Oracle© Enterprise Single Sign-on Logon Manager

Strong Authenticator Configuration Guide

Release 11.1.1.5.0

E21026-02

July 2011

ORACLE

Authentication ManagerStrong Authenticator Configuration Guide, Release 11.1.1.5.0

E21026-02

Table of Contents

Abbreviations and Terminology

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

Abbreviation or Term	Full Name
AD	Active Directory
ADAM	Active Directory Application Mode
Administrative Console	ESSO-LM Administrative Console
Agent	ESSO-LM Manager
FTU	First Time Use Wizard
ESSO-Anywhere	Oracle Enterprise Single Sign-on Anywhere
ESSO-LM	Oracle Enterprise Single Sign-on Logon Manager
ESSO-PG	Oracle Enterprise Single Sign-on Provisioning Gateway
ESSO-PR	Oracle Enterprise Single Sign-on Password Reset
ESSO-UAM	Oracle Enterprise Single Sign-on Universal Authentication Manager
OID	Oracle Internet Directory

Authentication Manager

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 strong authenticators such as smart cards, proximity devices, and RSA SecurID tokens.

ESSO-LM installed with Strong Authenticators

ESSO-LM includes both standard logon methods such as LDAP and Windows Logon, and 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 with ESSO-LM. You can have multiple installed authenticators but can only have one Primary Logon Method.

About ESSO-LM Strong Authenticators

ESSO-LM includes both standard logon methods such as LDAP and Windows Logon, and strong authenticators such as smart cards, proximity devices, and RSA SecurID tokens. ESSO-LM enables organizations to seamlessly bridge strong authentication to all of their applications. Users can employ different authenticators at different times and application access can be controlled based upon the authenticator used.

See the *Oracle Enterprise Single Sign-on Suite Plus Release Notes* for the most up-to-date list of supported authentication devices.

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

This purpose of this guide is to describe any specific settings that can be enabled within a strong authenticator in order for the authenticator to work with ESSO-LM. It also describes all the ESSO-LM Administrative Console settings and any steps that must be taken to integrate with Kiosk Manager, as well as any known issue or technical notes that apply to a specific strong authenticator.

Authenticator Configuration Settings

If the strong 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 strong authenticator, or view the Kiosk Manager integration notes which apply to all authenticators:

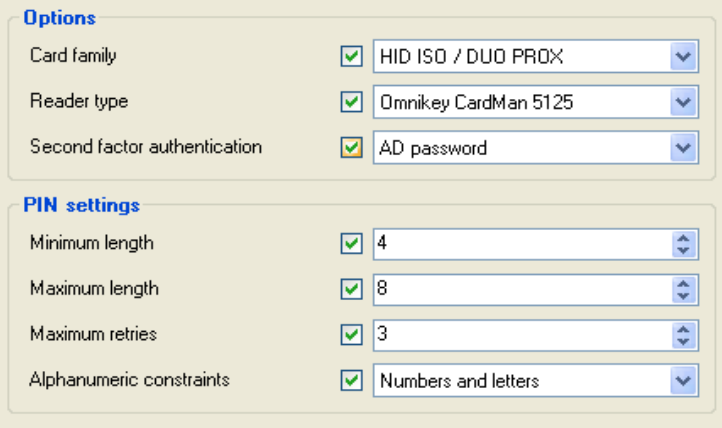
- Proximity Card
- Read Only Smart Card
- RSA SecurID
- Secure Data Storage
- Smart Card
- Kiosk Manager Integration Notes

Proximity Card

If you are using Proximity Cards, settings are available in the ESSO-LM Administrative Console. There are also steps that need to be taken when using AD or 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** > **Authentication** > **Proximity Card**.



Card family	The proximity card family type. **Options:** • HID ISO/DUO PROX (default) • iClass • Indala/EM
Reader type	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 Kiosk Manager is being used, Secure Data Storage must be enabled and configured in order for this setting to work.
Minimum length	Configures the minimum length of the user defined PIN. Default is 4.

Maximum length	Configures the maximum length of the user defined PIN. Default is 8.
Maximum retries	Configures the number of correct PIN attempts before the authentication fails. Default is 3.
Alphanumeric constraints	Configures the alphanumeric requirements of the user defined PIN. **Options:** • Numbers and letters (default) • Letters only • Numbers only

Integrating with Kiosk Manager

Support for storing and passing through the synchronization credentials with Kiosk Manager 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 Kiosk Manager session by tapping their proximity card and entering the correct PIN. This feature prevents a double authentication when starting a Kiosk Manager 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 AD 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.

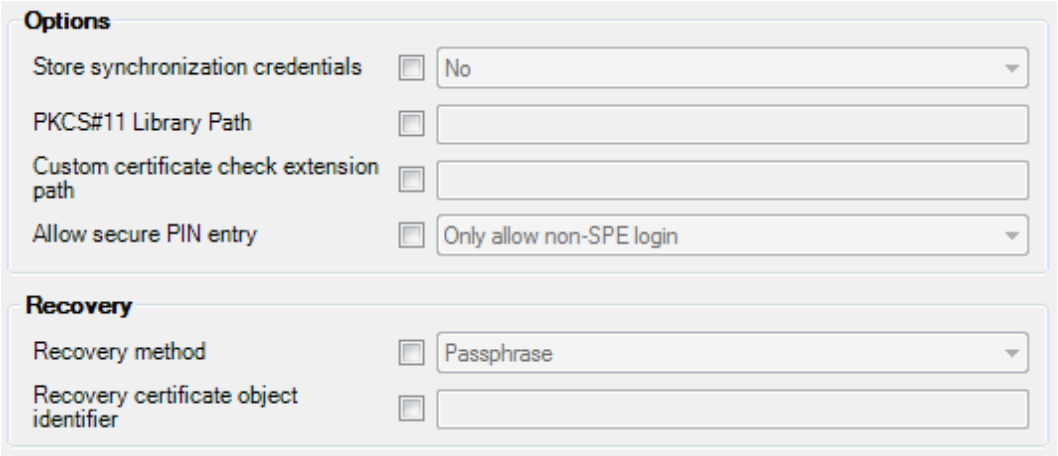
Read-Only Smart Card

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

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** > **Authentication** > **Read Only Smart Card**.



Options	
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 Kiosk Manager. Secure Data Storage must be enabled and configured in order for this setting to work. **Options:** • No (default) • Yes
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 Kiosk Manager.
Custom certificate check extension path	Use this setting to specify the path to the custom certificate check extension. There is no default for this setting. This entry is not required.

Options	
Allow secure PIN entry	Use this setting to allow users to enter a PIN on a smart card reader keypad that supports secure PIN entry. **Options** • **Only allow non-SPE login.** Use with cards that do not support Secure PIN entry. (Default) • **Only allow SPE login.** Use with cards that support/require Secure PIN entry.

Recovery	
Recovery method	Enables the use of the reset passphrase. The passphrase can be supplied either by the user (entering the passphrase in a dialog box) or by the newest non-default encryption certificate on the card itself. **Options:** • Passphrase (default) • Encryption certificate
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 **Recovery Method** option must be set to **Encryption certificate**.

Smart Card Initialization

Prior to use with Authentication Manager, 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 Kiosk Manager, they must have a serial number.

Authentication Manager 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 Kiosk Manager

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

When using Read-Only Smart Card authenticator with Kiosk Manager, the user's synchronization credentials can optionally be stored by setting **Store Synchronization Credentials** to **Yes** 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 Kiosk Manager 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 Kiosk Manager 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 Kiosk Manager Session and ESSO-LM **when Read-Only Smart Card is the Primary Logon Method:**

In a Kiosk Manager environment that uses read-only smart cards as the primary logon method, users are prompted to authenticate separately to Kiosk Manager 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 Kiosk Manager session starts, Kiosk Manager 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 Kiosk Manager process only; therefore, when the Kiosk Manager 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 Kiosk Manager 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 Authentication Manager 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 Authentication Manager 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 Kiosk Manager

When using the RSA SecurID authenticator with Kiosk Manager,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.

Support for storing and passing through the synchronization credentials with Kiosk Manager and RSA SecurID integration:

When using RSA SecurID authenticator with Kiosk Manager, 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 Kiosk Manager session with a RSA SecurID token. This feature prevents a double authentication when starting a Kiosk Manager 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

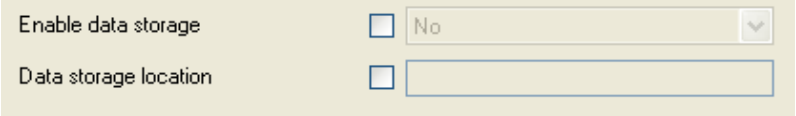
Secure data storage settings control the location for data storage. Secure data storage can be used for:

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

> Secure Data Storage is supported in Active Directory, Active Directory Application Mode, and Oracle Internet Directory.

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

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



Enable data storage	Configures whether to securely store users' synchronization credentials within the repository. **Options** • No (default) • Yes
Data storage location	Fully-qualified path to the location in the repository where the data will be stored.

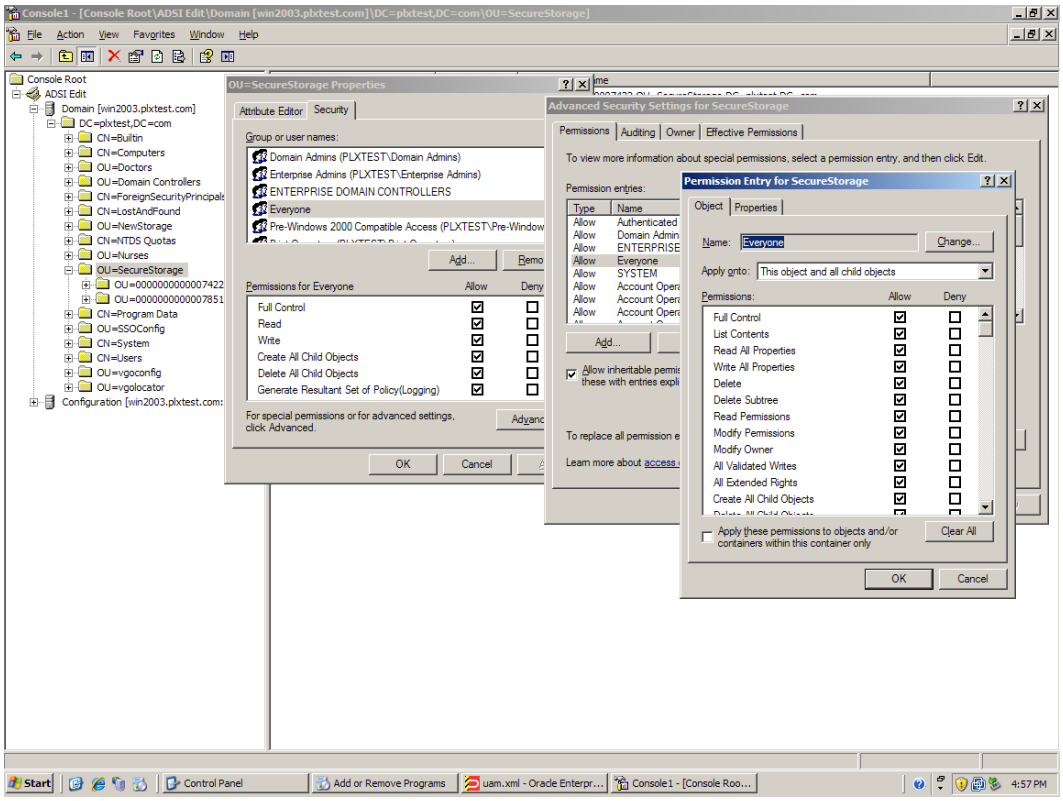
Enabling Secure Data Storage

Regardless of your repository, start the procedure for enabling secure data storage as follows:

1. On the Secure Data Storage pane, set **Enable Data Storage** to **Yes**.
2. Create a new Organizational Unit that will serve as the data storage location.
3. Specify the fully-qualified distinguished name for this object as the value of the **Data storage location** setting.
4. Continue to the next steps below for the appropriate repository.

Next Steps for Active Directory

5. Grant FULL CONTROL permission to this Organizational Unit to "Everyone."
6. Apply this to **This object and all child objects**.

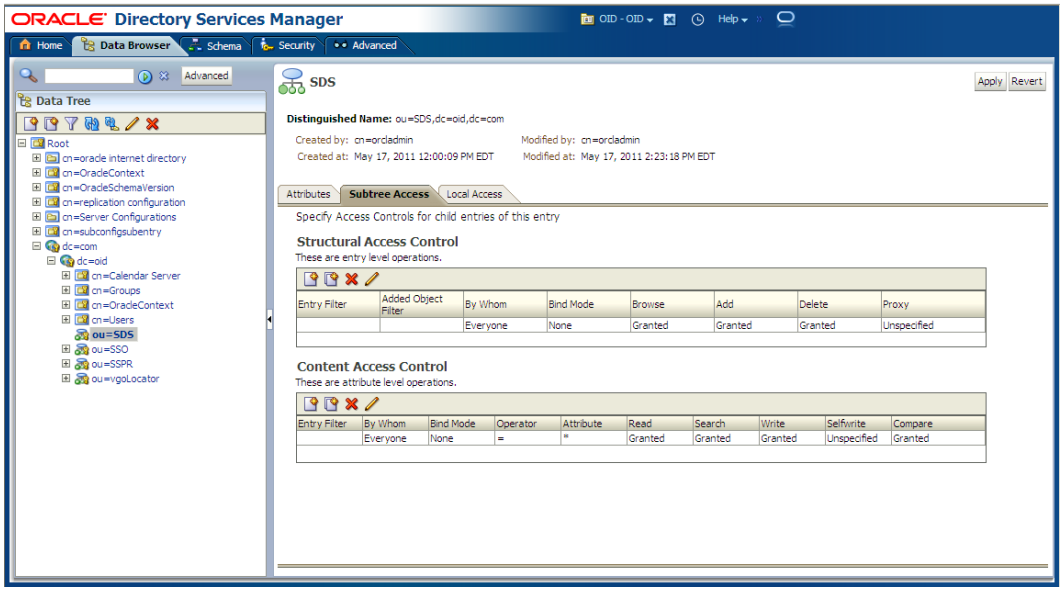


Next Step for ADAM

5. 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 "Everyone":GA`

Next Steps for Oracle Internet Directory

5. Grant anonymous users access to the Secure Data Storage container.
6. Log on to the Directory Services Manager as an administrator.
7. Select the **Data Browser** tab.
8. In the tree, navigate to and select the **Secure Data Storage** container that you created.
9. Select the **Subtree Access** tab.
10. Create a new access entry under Structural Access Control and Content Access Control. Accept the default permissions and click **OK**.
11. **Apply** the changes. The default permissions grant "Everyone" with bind mode "None" the appropriate access:



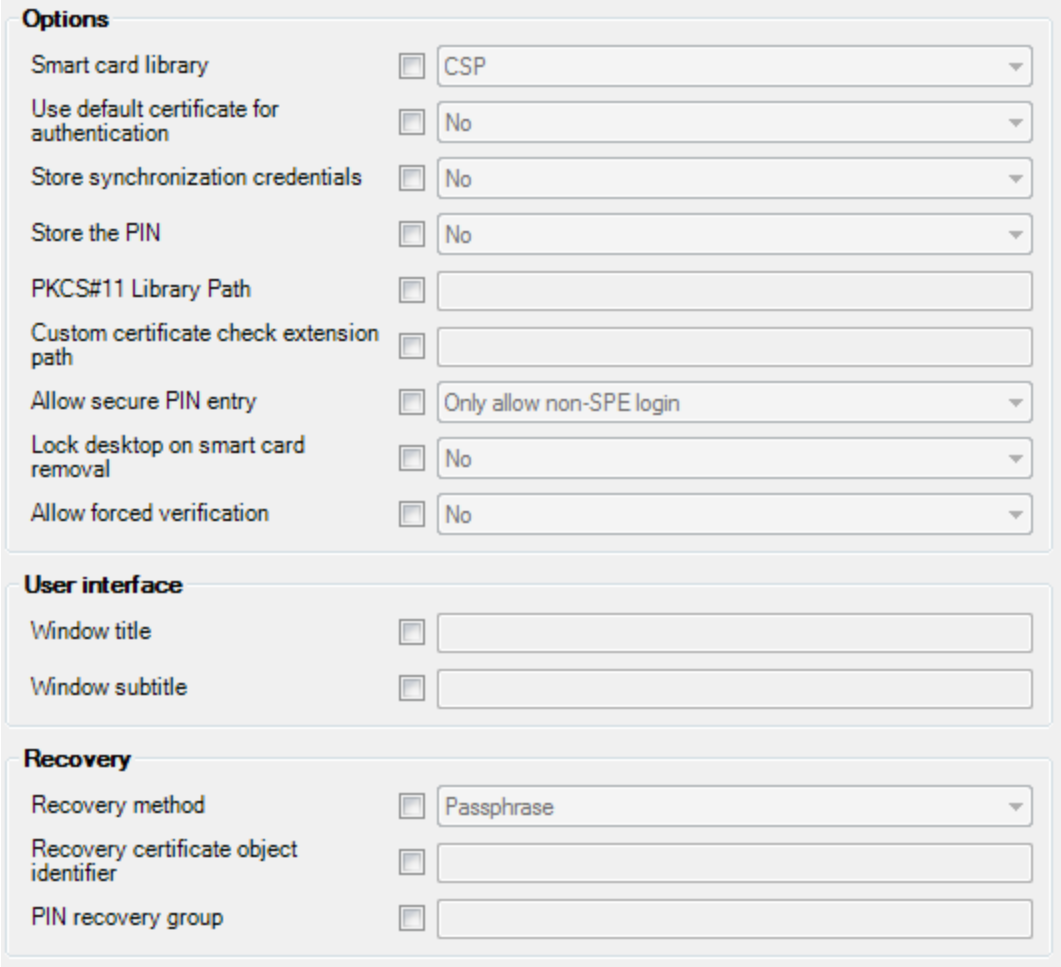
Smart Card

If you are using Smart Cards, settings are available in the ESSO-LM Administrative Console. There are also steps that need to be taken if integrating with Kiosk Manager 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** > **Authentication** > **Smart Card**.



Options	
Smart card library	Specifies whether to use the Cryptographic Service Provider (CSP) or the PKCS #11 library to perform cryptographic operations on the smart card. **Options** • CSP (default) • PKCS #11  Set this to PKCS # 11 only if using SafeSign/RaakSign middleware. `Registry node: AUI\SCauth:SmartCardAPI`
Use default certificate for authentication	Specifies whether to use the default logon certificate (provided by the administrator) on the card for authentication. If not enabled (the default), the public/private keys in the SSO container on the card will be used (and created if necessary). **Options** • No (default) • Yes `Registry node: AUI\SCauth:UseCertOnCard`
Store synchronization credentials	Specifies whether to store the user's synchronization repository credentials on the smart card. Store credentials when using smart card authorization in conjunction with Kiosk Manager and/or if using the read-only smart card authenticator.  Performance improves when credentials are not stored on the smart card because the read/write operation adds time to the authentication process. **Options** • No (default) • Yes `Registry node: AUI\SCauth:StoreSyncCreds`
Store the PIN	Specifies whether to store the smart card PIN (creating the possibility that the Agent might prompt for the PIN), or to let the smart card drivers handle the PIN request. **Options** • No (default) • Yes `Registry node: AUI\SCauth:AuthOptions`
PKCS #11 Library Path	Use this setting to configure the path to the smart card middleware file, which implements the PKCS#11 standard.  This entry is not required unless "Smart card library" is set to PKCS #11, "Store synchronization credentials" is set to Yes, or smart cards are being used with Kiosk Manager.

Options	
Custom certificate check extension path	Use this setting to specify the path to the custom certificate check extension. There is no default for this setting.  This entry is not required.
Allow secure PIN entry	Use this setting to allow users to enter a PIN on a smart card reader keypad that supports secure PIN entry.  You cannot use secure PIN entry in conjunction with a PIN recovery group. **Options** • **Only allow non-SPE login.** Use with cards that do not support Secure PIN entry. (Default) • **Only allow SPE login.** Use with cards that support/require Secure PIN entry.
Lock desktop on smart card removal	Specifies whether to lock the desktop when the smart card owner removes the smart card from the reader. By default, this value is set to **No**. If the value is set to **Yes**, the user's workstation locks when the smart card is removed. **Options** • No (default) • Yes
Allow forced verification	Specifies whether ESSO-LM should automatically authenticate users after they authenticate to Windows with a smart card. Setting this to **No** (the default) requires a user to enter a PIN for both Windows logon and to authenticate to ESSO-LM. Setting this to **Yes** eliminates the double PIN prompt and the user needs to enter a PIN only to authenticate to Windows, while ESSO-LM automatically authenticates the user.  To use this feature, Network Provider MUST be installed with ESSO-LM. This is available during the installation on the Advanced Setup panel under Authenticators. Refer to the *ESSO-LM Installation and Setup Guide* for more information. **Options** • No (default) • Yes `Registry Location: AUI\SCauth:AllowForcedVerification`

User interface	
Window title	Use this setting to customize the window title name for this authenticator.  This entry is not required.
Window subtitle	Use this setting to customize the window subtitle name for this authenticator.  This entry is not required.

Recovery	
Recovery method	Specifies the supplier of the reset passphrase to be used: the user (entering the passphrase in a dialog box), the newest non-default encryption certificate on the card itself, or the smart card PIN. You cannot use a PIN recovery group in conjunction with secure PIN entry. **Options** • Passphrase (default) • Encryption certificate • Smart card PIN
Recovery certificate object identifier	Configures the object identifier of the certificate used for the certificate-based passphrase feature. The authenticator searches the "Enhanced Key Usage" attribute of each certificate on the smart card for this object identifier. The "Recovery method" option must be set to "Encryption certificate." This entry is not required.
PIN recovery group	Enter the domain security group name (in format domain\group) for the PIN Recovery Group. Members of this group will be allowed to authenticate to ESSO-LM without a smart card, and using only a PIN. This setting is useful in a scenario where users lose their cards and are waiting for new ones. While the cards are being replaced, users can be added to this PIN recovery group so that they can authenticate to ESSO-LM without their cards. To use this feature, the Recovery method setting above MUST be set to Smart card PIN.

Smart Card Initialization

Prior to use with Authentication Manager, smart cards must be initialized and contain a valid PIN. If Authentication Manager 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 Kiosk Manager, they must have a serial number.

Authentication Manager 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 Kiosk Manager

The following information applies when using the Smart Card authenticator with Kiosk Manager:

Support for storing and passing through the synchronization credentials with Kiosk Manager and Smart Card integration:

When using Smart Card authenticator with Kiosk Manager, 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 Kiosk Manager session by inserting their smart card into the reader and entering the correct PIN. This feature prevents a double authentication when starting a Kiosk Manager 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 Kiosk Manager, inserting the smart card when Kiosk Manager 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 Kiosk Manager Session and ESSO-LM when Smart Card is the Primary Logon Method:

In a Kiosk Manager environment that uses smart cards as the primary logon method, users are prompted to authenticate separately to Kiosk Manager 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 Kiosk Manager session starts, Kiosk Manager 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 Kiosk Manager process only; therefore, when the Kiosk Manager 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 Kiosk Manager, 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** (located in the ESSO-LM Administrative Console **Global Agent Settings** > **Authentication** > **Smart Card**) is set to **No**, 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 users 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 Authentication Manager

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 Kiosk Manager

When starting a new Kiosk Manager 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 Kiosk Manager

RSA Middleware reports that no smart cards are present when Kiosk Manager is locked and a smart card is inserted into a reader. Sessions must be manually started. After Kiosk Manager 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.

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:** Kiosk Manager stops responding and requires a restart.

There are two workarounds to this issue:

1. Users can manually start a Kiosk Manager 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 Kiosk Manager will logon as the original user. This occurs because Kiosk Manager keeps a device-to-username mapping.

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

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.

Prerequisites

ESSO-LM 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, Authentication Manager 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.

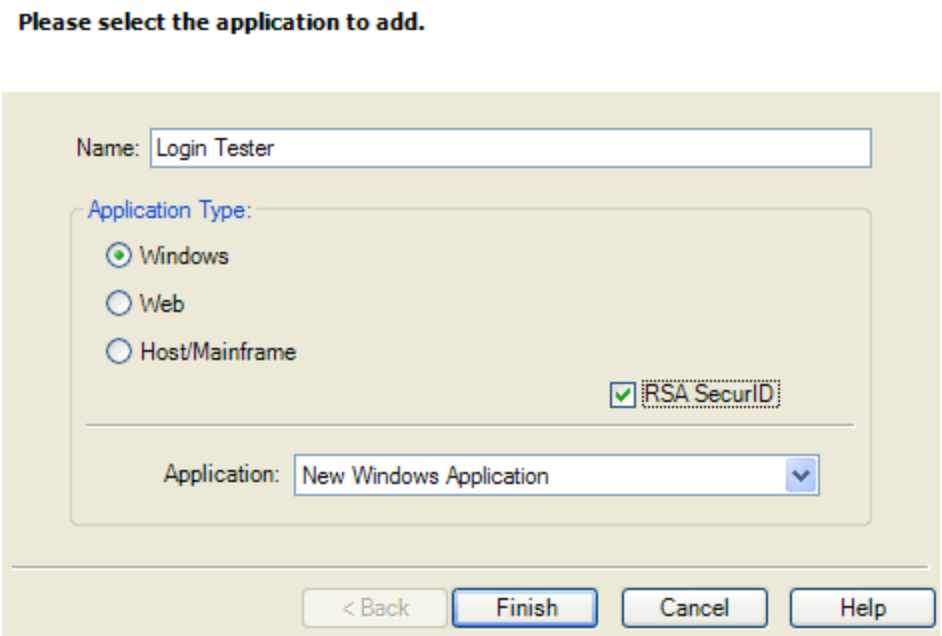
Install ESSO-LM

Install ESSO-LM with Authentication Manager and Authentication Manager with the SoftID helper. See the *ESSO-LM Installation and Setup Guide* for more information.

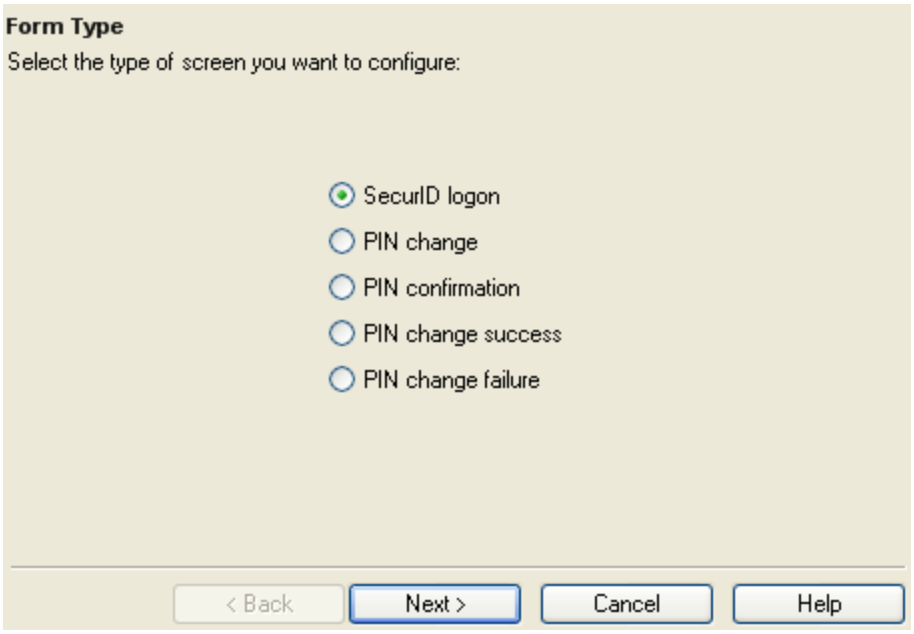
Configuring RSA SecurID Application Templates

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

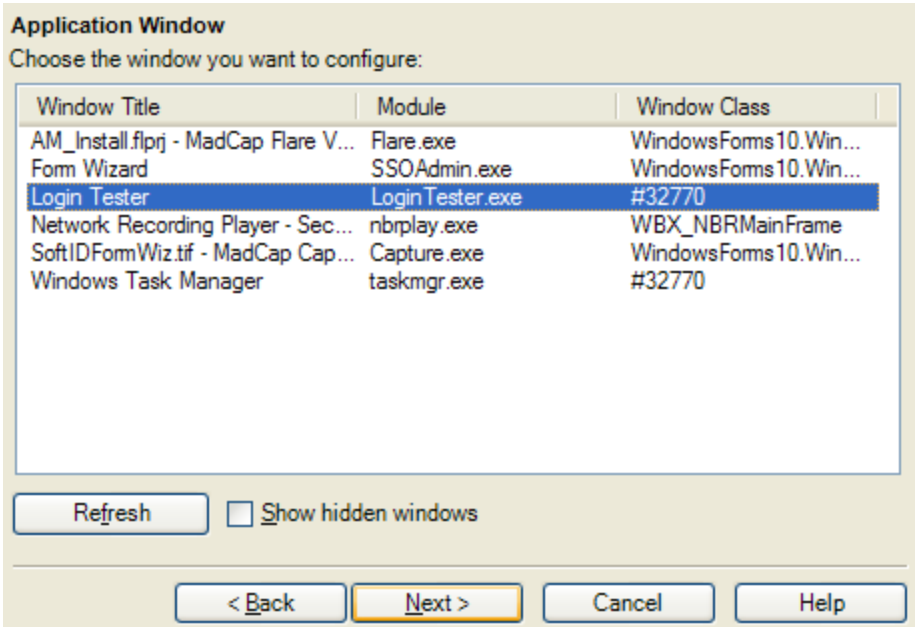
1. Open the ESSO-LM Administrative Console.
2. Launch the application for which you are defining a template.
3. Right-click **Applications** and select **New Windows Application**. The Add Application dialog appears.



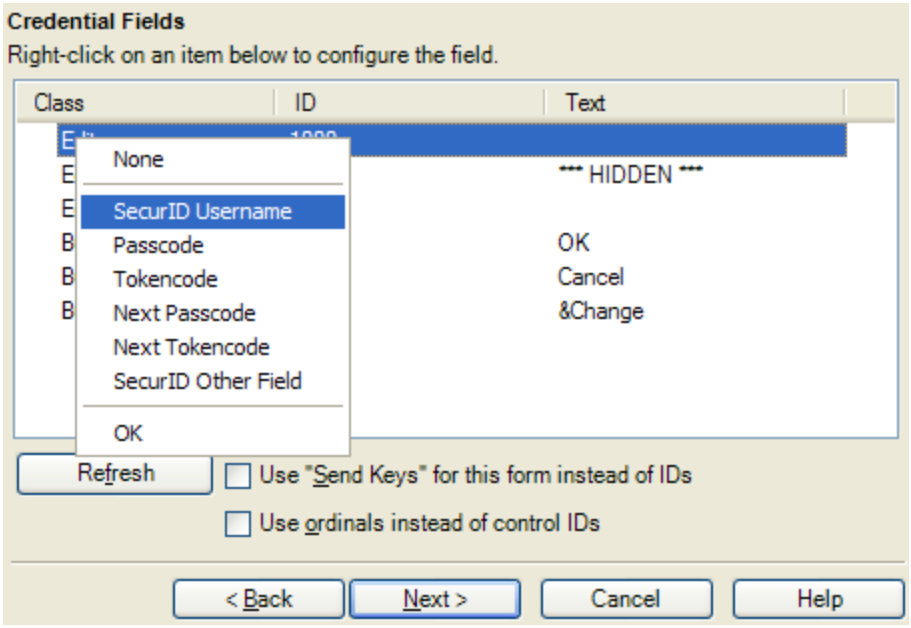
4. Enter the application **Name** and check the **RSA SecurID** check box. Click **Finish.** The Form Wizard appears.



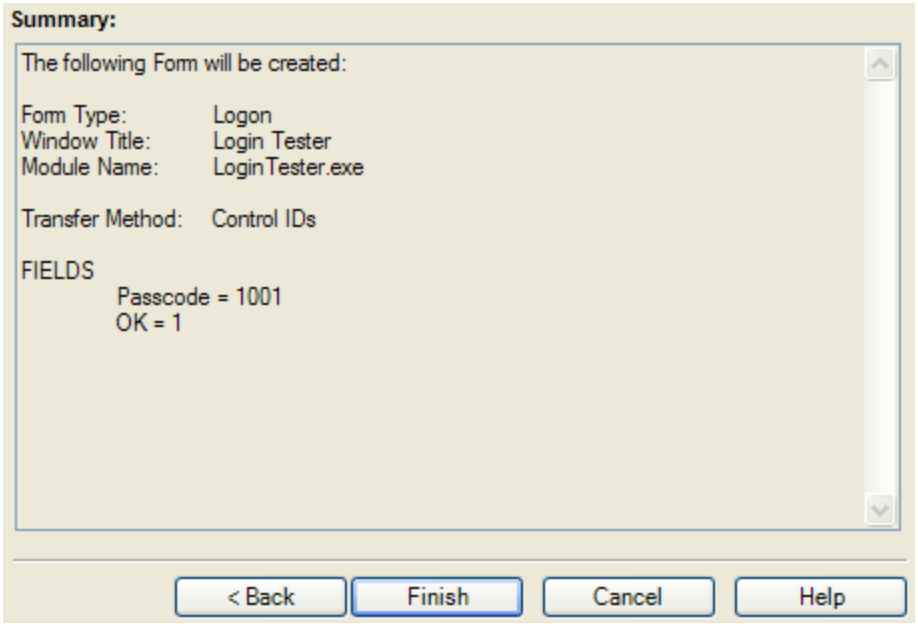
5. Select the **SecurID Login** button. Click **Next**. As long as the application for which you are defining a template is running, the window title will appear in the next wizard panel.



6. Select the Window Title for your application. Click **Next**.

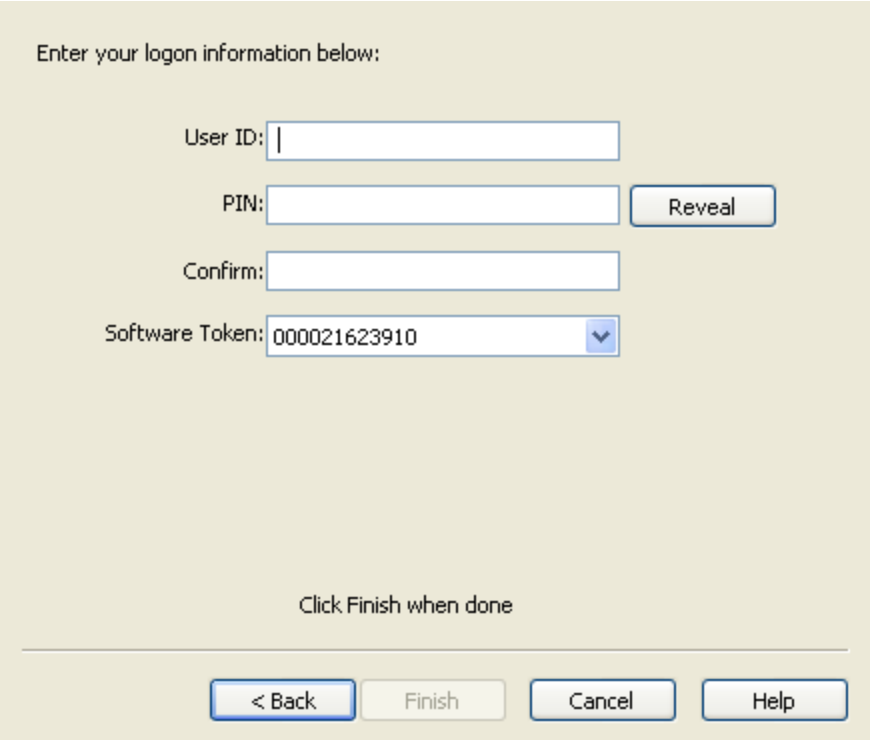


7. On this dialog, you configure the **SecurID Username**, **Passcode**, and **OK** button fields as well as any other applicable fields for your application. Right-click on the class and select the fields. Click the **Help** button for more information on configuring the credential fields. Click **Next** 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 application for which you defined a template 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 this application.



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 Authentication Manager. Authentication Manager 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.

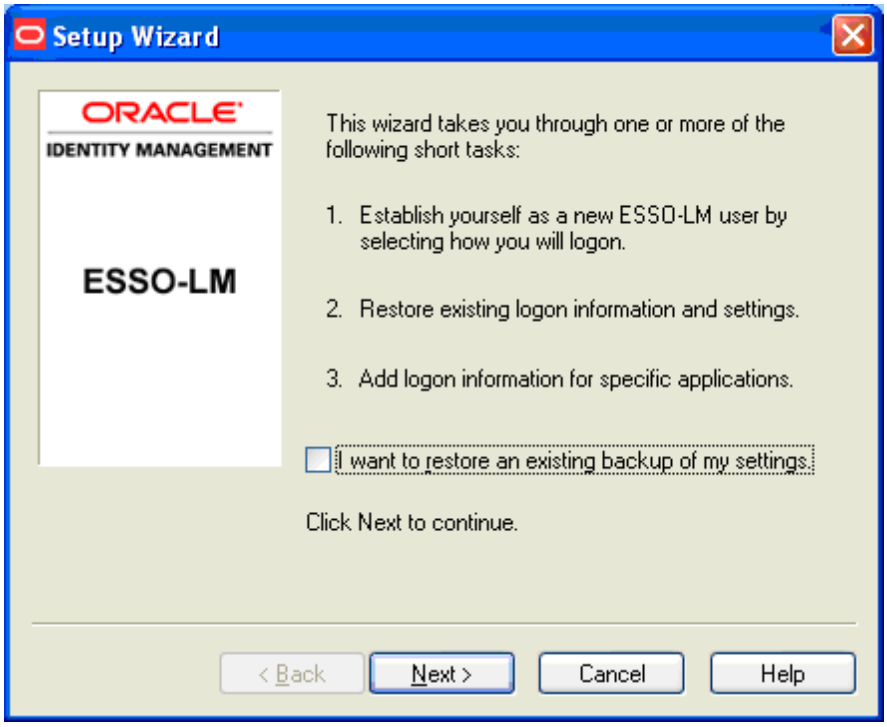
First Time Use Scenarios

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.

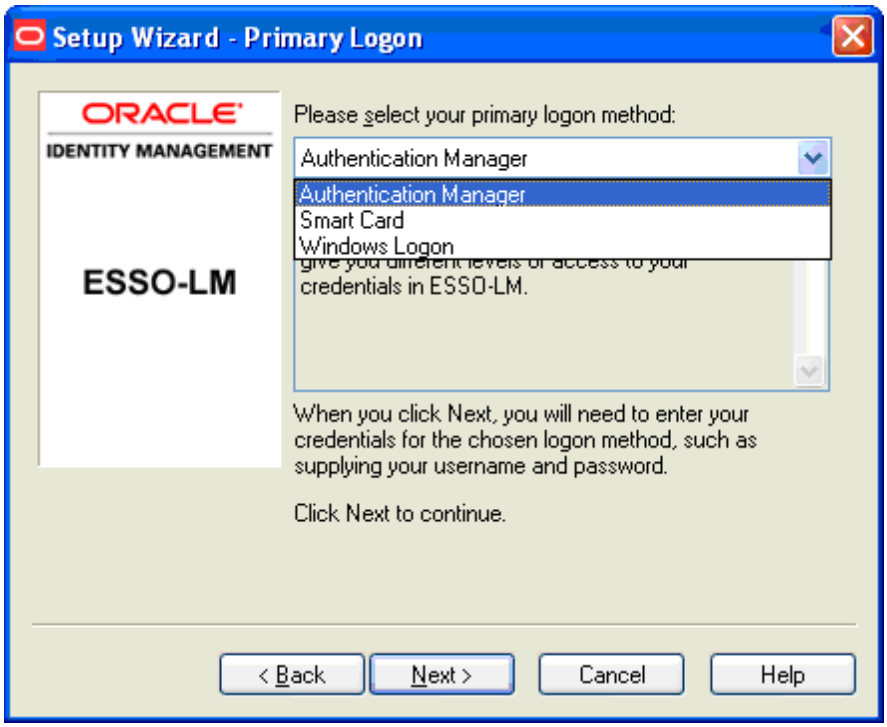
The behavior of this setup wizard is configured through the ESSO-LM Administrative Console.

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.