Oracle® Enterprise Single Sign-on
Logon Manager

How-To: Understanding the ESSO-LM Secondary Authentication API

Release 11.1.1.2.0

20415-01

ORACLE®

Oracle Enterprise Single Sign-on Logon Manager How-To: Understanding the ESSO-LM Secondary Authentication API

Release 11.1.1.2.0

20415-01

Table of Contents

Introduction

About This Guide

This document describes the ESSO-LM Secondary Authentication API. The API allows you programmatically supply the passphrase answer to the `MSAuth` (Windows Authenticator v2) authenticator.

Prerequisites

Readers of this document should have a thorough understanding of software development using the Microsoft .NET framework, including the Component Object Model (COM) technology, and related concepts.

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
Agent	ESSO-LM client-side software
Console	ESSO-LM Administrative Console
WinAuth v2	Windows Authenticator Version 2

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/E15624_01/index.htm.

Understanding the ESSO-LM Secondary Authentication API

Overview

The secondary authentication API allows a third party application to programmatically supply a passphrase to the Windows Authenticator v2 (a.k.a. `MSAuth`) during an authentication session. This eliminates the need for interaction with the user and automates the authentication process.

The API consists of the following functions:

- **`SecondaryAuthKey`** – allocates the passphrase answer buffer, fills the buffer with the passphrase answer, and returns a pointer to the answer buffer.
- **`FreeSecondaryAuthKey`** – clears the answer buffer once the answer is no longer needed by third party code.

Note: The custom secondary authentication library must be validated and digitally signed by Oracle; otherwise, it will not be accepted by ESSO-LM. For assistance with this process, please contact Oracle Support.

The SecondaryAuthKey Method

This method is used to obtain the user's passphrase answer (the user's SID) and store it in memory at a specified address for later retrieval.

```
BOOL SecondaryAuthKey( LPBYTE* pbAnswer, LPDWORD pdwSize )
{
	BOOL fRetVal = FALSE;

	// check for invalid parameters
	if ( NULL != pbAnswer )
	{
		// obtain user's SID - it will be used as passphrase answer
		CSid sid;
		CString strSid( sid.Sid() );

		// allocate the memory buffer
		LPBYTE pByte = new BYTE[strSid.GetLength() + 1];

		// copy the SID to the buffer
		::memcpy( pByte, strSid.GetBuffer(), strSid.GetLength() );

		// save the address of the buffer to the passed pointer
		*pbAnswer = pByte;

		// save the size of the buffer to the passed pointer
		if ( NULL != pdwSize )
		{
			*pdwSize = strSid.GetLength() + 1;
		}

		// set successful return code
		fRetVal = TRUE;
	}

	return fRetVal;
}
```

The FreeSecondaryAuthKey Method

This method is used to clear the passphrase answer buffer after `SecondaryAuthKey` has been successfully called.

```
void FreeSecondaryAuthKey( LPBYTE pbAnswer )
{
	// free the memory buffer
	delete[] pbAnswer;
}
```

Example Implementation

Below is an example of using the secondary authentication API to programmatically supply the passphrase answer to the authenticator.

```
BOOL CResetDlg::SecondaryAuth( LPCTSTR pszDllPath )
{
	BOOL fRetVal = FALSE;

	// load SecondaryAuth.dll
	HMODULE hSecondaryAuth = LoadLibrary( pszDllPath );

	If ( NULL != hSecondaryAuth )
	{
		SECONDARYAUTHKEY pfnSecondaryAuthKey = (SECONDARYAUTHKEY)
		GetProcAddress( hSecondaryAuth, "SecondaryAuthKey" );
		if ( NULL != pfnSecondaryAuthKey )
		{
			LPBYTE pbByte = NULL;
			DWORD dwAnswerSize = 0;

			// call SecondaryAuthKey to get the passphrase answer
			BOOL bAnswerResult = pfnSecondaryAuthKey( &pbByte,
			&dwAnswerSize );

			// use the returned answer – pbByte
			// ...

			// call FreeSecondaryAuthKey to let the library free the
			memory
			FREESECONDARYAUTHKEY pfnFreeSecondaryAuthKey =
			(FREESECONDARYAUTHKEY) GetProcAddress( hSecondaryAuth,
			"FreeSecondaryAuthKey" );
			if ( NULL != pfnFreeSecondaryAuthKey )
			{
				pfnFreeSecondaryAuthKey( pbByte );
			}

			// set successful return code
			fRetVal = TRUE;
		}

		// unload SecondaryAuth.dll
		FreeLibrary( hSecondaryAuth );
	}

	return fRetVal;
}
```

Switching Secondary Authentication Methods

You have the ability to change the method used by Windows Authenticator v2 (WinAuth v2) to verify the user's identity to another method if necessary. The following scenarios are supported:

- WinAuth v2 built-in passphrase support to external secondary authentication
- External secondary authentication → WinAuth v2 built-in passphrase support
- One external secondary authentication library to another

Switching from WinAuth v2 Built-In Passphrase Support to External Secondary Authentication

If you are currently using the built-in passphrase support of WinAuth v2 and want to use secondary authentication, do the following:

1. Disable the built-in passphrase support of WinAuth v2:
   a. Run the ESSO-LM installer.
   b. In the tree, navigate to **Logon Methods → Windows Logon v2**.
   c. Click **Passphrase Suppression** and select **This feature will be installed on the local hard drive**.
   d. Click **Next** and follow the installer prompts to complete the installation.
   e. If you want to use a custom secondary authentication library, place your custom `secondaryauth.dll` file in the following path (overwrite the original file when prompted):

      ```
      C:\Program Files\Passlogix\AUI\MSAuth\<GUID>\
      ```

      Note: Make a backup of the Oracle-supplied `secondaryauth.dll` file in case you want to revert to it at a later date.

2. 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.

Switching from External Secondary Authentication to WinAuth v2 Built-In Passphrase Support

If you are currently using secondary authentication and want to use the built-in passphrase support of WinAuth v2, do the following:

1. Enable the built-in passphrase support of WinAuth v2:
   a. Run the ESSO-LM installer.
   b. In the tree, navigate to **Logon Methods** → **Windows Logon v2**.
   c. Click **Passphrase Suppression** and select **This feature will not be available**.
   d. Click **Next** and follow the installer prompts to complete the installation.
2. 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.

Switching from One External Secondary Authentication Library to Another

If you are currently using an external secondary authentication and want to switch to a different library, do the following:

1. Replace your current secondary authentication library with the new library. Place your new `secondaryauth.dll` file in the following path (overwrite the original file when prompted):

   ```
   C:\Program Files\Passlogix\AUI\MSAuth\<GUID>\
   ```

   Note: Make a backup of your original `secondaryauth.dll` file in case you want to revert to it at a later date.

2. 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.