Oracle® Enterprise Single Sign-on Logon Manager

Best Practices: Deploying ESSO-LM with the Windows Authenticator Version 2

Release 11.1.1.5.0

E21009-01

March 2011

ORACLE

Oracle Enterprise Single Sign-on Logon Manager Best Practices: Deploying ESSO-LM with the Windows Authenticator Version 2

Release 11.1.1.5.0

E21009-01

Table of Contents

Introduction

About This Guide

This document describes the differences between the Windows Authenticator (WinAuth) version 1 and version 2, the advantages of WinAuth v2 over WinAuth v1, and the best practices for deploying WinAuth v2 on new and existing environments.

Prerequisites

Readers of this document should have a thorough understanding of ESSO-LM deployment and configuration, as well as cryptography topics and concepts such as key-based encryption, the Windows Data Protection API (DPAPI), and Windows operating system and Active Directory security.

Terms and Abbreviations

The following table describes the terms and abbreviations used throughout this guide:

Term or Abbreviation	Description
ESSO-LM	Oracle Enterprise Single Sign-on Logon Manager
ESSO-PR	Oracle Enterprise Single Sign-on Password Reset
Agent	ESSO-LM client-side software
Console	E SSO-LM Administrative Console
WinAuth v1	Windows Authenticator version 1
WinAuth v2	Windows Authenticator version 2
DPAPI	Windows Data Protection API

Accessing ESSO-LM Documentation

We continually strive to keep ESSO-LM documentation accurate and up to date. For the latest version of this and other ESSO-LM documents, visit http://download.oracle.com/docs/cd/E21040_01/index.htm.

Part 1: Understanding the Windows Authenticator

Overview

In order to authenticate a user and grant access to stored credentials, ESSO-LM offers a number of authentication methods implemented as authenticator plug-ins, with the most common method being a user name and password. On Active Directory environments, ESSO-LM supports this authentication method through its Windows Authenticator (WinAuth) v1/v2 plug-ins. Because the management of the credential store key is implemented in WinAuth v2 in a more robust and comprehensive way than in WinAuth v1, Oracle recommends deploying WinAuth v2 in place of WinAuth v1 as a best practice; Oracle will eventually phase out WinAuth v1 in favor of WinAuth v2 for this reason.

Understanding Credential Store Encryption

When the user enrolls with ESSO-LM for the first time, ESSO-LM generates a credential store key, which is then securely managed by WinAuth v1/v2.

WinAuth v1 relies on local machine keysets to encrypt the credential store key (generated during first-time enrollment with ESSO-LM). The encrypted credential store key is kept in the local machine's registry, and is also passed between the Agent and the repository (after being encrypted with a different, randomly generated authenticator key).

If you log on to a machine different from the machine on which original enrollment for your user account took place, the Agent will encrypt your credential store key with the new machine's local key. Because of this, under certain circumstances, including when roaming user profiles are in effect, logging on to multiple machines can result in loss of access to the stored credentials. Due to the limitations imposed by the design of WinAuth v1, the credential store key management scheme has been reengineered in WinAuth v2.

With WinAuth v2, once generated during enrollment, the credential store key can be managed, maintained, stored, and accessed using one of the following methods:

- **Directly by WinAuth v2.** By default, credential store key management is handled by WinAuth v2. The key is stored either in the local cache or within the user's object in Active Directory (as configured by the ESSO-LM administrator) and encrypted using authentication factors that "follow the user" (i.e., are provided by the user and stored in the directory). These factors include the user name, password, and domain name, and remain the same regardless of which machine the user logs onto, eliminating the possibility of using the wrong key to operate on the credential store. However, because these factors can be changed by the user or administrator (for example, the administrator may change the user's password), WinAuth v2 implements a recovery mechanism explained in Understanding Credential Store Key Recovery.

- **Using Windows Data Protection.** WinAuth v2 can be configured to delegate the management and maintenance of the credential store key to the Windows Data Protection service, through the Windows Data Protection API (DPAPI). This eliminates the need for a recovery key, because the credential store key is always secure, valid, and available to WinAuth v2 via DPAPI for silent authentication of the user. However, this configuration may be vulnerable to a rogue administrator changing the user's password, logging on as the user onto the local machine, and accessing the user's credential store, since the credential store key is always available to WinAuth v2 via DPAPI.

> **Note:** Your environment must meet the system requirements for DPAPI explained in Configuring WinAuth v2 for Credential Store Key Management via Windows DPAPI.

If you want to learn more about how WinAuth v2 encrypts and decrypts the credential store, contact your Oracle representative for a white paper on this topic.

Understanding Credential Store Key Recovery

The key advantage of WinAuth v2 over WinAuth v1 is the use of fully portable authentication factors (user name, password, domain name) to encrypt the credential store key in non-DPAPI scenarios. Because this data can change over time (for example, the user can change their password), WinAuth v2 includes the provision for a recovery key when credential store key management is not delegated to DPAPI. The recovery key is generated during enrollment and grants "second door" access to the credential store key (and thus the user's credential store) in the event that any of the factors that comprise the encryption for the credential store key have changed.

WinAuth v2 provides the following ways of accepting the recovery key:

- Interactive passphrase prompt
- Secondary authentication API

Recovery via Interactive Passphrase Prompt

The interactive passphrase recovery mechanism requires the user to provide an answer to a question presented during initial enrollment with ESSO-LM. (The question is defined by the administrator.) The user must supply the passphrase answer in order to authenticate to ESSO-LM each time any of the factors used to encrypt the credential store key have changed. Oracle highly recommends that your organization enforces the same cryptographic strength policy for passphrase answers as it does for passwords.

> **Note:** While it is possible to define more than one passphrase question, the current user enrollment interface is not well-suited for multiple passphrase questions. To reduce the complexity of the user enrollment process, Oracle recommends defining no more than one passphrase question.

Advantages:

- **Acts as "second password" to the credential store.** The passphrase can be used to regain access to the credential store in the event the user's Windows password is no longer functional or accessible.
- **Prevents rogue administrator attacks.** A rogue administrator could potentially change a user's password, log on as that user, and gain access to the user's credential store; however, with a passphrase in place, the rogue administrator will not be able to gain access to the stored credentials without providing the passphrase answer.

Disadvantages:

- **High cryptographic strength is not enforceable.** The user may choose a cryptographically weak passphrase answer, as only a minimum length of the answer can be enforced by ESSO-LM.
- **Not easily changeable and non-expiring.** The ESSO-LM interface does not provide a way to change the passphrase answer. It can currently only be done manually by an administrator as described in Resetting the User-Provided Passphrase Answer.

For instructions, see Configuring WinAuth v2 for Recovery via Interactive Passphrase Prompt.

Recovery via ESSO-LM Secondary Authentication API

WinAuth v2 provides a secondary authentication API which allows the passphrase answer to be programmatically supplied by an external secondary authentication library without the need for user interaction. You have the option of using a custom-written library, or one of ESSO-LM's built-in silent secondary authentication methods.

External Secondary Authentication Library

Using the API, you can develop a custom secondary authentication library, imparting full control over the way the secondary key is delivered to ESSO-LM during recovery.

> **Note:** For more information on the API, see the *ESSO-LM How-To* guide *Understanding the ESSO-LM Secondary Authentication API*.

Advantages:

- **Eliminates the passphrase prompt during recovery.** The passphrase answer is provided programmatically to WinAuth v2 whenever a recovery event occurs.
- **Enables seamless integration with an existing environment.** You can fully customize the secondary authentication process, making it either silent, or interactive, and integrating it with your existing applications.
- **Prevents rogue administrator attack when interactive challenge-response approach is chosen.** If you choose to challenge the user with passphrase questions through a custom user interface, a rogue administrator will not be able to access the stored credentials by simply changing the user's password and impersonating the user to ESSO-LM.

Disadvantages:

- **Does not prevent the rogue administrator attack if silent authentication approach is chosen.** If you choose to retrieve and supply the passphrase answer to WinAuth v2 silently, a rogue administrator could change the user's password, log on as the user onto the local machine, and access the user's credential store, as the passphrase answer would be automatically supplied during authentication to ESSO-LM.
- **If you choose to store the recovery key in a custom key store, your storage and management processes are responsible for the security of the recovery key.** A key store may lessen the security of the secondary authentication process if it is not designed to prevent rogue access to the recovery key.

Built-In Silent Secondary Authentication Methods

ESSO-LM provides the following silent secondary authentication methods:

- **User's AD SID** - silently supplies the Active Directory SID of the currently logged on user as the passphrase answer to WinAuth v2. The encrypted SID is stored in the Agent's local cache.
- **Secure random key** – silently supplies a randomly generated key as the passphrase answer to WinAuth v2. This random key is stored in encrypted form within the user's ESSO-LM credential store in Active Directory. Unauthorized access to the key is automatically restricted via Active Directory ACLs that are in effect for the user's credential store container.

Advantages:

- **Eliminates the passphrase prompt during recovery.** The passphrase answer is provided programmatically to WinAuth v2 whenever a recovery event occurs.
- **Knowledge of the user's SID is not enough to access the stored credentials.** Access is only granted through this recovery method if the user has been authenticated to ESSO-LM in the current session and the user's password has just changed; direct access to a user's credential store through simply knowing the user's SID is extremely difficult.

Disadvantages:

- **Does not prevent the rogue administrator attack.** A rogue administrator could change the user's password, log on as the user onto the local machine, and access the user's credential store, as either the SID or random key would be automatically supplied to WinAuth v2 during credential store key recovery. For this reason, Oracle recommends using ESSO-LM's built-in silent secondary authentication methods only in situations where you want to eliminate the interactive passphrase prompt during recovery but cannot use the Windows Data Protection service to manage and maintain the credential store key.

For instructions, see Configuring WinAuth v2 for Recovery via ESSO-LM Secondary Authentication API

Understanding the GINA and Network Provider Components

The GINA (Graphical Identification aNd Authentication) library and Network Provider service components of WinAuth v2 provide integration with the user authentication mechanism in the Windows operating systems. The GINA component hooks into the Microsoft-supplied `gina.dll` library on Windows XP and earlier systems, while the Network Provider service allows integration with Windows Vista, Windows Server 2003 and 2008, and Windows 7, which do not use a GINA library. The Network Provider service also enables integration on Windows XP systems on which changes to the GINA library are not permitted or feasible.

This integration provides the following advantages:

- **Eliminates the need for double authentication.** Without this integration, the user would need to provide their Windows credentials twice – once to the operating system in order to log on, unlock the desktop, or exit a secure screensaver, and again to ESSO-LM in order to access stored credentials.
- **Unlocking of the credential store is transparent to the user.** ESSO-LM automatically intercepts the user's Windows credentials during logon and unlocks the credential store so that the user does not need to authenticate to ESSO-LM in order to use automatic single sign-on, unless ESSO-LM has been configured otherwise.

Note: If you are deploying ESSO-LM with WinAuth v2 in an ESSO-PR environment in which client machines run either Windows XP or Windows Server 2003, do not install the Network Provider component, as it is incompatible with ESSO-PR. Install the GINA library only, ensuring that you install its most recent version (i.e., the version supplied with the more recent of the two applications.)

For instructions on installing the above components, see Installing WinAuth v2.

Summary of Key Advantages of WinAuth v2 over WinAuth v1

The table below summarizes the key advantages that WinAuth v2 holds over WinAuth v1.

Feature	WinAuth v1	WinAuth v2
Encryption of credential store key	Encrypted with non-portable local machine key.	Encrypted with key generated from portable authentication factors (user name, password, domain name).
Credential store key portability	Not supported. Non-portable credential store key encryption may cause key mismatch (and loss of access to credential store) when roaming between machines.	Supported. Portable credential store key encryption eliminates possibility of key mismatch.
Credential store key recovery	Recovery not needed. Logging on to local machine grants access to the credential store key. When you log in, you have access to the key and can decrypt the store.	Supported via the following methods in non-DPAPI scenarios: • Interactive passphrase prompt • Secondary authentication API Not needed when credential store key is managed via DPAPI.
Rogue administrator attack protection	Absent.	Present if prompting the user for the passphrase answer during recovery (either via built-in passphrase support or appropriately designed secondary authentication library).
Integration with the Windows user authentication mechanism	Not leveraged or possible.	Supported via the following methods: • GINA library hook (Windows XP only) • Network Provider service (Windows XP, Vista, Windows Server 2003 and 2008, and Windows 7) Provides close integration with the Windows user authentication mechanism (e.g., when logging on, unlocking the desktop, or exiting a secure screensaver).

In Active Directory environments in which the Windows user name and password are the chosen primary authentication method, Oracle highly recommends deploying WinAuth v2 with all new ESSO-LM installations, as well as migrating existing WinAuth v1-based installations to WinAuth v2. Instructions for installation, configuration, and migration are provided in the remainder of this guide.

Part 2: Installing, Configuring, and Migrating to Windows Authenticator Version 2

This section describes how to install and configure the Windows Authenticator v2 for each of the secondary authentication methods described earlier in this document. It covers the following topics:

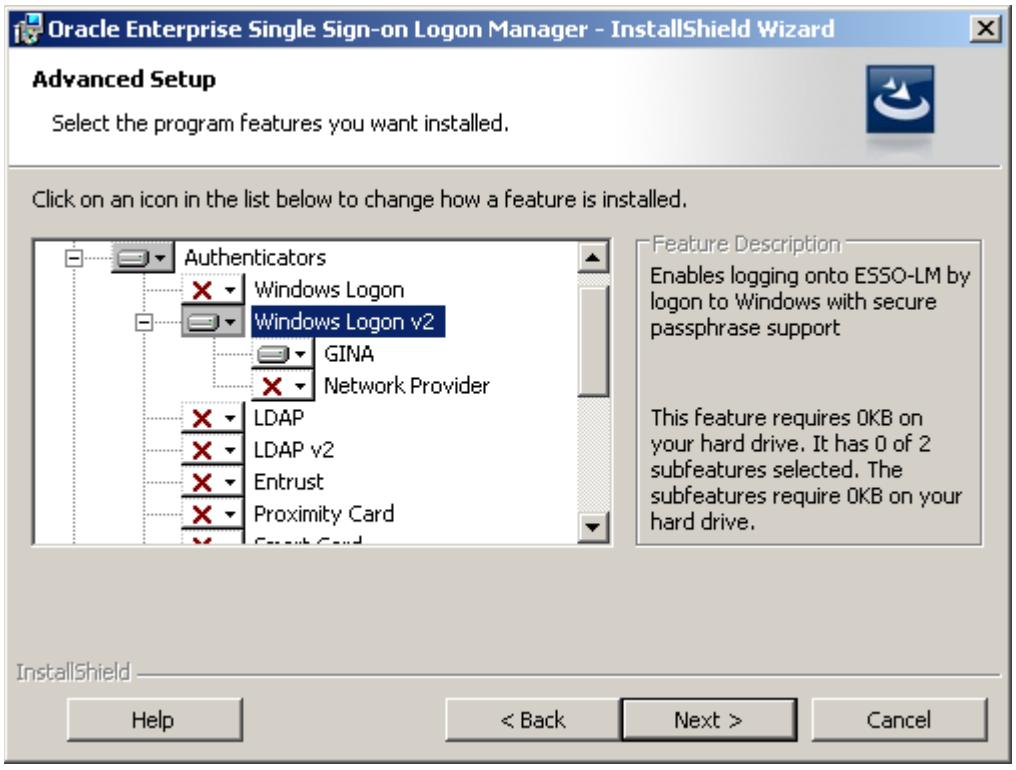
Note: The steps in this section illustrate how to manually perform the procedures listed above. If you wish to automate and/or customize any of those processes, see the *ESSO-LM Best Practices* guide *Packaging ESSO-LM for Mass Deployment* and/or request the assistance of Oracle Support to develop a deployment plan tailored specifically to your environment.

Installing WinAuth v2

Note: If you want to migrate an existing WinAuth v1 installation to WinAuth v2, skip this procedure and follow the steps in Migrating a WinAuth v1 Installation to WinAuth v2.

To install the Windows Authenticator Version 2 on a fresh deployment of ESSO-LM, do the following:

1. If you have not already installed ESSO-LM, follow the instructions in the *Installation and Setup* guide for your version of ESSO-LM, making sure to select the Custom installation mode. When you reach the component selection screen (shown below), continue to step 2 of this procedure.



2. Expand the **Authenticators** node, then expand the **Windows Logon v2** node.
3. Click the button next to the **Windows Logon v2** node and select **This feature will be installed on local hard drive** from the context menu**.**
4. Under the **Windows Logon v2** node, do the following:
   - If you want to install the GINA library, click the button next to the **GINA** node and select **This feature will be installed on local hard drive** from the context menu**.**
   - If you want to install the Network Provider service, click the button next to the **Network Provider** node and select **This feature will be installed on local hard drive** from the context menu**.**
5. Proceed with the remainder of the installation as described in the *Installation and Setup* guide for your version of ESSO-LM.

Migrating a WinAuth v1 Installation to WinAuth v2

To manually migrate from an existing WinAuth v1 deployment to WinAuth v2, do the following:

1. Reconfigure the First-Time Use wizard so that WinAuth v2 is the only available logon method:
    a. Start the ESSO-LM Administrative Console.
    b. In the tree in the left pane, right-click the **Global Agent Settings** node and select **Import → From Live HKLM** from the context menu.
    c. Under the "Live" settings set, navigate to **User Experience → Setup Wizard**.
    d. Select the check box next to the **Selected Authenticator** option and select **Windows v2** from the drop-down list.
    e. Save your changes locally or publish them to the repository, as applicable.

2. Using a plain text editor, create a batch (`.cmd`) file with the following content:

```
##Install WinAuth v2

<esso-lm_installer> /s /v"/qb RUNVGO="YES" ADDLOCAL="MSauth""

##Initiate primary logon method change

"<oracle_install_dir>\v-GO SSO\ssoShell.exe" /shellLoad Themes /shellLock
```

> **Note:** Substitute the full path and name of the ESSO-LM installer executable in place of `<esso-lm_sso_installer>`, as well as the full path of the directory in which Oracle ESSO products are installed for `<oracle_install_dir>`.

3. Save and close the file.
4. Run the file on the target machine.
5. When the FTU wizard appears, follow the displayed instructions to complete the migration process.

Configuring WinAuth v2 for Credential Store Key Management via Windows DPAPI

To configure WinAuth v2 for credential store key management via Windows DPAPI, complete the steps below.

> **Note:** This procedure assumes WinAuth v2 has already been installed and configured to work with your ESSO-LM deployment.

Before you begin, ensure that your environment meets the following minimum software requirements in order for secondary authentication via Windows DPAPI to function:

- **Domain controllers:** Windows Server 2003 SP1 and above.
- **Client machines running ESSO-LM:**
  - Windows XP SP2 and above
  - Windows Server 2003 SP1 and above
  - Windows Server 2008 and above
  - Windows Vista
  - Windows 7

> **Note:** Windows XP SP2 and Windows Server 2003 SP1 require *KB907247: Credential Roaming Software Update* available at http://support.microsoft.com/kb/907247.

The following Microsoft Developer Network and TechNet articles provide detailed information on Windows DPAPI and credential roaming:

- Windows Data Protection: http://msdn.microsoft.com/en-us/library/ms995355.aspx
- Credential Roaming: http://technet.microsoft.com/en-us/library/cc700815.aspx

If your environment meets the listed minimum requirements, configure WinAuth v2 to use Windows DPAPI as the secondary authentication method as follows:

1. Start the ESSO-LM Administrative Console.
2. In the tree in the left pane, right-click the **Global Agent Settings** node and select **Import → From Live HKLM** from the context menu.
3. Under the "Live" settings set, navigate to **Authentication → Windows v2**.
4. If you have previously configured ESSO-LM to use either the user's AD SID or a secure random key as a secondary authentication method, revert back to interactive passphrase by deselecting the check box next to the **Recovery Method** option. (This reverts the option to its default value, **User passphrase**.)
5. Enable Windows DPAPI for WinAuth v2. Select the check box next to the **Use Windows Data Protection (DPAPI)** option, then select **Yes** from the drop-down list.
6. Save your changes by publishing them to the repository.

7. Test your configuration. The tests below ensure proper configuration of ESSO-LM and your environment to handle credential roaming, password changes, and keyset rotation:
    a. Enroll a new user with ESSO-LM by completing the First Time Use (FTU) wizard; during enrollment, ESSO-LM will prompt for the user name and password but should not prompt to select a passphrase answer.
    b. Enroll an application with ESSO-LM and store a set of credentials for the application.
    c. Close and re-open the application. ESSO-LM should automatically respond and log you on to the application without prompting for a passphrase answer.
    d. Log out of the machine and log on to another machine as the same user. ESSO-LM should behave exactly as on the original machine, without prompting for a passphrase answer or any other extraneous information.
    e. Use the **Log on using ESSO-LM** option (accessed by right-clicking the ESSO-LM system tray icon) to confirm that application response functions as desired.
    f. Open the properties dialog for the application within the Agent and use the Reveal Password option to reveal the stored password. There should be no prompt for the passphrase answer.
    g. Change the user's Windows password before the Agent is launched, and then again while the Agent is running. There should be no prompt for the passphrase answer; stored credential should remain accessible.
    h. Log on to a third machine and confirm that stored credentials remain accessible.
    i. Test that the 90-day keyset rotation enforced by Windows DPAPI functions correctly. Advance the machine's clock, as well as the domain controller's clock, by 120 days, then log on to at least two different machines and confirm that the stored credentials remain accessible.

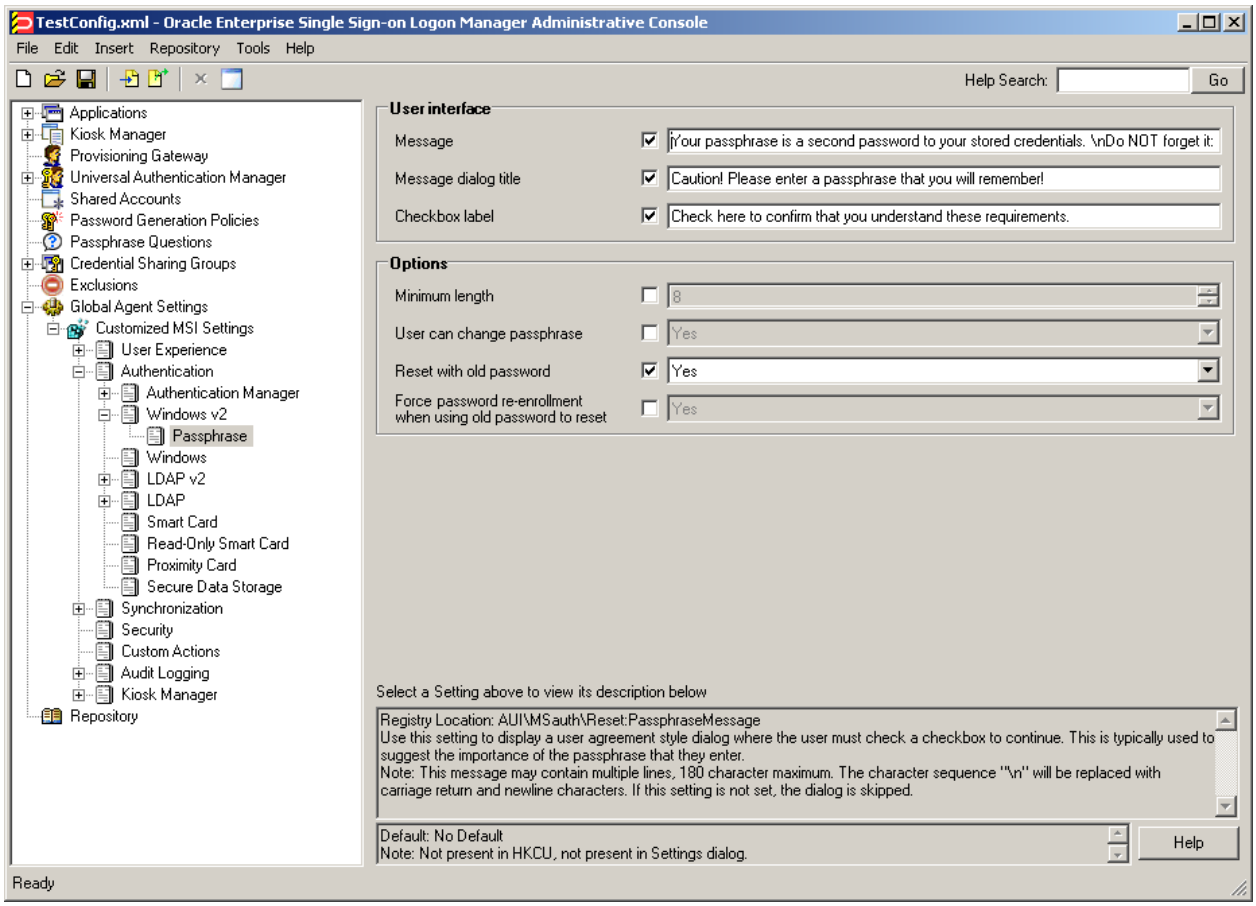
Configuring WinAuth v2 for Recovery via Interactive Passphrase Prompt

To configure WinAuth v2 for credential store key recovery via interactive passphrase prompt, simply install WinAuth v2 as described in Installing WinAuth v2. The "Recovery Method" option in the Console defaults to **User passphrase** unless manually changed.

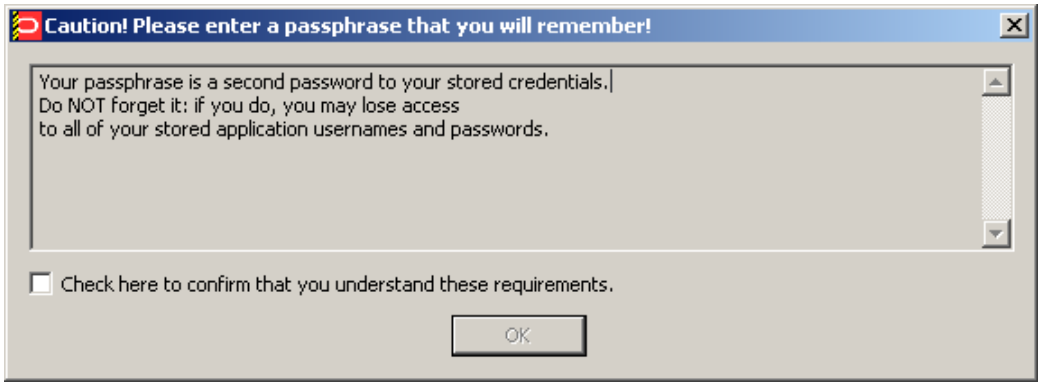
> **Note:** This procedure assumes WinAuth v2 has already been installed and configured to work with your ESSO-LM deployment.

1. Start the ESSO-LM Administrative Console.
2. In the tree in the left pane, right-click the **Global Agent Settings** node and select **Import → From Live HKLM** from the context menu.
3. Under the "Live" settings set, navigate to **Authentication → Windows v2**.
4. If you have previously configured ESSO-LM to use either the user's AD SID or a secure random key as a secondary authentication method, revert back to interactive passphrase by deselecting the check box next to the **Recovery Method** option. (This reverts the option to its default value, **User passphrase**.)
5. Configure the user warning that appears during recovery. This warning should emphasize the importance of remembering the passphrase answer:
    a. Under the "Live" settings, navigate to **Authentication → Windows v2 → Passphrase**.
    b. Select the check box next to the **Message** option and enter a message explaining the importance of remembering the passphrase answer to the user. (When filling in the fields in the steps below, use the \n character sequence to indicate a line break.) This message appears during enrollment and requires the user to check a check box and click the **OK** button in order to continue.
    c. Select the check box next to the **Message Dialog Title** option and enter the desired window title for the dialog described in step 9a above.
    d. Select the check box next to the **Checkbox Label** option and enter the desired label for the check box that appears in the dialog described in step 9a above.
    e. Select the check box next to the **Reset with old password** option and select **Yes** from the drop-down list. This option allows the user to recover access to their credential store using the old (most recent) password.
    f. Ensure that the check box next to the **Force password re-enrollment when using old password** to reset option is not selected (i.e., option is at its default value of **Yes**). This setting forces ESSO-LM to re-enroll the user when the option **Reset with old password** from step 9d is in effect, and the user has used the old (most recent) password as the passphrase answer during recovery.

For example, if you configure the warning as follows:



It will appear as follows when the user is prompted for the passphrase answer during recovery:



6. Save your changes locally or publish them to your repository, as appropriate.

Configuring WinAuth v2 for Recovery via ESSO-LM Secondary Authentication API

To configure WinAuth v2 for recovery via the ESSO-LM secondary authentication API, complete the instructions in one of the following sections.

- Recovery via Custom Secondary Authentication Library
- Recovery via a Built-In Silent Secondary Authentication Method

Recovery via Custom Secondary Authentication Library

Before starting this procedure, make sure you have done the following:

1. Written your custom secondary authentication library according to the document *Understanding the ESSO-LM Secondary Authentication API*.
2. Know your custom library's GUID and made sure that library returns that GUID to ESSO-LM via its `GetID` method.
3. Submitted your custom library file to Oracle to obtain a digital signature and received a digitally signed copy of the file back from Oracle. ESSO-LM will not load the custom file without a valid digital signature.

To configure WinAuth v2 for recovery via custom secondary authentication library, do the following:

1. Start the ESSO-LM Administrative Console.
2. In the tree in the left pane, right-click the **Global Agent Settings** node and select **Import → From Live HKLM** from the context menu.
3. Under the "Live" settings set, navigate to **Authentication → Windows v2**.
   If you have previously configured ESSO-LM to use either the user's AD SID or a secure random key as a secondary authentication method, revert back to interactive passphrase by deselecting the check box next to the **Recovery Method** option. (This reverts the option to its default value, **User passphrase**.)
4. Create a directory named identically to the GUID of your custom library in the following directory:
   `<oracle_install_dir>\v-GO SSO\AUI\Recovery\`

   Note: Substitute the full path of the directory in which Oracle ESSO products are installed for `<oracle_install_dir>`.

   For example, if your library's GUID is `{B623C4E7-A383-4194-A719-7B17D074A70F}`, you would create the following directory:

   ```
   <oracle_install_dir>\v-GO SSO\AUI\Recovery\{B623C4E7-A383-4194-A719-7B17D074A70F}
   ```

5. Place your custom library file in the directory you created in step 4.

6. Add a GUID entry to ESSO-LM's secondary authentication methods list for your custom library.
    a. Create a key named identically to the GUID of your custom library under the following registry location:
        - On 32-bit systems:
          `HKEY_LOCAL_MACHINE\Software\Passlogix\AUI\MsAuth\RecoveryMethods\`
        - On 64-bit systems:
          `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Passlogix\AUI\MsAuth\RecoveryMethods\`

        For example, if your library's GUID is `{B623C4E7-A383-4194-A719-7B17D074A70F}`, you will create the following key on a 32-bit system:

        ```
        HKEY_LOCAL_MACHINE\Software\Passlogix\AUI\MsAuth\RecoveryMethods\
        {B623C4E7-A383-4194-A719-7B17D074A70F}
        ```

    b. Under the key you created in step 6a, create a string value named `Path` and set it to the full path and file name of your custom library. In our example, you would set it to:

        ```
        <oracle_install_dir>\v-GO SSO\AUI\Recovery\{B623C4E7-A383-4194-
        A719-7B17D074A70F}\<MyCustomLibrary.dll>
        ```

        Where `<oracle_install_dir>` is the full path of the directory in which Oracle ESSO products are installed and `<MyCustomLibrary.dll>` is the file name of your custom library.

7. Set ESSO-LM's recovery method to your custom secondary authentication library.
   If it does not already exist, create a string value named `ResetMethodGUID` under `HKEY_LOCAL_MACHINE\Software\Passlogix\AUI\MsAuth\RecoveryMethods\` and set it to the GUID of your custom library.
8. Reinitialize the WinAuth v2 settings with the newly selected configuration:
    a. Launch ESSO-LM, double-click its system tray icon, and select **Settings** in the left-hand pane of the window that appears.
    b. Select the **Authentication** tab, then click **Change**. The Setup Wizard appears.
    c. Follow the prompts in the wizard. When prompted to select your primary logon method, make sure that **Windows Logon v2** remains selected.
    d. Complete the remaining steps in the wizard.

Recovery via a Built-In Silent Secondary Authentication Method

To configure WinAuth v2 for recovery via one of ESSO-LM's built in silent secondary authentication methods, do the following:

1. Start the ESSO-LM Administrative Console.
2. In the tree in the left pane, right-click the **Global Agent Settings** node and select **Import → From Live HKLM** from the context menu.
3. Under the "Live" settings set, navigate to **Authentication → Windows v2**.
4. Select the check box next to the Recovery Method option and do one of the following:
    - To use the user's AD SID for silent secondary authentication, select **Passphrase suppression using user's SID** from the drop-down list
    - To use a secure random key for silent secondary authentication, select **Passphrase suppression using secure key** from the drop-down list
5. Save your changes locally or publish them to the repository, as applicable.

Resetting the User-Provided Passphrase Answer

To force a user to provide a new passphrase answer based on new passphrase questions, do the following as a user with administrative privileges:

1. Using the ESSO-LM Administrative Console, do the following:
    a. Disable existing questions that are no longer desired.
    b. Add the new questions.
2. For each user, perform the following steps on the target machine as the target user:
    a. Delete the following registry key and its contents:
    `HKEY_CURRENT_USER\Software\PassLogix\AUI\msauth\ResetMethods`
    b. Execute the following command:
    `<oracle_install_dir>\v-GO SSO\ssoshell.exe /forceverify now`

> **Note:** Substitute the full path of the directory in which Oracle ESSO products are installed for `<oracle_install_dir>`.

When automating the above steps, Oracle highly recommends that you:

- Create a script to manage the process
- Provide end-user instructions that explain what is happening
- Include a logging capability that centrally records the success or failure of each step, including:
    - Script launch
    - Old registry key deletion
    - New registry key creation
    - Passphrase answer entry by user
- Include reporting capability to audit recorded data for users who have successfully completed passphrase answer change
- Once all users have completed the change, delete the unwanted passphrase questions.

Enabling WinAuth v2 Strong Authentication Device Support

Note: The following instructions apply to Windows Vista and Windows 7 only.

If you are planning to use strong authentication devices, such as SmartCards, to authenticate to Windows Vista or Windows 7, you must configure Windows to permit the hand-off of strong authentication events to third-party credential providers, such as ESSO-LM deployed with WinAuth v2. Otherwise, ESSO-LM will not be able to communicate with the device and you will not be able to authenticate to ESSO-LM.

To do so, complete the following steps:

1. Launch the Windows registry editor and navigate to the following path:

   ```
   HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion\
    Winlogon\Notify
   ```

2. Under the above key, create a `DWORD` value named `SmartCardLogonNotify`.
3. Set the above value to `1`.
4. Restart the machine.