel and select **Add/Remove Programs**.
3. Select **Oracle Enterprise Single Sign-on Authentication Manager** and click **Remove**.
4. Follow the prompts to uninstall ESSO-AM.