Oracle® Enterprise Single Sign-on Suite Plus

Release Notes

Release 11.1.1.5.0

E21025-01

March 2011

ORACLE®

Oracle Enterprise Single Sign-on Suite Plus Release Notes, Release 11.1.1.5.0

E21025-01

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Table of Contents

Abbreviations and Terminology

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

Abbreviation or Term	Full Name
Bio API	Biometric Application Programming Interface
BSP	Biometric Service Provider
FTU	First Time Use Wizard
Microsoft AD	Microsoft Active Directory
Microsoft ADAM	Microsoft Active Directory Application Mode
LDAP	Lightweight Directory Access Protocol
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

About Oracle Enterprise Single Sign-on Suite Plus

Oracle® is releasing version 11.1.1.5.0 of Oracle Enterprise Single Sign-on Suite Plus. These release notes provide important information about this release. The information in this document supplements and supersedes information in the related product documents.

Oracle Enterprise Single Sign-on Suite Plus Installation and Upgrade Notes

If you currently have multiple components of the suite installed together, you must upgrade all components to this version. Older versions of components may not work properly with version 11.1.1.5.0. Consider the following as you plan your installations:

- You must install ESSO-LM prior to installing any other component.
- If you have a previous version of Kiosk Manager installed and are updating it with the ESSO-LM Agent, you must first uninstall the previous Kiosk Manager using the **Control Panel Add/Remove Program** or the **Uninstall** option of the earlier software installer.
- For components containing both a server and client:
    - Always keep server and client versions in sync; be sure to upgrade both.
    - Always upgrade the server component first, then the client component.

Refer to the individual components' installation and deployment guides for more detailed information. See "Product Documentation and Support" on page 46 for a list of all documentation that supports this suite.

What's New in Oracle Enterprise Single Sign-on Suite Plus 11.1.1.5.0

A number of features and improvements have been incorporated into Oracle Enterprise Single Sign-on Suite Plus 11.1.1.5.0. This section describes these additions, by component.

For more information on these features and settings, see the Oracle online documentation center and the online help systems for each suite component.

Addition of Oracle Enterprise Single Sign-on Universal Authentication Manager Component to Suite

A new component has been added to Oracle Enterprise Single Sign-on Suite Plus, the Universal Authentication Manager (ESSO-UAM) component. ESSO-UAM enables enterprises to replace the use of native password logon to Microsoft Windows and Active Directory networks with stronger and easier to use authentication methods. The ESSO-UAM system also enhances enterprise security beyond traditional password authentication by providing two-factor authentication methods. ESSO-UAM enables users to rapidly and securely enroll credentials that will be used to identify and authenticate them. ESSO-UAM offers built-in and configurable authentication methods: smart cards, passive proximity cards, biometric fingerprint, and other biometric technologies compatible with the BioAPI standard. Native Windows Passwords are also supported.

Smart Cards

A smart card is a credit card-sized token containing a chip or embedded circuits that can store and process data securely. Information stored on a smart card can also be used for identification and authentication. ESSO-UAM enables enrolling and using smart cards for user logon and authentication without writing any data on a smart card chip. ESSO-UAM also supports the option to require a smart card PIN during logon to provide stronger two-factor authentication.

Proximity Cards

A passive proximity card or token is an identity object (such as a workplace ID badge) containing a circuit that a card-reading device can detect and decipher. When the proximity card is placed in close proximity to a reader, the reader detects the token’s presence and recognizes identifying information that is associated with a specific user. This ESSO-UAM method includes the option to require a user to enroll a PIN that is associated with a proximity token enabling two-factor authentication. When so configured, ESSO-UAM prompts the user for the enrolled PIN associated with a token during logon, strengthening user authentication.

Biometrics

The Fingerprint Logon Method supports the use of numerous external and embedded laptop biometric fingerprint devices to provide a convenient and secure fingerprint authentication mechanism to ESSO-UAM.

The BioAPI Logon Method leverages the BioAPI framework , thus enabling support of almost any third-party BioAPI-compliant Biometric Service Provider (BSP) module. In addition to fingerprint biometrics, this logon method can also support other biometric technologies that offer a BioAPI compatible BSP such as palm, facial, and iris recognition solutions.

ESSO-UAM Administration

ESSO-UAM leverages the ESSO-LM Administrative Console to configure a supported central repository to store and manage policies, users, and user groups. The ESSO-LM Administrative Console contains ESSO-UAM settings that allow administrators to configure policies; these policies specify how authentication operates for different users and user groups. When you edit and publish a policy, the changes are applied to domain user accounts running in Enterprise mode each time the Client synchronizes with the repository, guaranteeing that the most up-to-date policies are enforced.

ESSO-LM Enhancements

Installation Wizard

The ESSO-LM Installation Wizard has a new, intuitive flow that offers a Q&A-type, guided installation as an alternative to the traditional feature selection method. The option to install Kiosk Manager is now also a part of the ESSO-LM installer.

ESSO-LM Agent

The following capabilities have been added to the Agent.

Ability to Select Multiple Items in the My Accounts List

Users can now use the standard Shift-Click (for adjacent items) or Ctrl-Click (for non-adjacent items) methods to delete multiple items in the My Accounts list.

Silent Credential Capture

ESSO-LM can now be configured to capture users' credentials as they enter them, the first time they encounter an application. You can specify whether to inform the user and ask to confirm the credentials, or make the capture completely transparent.

Support for Multiple Monitor Environments

ESSO-LM dialog box positioning now conforms to multiple monitor layouts.

ESSO-LM Administrative Console

The following capabilities have been added to the ESSO-LM Administrative Console.

General Administrative Tasks

Reorganization of Global Agent Settings

The Global Agent Settings layout has received a complete redesign. Screens have been consolidated and reorganized to make configuration simpler; some screens and settings have been renamed, some settings' default have changed, and some settings have been removed. The new *ESSO-LM Global Agent Settings Reference Guide* lists all the changes and current setting information.

Enhanced MSI Generator

The enhanced MSI Generator eliminates reliance on third-party software and offers administrators a fully-integrated, end-to-end MSI Wizard.

Kiosk Manager Events Captured for Reporting

ESSO-LM now captures Kiosk Manager event information and sends it to the SSO Reporting Service. Reports can be manually generated using these event records.

Template Creation

Simplified Template Creation

Administrators can now initiate template creation from a selection in the title bar button menu. The form can be completely new or an addition to an existing template.

Template Test Manager

Administrators can now validate templates that they have created, before publishing them. The Template Test Manager engages the Agent directly, bypassing the repository and synchronization. The manager guides you through the test, prompting you to take action at various points, and asking questions about the results in order to determine how to proceed.

Configuration Test Manager

Administrators can now validate Global Agent Settings configurations that they have created, before deploying them. The Configuration Test Manager provides a step-by-step procedure to select a Global Agent Settings set and verify that all repository and synchronization tasks function properly. *(This manager supports Active Directory only.)*

SendKeys Capability for Web Application Templates

It is now possible to configure Web application templates using SendKeys to simulate keystrokes for Web page navigation in the same way as is possible for Windows applications.

Form Awareness of Logon Loop Grace Period

Administrators can now configure individual forms of a template to adhere to the logon loop grace period specified on the Miscellaneous tab of a selected template.

Bypass Logon Chooser Setting for Logon Forms

The "Bypass Logon Chooser" setting, which configured the Agent to select the last credentials used automatically, previously applied only to Password Change forms. Administrators now have the option to apply this setting to Logon forms also.

Ignored Java Versions Based on Vendors

A new Global Agent Setting allows the administrator to configure the Agent to ignore the Java version of specific vendor(s).

Form-Based Settings for Auto-Submit and Auto-Recognize

Auto-Submit and Auto-Recognize can now be configured to apply to specific forms instead of across all the forms of a template.

New Form Types for Logon Success and Failure Screens

In order to enhance the usability of the Retry Logon Error Loop and to implement the Silent Credential Capture feature, two new form types, Logon Success and Logon Failure, have been created. The Logon Failure form eliminates the need for the Agent to wait for the maximum time or attempts before displaying the Retry Logon Error Loop; and Silent Credential Capture requires a way to verify that the credentials that the user enters are correct before saving them.

Window Title Matching for Mainframe Applications

In order to alleviate the problem of host/mainframe emulator sessions that do not have any unique characteristics within their screens to differentiate one from another, ESSO-LM now has the ability to identify each session using the emulator's window title.

IMG Tag Support

ESSO-LM now recognizes IMG tags when parsing Web pages, making it possible for an IMG element with a Submit event script to perform the submission as programmed. The IMG can be an independent element or embedded in an anchor tab.

Ability to Inject Data Fields Multiple Times on the Same Form

ESSO-LM now supports injection of the same data into multiple fields on one form, as when the user must enter and confirm a password, or enter the same information in different places on the same Web page.

Support for Windows 7 Authentication Dialog Boxes

The ESSO-LM Administrative Console is now capable of reading the controls in Internet Explorer 8 pop-up authentication dialog boxes with 256-bit encryption, thus enabling creation of templates or on-the-fly pop-ups that use this technology.

Fallback to SendKeys Setting Made Optional

Administrators now have the option to restrict applications from falling back to SendKeys when direct credential injection fails. Fallback was previously the default behavior, with no option of turning it off. It is configurable per-form and as a Global Agent Setting, and is available only for Windows applications.

Synchronization

ADAM Synchronization Error Messages

ADAM Synchronization error messages now match the message scheme of Active Directory Synchronization error messages. These settings are configured on their respective Global Agent Settings Synchronization screens.

User Management

Application Username Exclusions

The ESSO-LM Administrative Console now contains an "Exclusion" object that identifies sets of usernames prohibited from being added to an ESSO-LM account. This feature is designed for use in scenarios for which you want *some*, but not *all*, usernames excluded from an application.

Repository Tree Node Filtering

To facilitate viewing repositories with many nodes within the ESSO-LM Administrative Console, Administrators can now filter or truncate lists in the nodes of the Repository tree for the following views:

- Repository View
- Browse for Repository
- Select Search Base
- Add Locator Object

Ability to Move Users Between OUs in LDAP Directories

ESSO-LM no longer displays an error message if an administrator moves a user from one LDAP OU to another since the last synchronization. The Agent searches the directory for the user who is attempting to log on, and displays an authentication dialog box if the user is not found.

Field-Based Sharing for Credential Sharing Groups

Administrators can now designate one credential field as the key field, so that they can target certain accounts to change. Updates will occur only for the accounts in a Credential Sharing Group that have the information in that key field in common.

Option to Pre-Fill Shared Fields for Applications in a Credential Sharing Group

ESSO-LM is configurable to pre-fill shared fields for applications in a Credential Sharing Group. Administrators can designate which fields to pre-fill on a per-group basis. Non-shared fields will remain open for manual entry.

Automatic Account Creation When All Fields Are Predetermined

ESSO-LM now creates a new account automatically when the user encounters an application that the administrator has configured as a member of a Credential Sharing Group that has all fields predetermined.

Configurable User Setting to Opt Out of a Credential Sharing Group

Administrators can configure the presence of the "Exclude from Credential Sharing Groups" checkbox in the New Logon dialog box, thereby controlling whether users have this choice.

Application Support

- Hummingbird HostExplorer 2008 version 13
- Lotus Notes 8.5
- Lotus Notes 7

Operating System Support

ESSO-LM has added support for the following operating systems:

- Windows Server 2008 R2 64-bit

Browser Support

- Mozilla Firefox 3.6

ESSO-PG Enhancements

Operating System Support

ESSO-PG has added support for the following operating systems:

- Support for Windows Server 2008 R2

ESSO-Anywhere Enhancements

Operating System Support

ESSO-Anywhere has added support for the following operating systems:

- Microsoft Windows XP SP3
- Microsoft Windows Vista Business Edition SP1
- Microsoft Windows Server 2003 SP2
- Microsoft Windows Server 2003 64-bit
- Microsoft Windows Server 2008 R2
- Microsoft Windows 7 32- and 64-bit

Oracle Enterprise Single Sign-on Suite Plus Reporting Enhancements

Operating System Support

- Microsoft Windows Server 2003 64-bit
- Microsoft Windows Server 2008 64-bit
- Microsoft Windows Server 2008 R2

Repository Support

- MS SQL 2008 R2

Support for Oracle Database version 11g

Reporting now supports Oracle Database. Reports may be manually generated by querying the Oracle Database. The Oracle Database is not accessible through the Reporting Administrative Console.

ESSO-PR Enhancements

ESSO-PR Events Captured for Reporting

ESSO-PR now captures event information and sends it to the SSO Reporting Service. Reports can be manually generated using these event records.For more information about using Reporting, see the Oracle online documentation center.

Operating System Support

- Microsoft Windows 7 64-bit
- Microsoft Windows Windows Server 2008 SP2
- (Client) Microsoft Windows Windows Vista 64-bit
- (Client) Microsoft Windows Server 2008 64-bit
- Microsoft Windows Server 2008 R2

Repository Support

- MS SQL 2005
- MS SQL 2008

What's Changed in Oracle Enterprise Single Sign-on Suite Plus 11.1.1.5.0

A number of changes have been incorporated into Oracle Enterprise Single Sign-on Suite Plus 11.1.1.5.0. This section describes these changes.

For more information, see the Oracle online documentation center and the online help systems for each suite component.

ESSO-LM

.NET Requirements

The ESSO-LM Administrative Console version 11.1.1.5.0 requires .NET 4.0.

Expanded Documentation Suite

The Oracle Enterprise Single Sign-on Suite Plus document suite now includes several new guides and a Best Practice series that discusses in detail all major administrative tasks required for optimal software performance. See the Documentation and Support section for a complete list of the guides that support the suite.

Global Agent Settings Changes

Several Global Agent Settings have been renamed or moved, and some default settings have changed. Refer to the new *ESSO-LM Global Agent Settings Reference Guide* for complete information.

Passphrase Suppression Option Moved

The Windows Authentication v2 Passphrase Suppression option has moved from an Installation Wizard selection to a setting in the ESSO-LM Administrative Console. Refer to the *ESSO-LM Installation and Setup Guide* for the procedure to customize passphrase suppression.

ESSO-PR

Excluding Users from Forced Enrollment

The Enrollment Exclusion feature has been removed from the ESSO-PR Management Console and replaced with a simpler method to accomplish exclusions. Refer to the *ESSO-PR Administrator's Guide* and ESSO-PR Management Console help system for information about the new procedure.

ESSO-PR Server EnrollmentClient Web Application

The authentication method for the ESSO-PR Server's EnrollmentClient Web application has been changed from Integrated Windows Authentication to Digest Authentication. This causes Internet Explorer to require that end users enter their Active Directory credentials before permitting them access to the Enrollment Interview.

Resolved Issues

The following table describes issues that were reported in earlier releases of ESSO-LM and have been resolved in this release

Tracking Number	Description of Issue
Bug 8599446, s7201, a14978	Users were prompted to re-authenticate repeatedly when creating or deleting application credentials in the Agent.
Bug 8627596, s7269, a14972	The Spanish language pack contained an error in the text of the password change failure dialog box.
Bug 8690723, s7348, a14880	LDAP v1 authentication did not function correctly against Novell eDirectory when a multiple level LDAP repository was set up.
Bug 8761059, s7439, a14714	Using Windows Server 2003, an attempt to create a backup (.bkv) file resulted in an error message with an overwrite warning. When the user selected not to overwrite, the Agent terminated.
Bug 8823726, s7501, a14976	The setting "Do not store user data on disk file" did not clear all local data for standard users.
Bug 8937400, s7493, s7654, s7691, s7750, a14934	The Agent caused Microsoft Outlook and Internet Explorer to cease responding.
Bug 9017095, s4499, s6296, s6685, s7487, s7654, s7733, s7751, s7778, s7934, s8203, a14953	The ssobho.exe caused Internet Explorer to drop keystrokes.
Bug 9110039, s7923, a14787	Internet Explorer 7 exhibited intermittent, unexpected terminations with the Agent running.
Bug 9289067, s7986, s8230, s8484, s8536, s8759, a15257	PuTTY support has been enhanced with an improved copy/paste functionality.
Bug 9432369, s8477, a15654	Windows Authentication v2 prompted the user to authenticate to an application on Citrix after the user changed a password with ESSO-PG installed.
Bug 9433551, s8933, s8935, s8936, s8941, s8942, s8950, aa15952	There were several errors in the Japanese localization of the Agent interface.
Bug 9586004, s7789, s8951 14716	During a password change, the password constraints window did not resize to accommodate all settings in the policy.
Bug 10277355, s10450, a17134	ESSO-LM failed to report an error and corrupted the aelist when the entlist.ini was unwritable.
Bug 10381832, a17073	The specified custom image for authentication prompt did not appear in the authentication prompt.
s2654, s4433, s5238, s6334, a14139	The Agent was unable to inject the same credentials several times on a single form.
s5357, a15668	The Windows GINA lost focus in a Citrix desktop session in certain environments.
s6280, s6956, a15074	An error occurred using certain printers with Win3270 Client.

Tracking Number	Description of Issue
s6492, a15050	The ESSO-LM Administrative Console could not open saved XML files when session actions were configured.
s6680, a14981	Synchronization failed for users with access over a VPN.
s6684 a14979	The Agent occasionally failed to log on to Web applications accessed through a hyperlink using Internet Explorer 7.0.
s6737, a15053	The New Logon dialog box did not populate the third or fourth fields with application data from a Web drop-down menu when multiple forms were used within the same template.
s6837, a14848	The position of the Submit button for a dynamic Web page was not in a fixed location.
s7218, a14851	Users were unable to open a new tab in Internet Explorer 8 when the Agent detected a logon and users selected to cancel the prompt.
s7219, a14863, a15320	The Agent occasionally ceased responding when using Microsoft Windows Vista.
s7222, a14928	The Agent occasionally ceased functioning after the workstation resumed from a low-power state.
s7242, a15601	ESSO-LM has added support for LDAP Authentication over Microsoft IAG VPN.
s7244	The French language pack contained an error in the text of the New Logon dialog box.
s7260, a14873	The Agent carried the User ID field to a new application in a Credential Sharing Group that shared only the password field.
s7379	Starting or stopping the SSO Sens Server was being logged as an event.
s7404, a14881	The Agent was unable to complete a password change due to the presence of a pop-up window.
s7440, a14622	When Internet Explorer was not the active window as the Agent populated the window's credential fields, the Agent did not auto submit the credentials.
s7445, a14980	An access violation occurred in ssoJHO.dll using the Lotus Notes DMS plug-in.
s7480 14717	Synchronization was delayed when using ADAM with a virtual name.
s7504, a14931	The Agent did not respond to a Web application, both automatically and after the user selected "Logon using ESSO-LM" from the system tray and title bar button menus.
s7522, a14798	Setting the Logon Loop Grace Period to "Silent" interfered with or prevented a password change.
s7584, a17003	Caching credentials did not work properly when used for multiple Windows accounts on the same workstation.
s7597, s7854, a15412	The SSO GINA caused some workstation systems to cease operating, resulting in a blue screen and requiring a system restart.
s7639, a14860	The Windows password change was updating an excluded Domain's Credential Sharing Group password.

Tracking Number	Description of Issue
s7722, a14712	The Agent did not respond to a Web application until the user restarted.
s7736, a15181	SendKeys incorrectly processed Up/Down commands for CTRL and SHIFT.
s7745, a16318	Kiosk Manager did not open multiple sessions if "Track Memory Consumption" was set to a value other than zero.
s7796, s8087, a14997	The SendKeys option, "Click on coordinates set relative to active window," functioned incorrectly.
s7797, a15478	The Agent did not respond to a Web page using Internet Explorer.
s7810	It was not possible to configure the ability to exclude accounts from Credential Sharing Groups during initial credential capture.
s7818, a14730	The Agent responded intermittently to a scrolling console host application.
s7828, a15119	The Agent did not respond to password changes in an SAP application.
s7831, a17002	It was possible for a user to terminate Kiosk Manager if the Agent took an excessive time to display its user interface.
s7856, a15250	The Agent responded incorrectly, by locking templates, to LDAP error messages.
s7900, a14558	The userinit setting in the registry changed, causing it to disregard previous settings.
s7977	The ESSO-LM Administrative Console documentation had insufficient information about the Credential Sharing Group settings.
s7998, a15040	ESSO-LM hooks caused some applications to terminate unexpectedly.
s8040	The Agent entered credentials in the wrong field of a scrolling-screen emulator when the cursor location changed.
s8041	The Agent incorrectly passed the username from an existing account to a new account in a credential sharing group.
s8054, a14810	Products and modules that were dependent on support6.dll ceased functioning after the DLL was removed.
s8071, a14954	The Agent displayed an unknown software exception error. This error usually specified ssomho.exe, but occasionally specified either ssobho.exe or ssomozho.exe.
s8106, a15157	The New Logon window displayed a cleared password field and an incorrect third field if the user advanced to the next screen and then reverted back to make a change.
s8124, a15336	Network Provider did not receive Windows logon notification when a Smart Card was used to log on.
s8145, a16541, a17005	The logging method was changed from File to Event Tracing, which is more space-efficient and flexible.
s8194, a15417	The "EventServer" administrative override did not log events to the server.

Tracking Number	Description of Issue
s8206, s8352, a17004	Some Kiosk Manager session state lists did not execute correctly.
s8234, s8514, s8555, s8583, s7815	The Agent did not respond to a Web application using a DIV tag as a "Submit" button.
s8257, a15302	The notification service library did not link with third-party modules.
s8356, s8443, s8444, a17006	Kiosk Manager caused incorrect behavior in some applications.
s8363, a17012	Kiosk Manager dropped the entered domain name when the ESSO-LM Active Directory synchronization prompt was pre-populated.
s8454, a16079	Clipboard data that the user did not clear after logging off from Kiosk Manager was available to the next user.
s8483, a16340	The Retry Logon dialog box did not appear after a failed logon attempt for a Web application.
s8497, a15759	The inmemshr.dll quit unexpectedly, causing the Agent to cease responding.
s8524, s8457, a16129	The ESSO-LM Administrative Console help has been updated to reflect the latest MSI package contents.
s8541, s8638, a15748	WinAuth2 did not permit users to enroll with the "access this computer from network" permission disabled.
s8557	When the Reporting tool was running for one SAP application, the Agent did not respond to a second SAP application instance. The lack of response continued until the SAP helper process was terminated in Task Manager. Other applications were not affected.
s8637, a16835	The Agent ceased responding or went into a loop while creating new application credentials.
s8651, a16450	The Agent did not respond to minimized windows when the windows were opened before the Agent started, or when using the "Log On Using ESSO-LM" menu selection.
s8689, a15954	It was not possible to add applications in a Domain Sharing Group on a kiosk workstation.
s8773, a16288	The Agent caused multiple instances of Attachmate Extra! to launch even when the application was not in use.
s8901, a15728	A published application was not available for all users.
s8932, s8949, a15857	The Agent installer messages for the Japanese language pack were incomplete and contained some translation errors.
s8934, a16368	An ESSO-LM 10.1.4.1.0 template stopped submitting after Fix Pack 4 was applied.
s8953	The Agent responded multiple times to an application, resulting in the appearance of an error message.
s8955, a16444	Kiosk Manager users received the ESSO-LM error message, "Failed to log on to directory."
s8987, a16252	The Agent failed to recognize a third field that was configured as a drop-down box in the application template. Instead it recognized the third field as a text box.

Tracking Number	Description of Issue
s9000, s9051, a16234	The Agent did not respond to applications whose templates were configured with a blank window title or a regular expression.
s9053, a17000	A workstation running the Agent and Kiosk Manager ceased responding and required restarting.
s9193, a16239	A Windows template was unable to submit credentials when the "Submit" button was not a direct child of the main window.
s9385, a16213	SSOSensSrv.exe caused a 30-40 second startup delay.
s9425, a16441	It was not possible to bring some applications to template in the ESSO-LM Administrative Console from the repository. It was also not possible to import a .INI file with this template back to the ESSO-LM Administrative Console.
s9576, a16390	The ESSO-LM Administrative Console help contained an incorrect description for SSL in ADSync parameter.
s9609, a16334	The ESSO-LM Administrative Console help contained errors in the Password Change tab for a Selected Application topic.
s9637, a16389	The ESSO-LM Administrative Console help was missing information on the use of the Event Logging Database Fields.
s9682 a16916	It was not possible to create a Password Change template for a Web site that was implemented with DIV tags.
s9687, a16635	Auto-Submission did not work for Web applications when there was no Submit control in the template.
s9907, a16999	Kiosk Manager logged users on without prompting them for a password.
s10236, a16951	Japanese characters appeared garbled for an application.
s10254, a16831	A search error during ADAMsynchronization caused the synchronizer to hang.
s10272, a16864	The description of the "Location of entlist.ini file" parameter has been updated.
s10654, a17099	The ADAM synchronization "Change expired Windows password" feature caused the Agent's synchronization process to take longer than needed.
s10671, a17326	The Agent did not respond to Web pages using Internet Explorer 32-bit when running in Windows 7 64-bit and Windows Vista environments.
a14253	The ESSO-LM Administrative Console did not save the "4th Field Label" setting of an RSA SecurID application template in XML-file.
a14358	Users could not complete the First Time Use wizard when using multiple synchronizers.
a14433	The Agent required 20 seconds to load with User Account Control (UAC) enabled.
a14453	Resizing the Web Form Wizard caused undesirable splitter bar movement under certain conditions.

Tracking Number	Description of Issue
a14577	The Logon Manager context menu (when accessed via the keyboard) covered most of the associated list item when the item was in view, and appeared outside the Logon Manager window when scrolled out of view.
a14605	Reporting failed to trigger a "Shutdown_Programmatic" event during a Windows session logoff with the Agent running.
a14710	Support was added for Oracle Enterprise Single Sign-on Universal Authentication Manager (ESSO-UAM).
a14829	Auto-Enter failed for Internet Explorer modal dialog boxes.
a14835	If a user refreshed a Web browser while logged on to the Reporting Administrative Console, the Log On page appeared and forced the user to log on again.
a14895	Occasionally a report was not viewable when using Microsoft Vista to view reports or email links from the Reporting Administrative Console. This occurred with the MHT output format.
a14932	The "Usage" parameter had only the "All Usages" option available. This parameter now has three options: "All Usages," "Last Time Used," and "# of Times Used."
a14966	The "Date Run" column in the View > Output screen of the Reporting Administrative Console sorted alphabetically rather than chronologically.
a14982	The "Estimated End Time" column in the View > Running screen of the Reporting Administrative Console would update once a report had completed.
a14994	Monthly reports were not retained in the Manage > Scheduled list after they ran one time.
a15010	Reporting has added Pause and Shutdown reports.
a15075	The Trace Controller did not store some information correctly in a 64-bit processor environment.
a15091	The "SSOUserID" field in the Reporting database was not populated when "Credentials to Use" was not set to "Use Active Directory Server Account Only."
a15104	PuTTY was able to capture credentials that the Agent placed in the wrong fields.
a15182	The Agent did not respond to a Web page with no form.
a15222	Support was added for Microsoft Windows Server 2008 R2.
a15234	The ESSO-LM Administrative Console extended the schema after the user selected "No" in response to the dialog box question, "The schema objects appear to already exist. Continue anyway?"
a15375	It was not possible to add a locator object that pointed to the user object.
a15382	The "Retry Logon" dialog box appears even when the Logon Timeout for an application template is set to 0.

Tracking Number	Description of Issue
a15397	The Trace Controller command line contained two misspelled words.
a15433	Settings exclusive to ESSO-LM appeared in the ESSO-LM Administrative Console when it was set for ESSO-UAM only.
a15517	The ESSO-LM Administrative Console and Agent can only be installed from an elevated command prompt on Windows Vista and Windows 7 with UAC enabled.
a15520	An ASP-based logon page has been added for the Reporting Administrative Console, which is supported by ESSO-LM: http://<server>/Reporting/Logon.aspx. The previous URL still works, but is not supported.
a15582	The SendKeys option to click on coordinates was automatically being followed by a press Enter event.
a16267	Java and Mozilla administrative overrides were not being deployed to the Agent correctly.
a16603	The password change form did not appear using "Logon as user" with an expired password for LDAP Authentication with Novell eDirectory.
a17330	ESSO-LM cleared pre-populated information prior to synchronization.

The following table describes issues that were reported in earlier releases of Kiosk Manager and have been resolved in this release

Tracking Number	Description of Issue
s7584, a16201	Due to an issue with the Credential Caching feature, cached credentials from one Windows account are being erroneously used for other Windows accounts.
s7745, a16294	If the Track Memory Consumption feature is set to anything other than 0 (zero), multiple Kiosk Manager sessions will not run. When a session is suspended and another user opens a new session, the first session terminates.
s7831, a16202	Kiosk Manager can be terminated by clicking on the X button if ESSO-LM takes a long time to launch.
s8145, a16199	The Kiosk Manager error log file causes high consumption of disk space.
s8206, s8352, a16203	Some session state lists are not executing during the designated events.
s8356, s8443, s8444, a16205	Kiosk Manager causes incorrect behavior in some applications.
s8363, a16204	Kiosk Manager drops the entered domain name when the ESSO-LM Active Directory synchronization prompt is pre-populated.

Tracking Number	Description of Issue
s8454, a15557	When a user logs off from Kiosk Manager, user data is erroneously left on the clipboard.
s8689, a16292	Applications which are part of a Domain Sharing Group cannot be added on a kiosk machine.
s8995, a16194	An application stops running if multiple sessions are running and a session is locked to allow the next user to log on.
s9053, a16448	A windows application freezes when using Kiosk Manager with ESSO-LM.
s9907, a16943	User is not prompted for password when logging onto Kiosk Manager. Kiosk Manager automatically logs the user onto the desktop.
a13155	When using RSA Secur ID to authenticate to Kiosk Manager, a user will see a synchronization dialog after authenticating to a session. This only happens when the Use cached credentials setting is disabled. This setting is located in the ESSO-LM Administrative Console under Global Agent Settings > Kiosk Manager > Cached Credentials: Use cached credentials.

The following table describes issues that were reported in earlier releases of ESSO-PG and have been resolved in this release

Tracking Number	Description of Issue
a11163	On theESSO-PG Console, using Active Directory with Configuration Objects, an authorized user cannot delete all logons: 1. From the ESSO-LM Administrative Console, an administrator is given Add, Modify, and Delete permissions to an application from its provisioning tab, then pushes the application to the repository CO. 2. From the ESSO-PG Console, the administrator selects a user in the user list and selects Delete All Logons and receives the error message, “The user is not authorized for this action.”

The following table describes issues that were reported in earlier releases of ESSO-PR and have been resolved in this release

Tracking Number	Description of Issue
Bug 11657427, a17285	An exported list of enrolled users generated from the Reports section of the ESSO-PR Management Console included users from a domain other than the one selected for the report.

Tracking Number	Description of Issue
Bug 11669683, a17499	The Password Reset user interface was not compliant with the following Section 508 requirements: • The questions could not get focused by the keyboard or read by a screen reader. • The status bar could not get focus by a keyboard. • There were no Label, ID or Title tags for the question; it could not be read by a screen reader. • There was no alert before a timeout.
Bug 11669694, a17500	The Enrollment user interface was not compliant with the following Section 508 requirements: • The status bar could not get focus from a keyboard. • There was no text equivalent to describe the status bar. • Messages were difficult to read due to color issues. • The status bar was lost. • There were no Label, ID or Title tags for the question; it could not be read by a screen reader. • There was no alert before a timeout.
s5357, a15102	The Windows GINA lost focus in a Citrix desktop session in certain environments.
s6054, s6511	ESSO-PR enhanced the capability for customizing reset messages. See the *ESSO-PR Administrator's Guide* for complete information.
s7383	Initializing storage failed, resulting in the error message, "Error Saving Changes: Unable to find the specified Storage location."
s7854	The SSOGina caused some workstation systems to cease operating, resulting in a blue screen and requiring a system restart.
s8980, a16165	ESSO-PR failed to send email alerts to users who were locked out of their accounts.
s10220, a16788	If running a report on the Users tab of the ESSO-PR Management Console produced an error, report generation ceased.
s10201, s10235, a16962	The ESSO-PR server prompted already enrolled users to re-enroll under heavy load.
s10220, s10808, a16981	The ESSO-PR server returned the error, "Could not retrieve list of enrolled users from domain."
a14326	If the user entered "\" or "@" as a username in the Password Reset Quiz, ESSO-PR displayed an incorrect error message.
a14967	Using Microsoft Windows 7, the Password Reset page incorrectly prefilled the username field with the local administrator's name instead of the name of the last logged-on user.

Open Issues

The following table describes issues that remain open in ESSO-UAM version 11.1.1.5.0

Tracking Number	Description of Issue
a15383	When a user is enrolling in a token method at logon, the dialog box prompting the user to tap/insert a token for enrollment displays a Help button. Clicking this Help button does not launch Help. To work around this issue, click the **Help** button while enrolling from the ESSO-UAM Client Application.
a15449	When a user is using the ESSO-UAM Client Application on a workstation that is connected to a network (that is, an intranet or the internet), but not connected to the Active Directory network, there may be a delay in operations such as authentication and enrollment. To work around this issue, connect the workstation to the Active Directory network or disconnect the workstation from all network access while completing these operations.
a15861	Non-administrative users may see the error messages, “ERROR: BioAPI requires BioAPI BSP to be installed.” followed by, “ERROR: Credential Capture failed.” when enrolling in Fingerprint or BioAPI Logon Methods. This is because some BioAPI BSP installers do not grant read/write permissions for non-administrative users to the BioAPI BSP data storage location and its subfolders. To work around this issue, manually grant Full Control permissions for Everyone to the BioAPI BSP data storage location and subfolders: C:\WINDOWS\system32\BioAPIFFDB. Refer to the *ESSO-UAM Installation Guide* for more information on prerequisites for biometrics.
a16189	If a biometric reader has not been configured for use with the BIO-key BioAPI BSP and a user attempts to enroll in BioAPI Logon Method during logon, the user receives the error message, "No fingerprint reader has been configured. Please log in with your password and use the BIO-key control panel to configure a reader." Clicking **Cancel** on this error message may cause the system to cease responding or fail entirely, requiring the user to reboot the workstation, log on with **Password**, and click **Not Now** on the ESSO-UAM Enrollment Prompt dialog box. This issue does not affect the Fingerprint Logon Method. To work around this issue, configure a biometric reader for the BioAPI BSP prior to installing ESSO-UAM and attempting enrollment in BioAPI Logon Method. Refer to the *ESSO-UAM Installation Guide* for more information on prerequisites for biometrics.

Tracking Number	Description of Issue
a17372	After a workstation restart, there may be a delay at logon while ESSO-UAM waits for system processes and services to start. During this delay, if a user logs on to the workstation with Password and attempts to enroll in a token logon method, user may see the message, "ERROR: A reader device is required to enroll in this logon method and is either not installed or not functioning." If a user is attempting logon with a token logon method, there may be a delay before the token is recognized as being present. To work around this issue, when the Ctrl + Alt+ Delete dialog displays on restart, if a token is already enrolled, wait a minute or so before presenting the enrolled token to initiate logon. If a token is not enrolled, log on with a non-token method and wait a minute or so before enrolling the token during logon, or enroll from the ESSO-UAM Client Application.
a17420	In the Client Application, if a user modifies the value of either Proximity Card PIN Min Length or Fingerprint Number of Fingers to Enroll by selecting the current field value and entering an invalid value, user may see the error message, "Unable to save changes." when the invalid value is applied. To work around this issue, type a valid value, or use the up/down arrows of the control to set a valid value, and click **Apply** to save the change. Refer to the *ESSO-UAM User Guide* for valid setting values in the Client Application.
a17551	With Authentication Manager installed, if the user clicks **Reveal** in the Retry Logon dialog box and then cancels the initial authentication attempt, the resulting Authentication Manager dropdown dialog box appears behind the Retry Logon's. It is then impossible for the user to enter credentials or dismiss the Retry Logon. To work around this issue, use the Task Manager to close the Agent and the application requiring credentials, and relaunch both.

The following table describes issues that remain open in ESSO-LM version 11.1.1.5.0

Tracking Number	Description of Issue
Bug11664956, a17246	ESSO-LM does not immediately recognize a password change to a credential sharing group for users running Windows Vista or Windows 7, who are logged on when the administrator implements the password change. This is due to differences between Microsoft's security model for previous Windows operating systems and that of Windows Vista/Windows 7. Microsoft has removed the "NPPasswordChangeNotify" function that previously informed ESSO-LM of the need to refresh cached credentials, and therefore the local cached credentials are not updated. This Microsoft change only affects users who are logged on when the administrator changes the password remotely. Administrators should always ensure that a user has logged off all client workstations before assigning a new password.
a15782	An "Auth_Failure" event is triggered when ESSO-LM starts after the user resets a password either with ESSO-PR or on the Active Directory account itself. The event appears in the Reporting Database. There is no workaround necessary for this issue. Users will not experience any effects.

Tracking Number	Description of Issue
a17339	With Silent Credential Capture set to "Do not capture silently" and engaged in capturing credentials for several applications, an untemplated application's credentials are not captured and the new account is not created. Refer to the *Template Configuration and Diagnostics* series in the Oracle online documentation center for more information.
a17362	The ESSO-LM Administrative Console does not recognize control fields for Skype 5.1. To work around this issue, create the template using SendKeys.
a17399	Silent Credential Capture does not capture credentials for .NET applications if the user presses the **Enter** key instead of clicking the **Submit** button after entering credentials. Refer to the Oracle online documentation center for detailed information. To work around this issue, set "Credential Capture Mode" to "Do not capture silently" for .NET applications.
a17429	Certain applications are displaying an extra instance of the New Logon dialog box when Silent Credential Capture mode is set. This happens with applications that have their Change Password dialog box launched immediately after the user submits credentials. To work around this issue, set "Credential Capture Mode" to "Do not capture silently."
a17513	The ESSO-LM Administrative Console help incorrectly identifies the default value for the Global Agent Setting: Audit Logging> Reporting Server> Cache limit. Although it reads 1000, the correct value is 0xFFFFFFFF. The *ESSO-LM Global Agent Settings Reference Guide* contains the most up-to-date information for this and all other Global Agent Settings.
a17523	The ESSO-LM Administrative Console incorrectly calculates the ordinal index of the <input type=image> fields. To work around this issue, change the ordinal value of the field manually.

The following table describes issues that remain open in ESSO-PG version 11.1.1.5.0

Tracking Number	Description of Issue
a16315	Reports generated for ADAM storage from the ESSO-PG Console contain blank information for "logon name," "principal name," "DN," and "GUID." There is no workaround for this issue.
a16403	The ESSO-PG event log contains hex strings rather than the user name. There is no workaround for this issue.
a16568	When event logs are generated for a specific period of time, an exception error occurs: "Conversion failed when converting datetime from character string." There is no workaround for this issue.

The following table describes issues that remain open in ESSO-Anywhere version 11.1.1.5.0

Tracking Number	Description of Issue
a17397	Due to limitations in Microsoft's ClickOnce technology, a deployment version format cannot have more than four segments separated by three dots; that is, the format: X.X.X.X. This prohibits naming a deployment version identically to the Oracle product version. Administrators can version the deployment in any way they choose within the framework of this limitation, for example, X.X.XXX or X.X.X.XX.
a17493	The *ESSO-Anywhere Console Administrator's Guide* contains more accurate information regarding registry settings for a deployment than does the online help. This will be rectified in the next release.

The following table describes issues that remain open in ESSO Suite Plus Reporting version 11.1.1.5.0

Tracking Number	Description of Issue
a15168	Since Reporting version 10.1.4.1.0 Fix Pack 1, installation of a newer version overwrites the Reporting registry settings. To work around this issue, export the registry file: HKLM\SOFTWARE\Passlogix\Reporting to a .REG file. Install the fix pack, then write the exported registry settings back to HKLM by double clicking the .REG file.

The following table describes issues that remain open in ESSO-PR version 11.1.1.5.0

Tracking Number	Description of Issue
a17501	In Windows 7, Auto Enrollment prompts users to authenticate a second time immediately after their initial authentication. Turning off Digest Authentication eliminates this issue. However, this also makes it possible for an unauthorized user to change the password on an unlocked workstation.

Hardware and Software Requirements

This section lists hardware and software requirements and optional supported software of the products and components in Oracle Enterprise Single Sign-on Suite Plus.

- Supported Operating Systems
- Disk Space Requirements
- Repositories
- Web Servers
- Browsers
- Microsoft .NET Framework
- Optional Software Support for ESSO-LM
  - Java
  - Host Emulators
  - Windows Event Logging
  - Citrix Presentation Server/XenApp
  - SAP
- ESSO-UAM Supported Third-Party Cards, Middleware, and Hardware
- Additional ESSO-PG Requirements

Supported Operating Systems

The Oracle Enterprise Single Sign-on Suite Plus components are supported on the following operating systems:

Operating System	ESSO-LM	ESSO-LM Strong Auths*	Kiosk Manager	ESSO-UAM	ESSO-PG Server	ESSO-PG Client	ESSO-PR Server	ESSO-PR Client	ESSO-Anywhere	Reporting Console
Microsoft Windows XP Professional SP3 (32-bit)	✓	✓	✓	✓		✓		✓	✓	
Microsoft Windows Vista™ Business Edition SP1 (32-bit)	✓	✓				✓		✓	✓	
Microsoft Windows 7 (64-bit)	✓					✓		✓	✓	
Microsoft Windows 7 (32-bit)	✓					✓		✓	✓	
Microsoft Windows Server 2008 R2 (64-bit)	✓	✓			✓		✓		✓	✓
Microsoft Windows Server 2008 SP1+(64-bit)	✓	✓			✓		✓		✓	✓
Microsoft Windows Server 2008 SP1+(32-bit)	✓	✓			✓	✓	✓	✓	✓	✓
Microsoft Windows Server 2003 SP2/R2+ (64-bit)	✓	✓			✓	✓	✓	✓	✓	✓
Microsoft Windows Server 2003 SP2/R2+ (32-bit)	✓	✓			✓	✓	✓	✓	✓	✓

ESSO-LM includes both standard logon methods such as LDAP and Windows Logon, and "Strong Authenticators" such as smart cards, read-only smart cards, proximity devices, and RSA SecurID tokens.

Disk Space Requirements

The minimum disk space requirements for the Oracle Enterprise Single Sign-on Suite Plus components are as follows:*

Resource	ESSO-LM Console	ESSO-LM Agent	Kiosk Manager	ESSO-UAM	ESSO-PG Server	ESSO-PG Client	ESSO-PR Server	ESSO-PR Client	ESSO-Anywhere	Reporting Console
Disk Space	22 MB	135 MB	20 MB	30 MB	7 MB	25 MB	44 MB	10 MB	5 MB	256 MB

*Consult the Microsoft Web site for the most up-to-date requirements and recommendations for your operating system.

Repositories

The Oracle Enterprise Single Sign-on Suite Plus components support the following repositories:

Repository	ESSO-LM	Kiosk Manager	ESSO-UAM	ESSO-PG Server	ESSO-PR Server	Reporting
Oracle Directory Server Enterprise Edition 11gR1	✓	✓		✓	✓	
Oracle Internet Directory 11gR1	✓	✓		✓	✓	
Oracle Internet Directory 11.1.1.3.0	✓					
Oracle Internet Directory 10.1.4.0.1	✓					
Oracle Virtual Directory 11gR1	✓	✓		✓	✓	
Oracle Database Management System 11gR2	✓			✓	✓	✓
Oracle Database Management System 11gR1	✓			✓	✓	✓
Oracle Database Management System 10g	✓			✓	✓	
Microsoft Active Directory 2008 R2	✓	✓	✓	✓	✓	
Microsoft Active Directory 2008	✓	✓	✓	✓	✓	
Microsoft Active Directory 2003 SP1	✓	✓	✓	✓	✓	
Microsoft Active Directory Application Mode 2003 SP1	✓	✓	✓	✓	✓	
Microsoft Active Directory Lightweight Directory Services 2008	✓	✓	✓	✓	✓	
Microsoft SQL Server 2008 R2	✓			✓	✓	✓
Microsoft SQL Server 2008	✓			✓	✓	✓
Microsoft SQL Server 2005	✓			✓	✓	✓
IBM DB2 Database 8.1.6	✓					
IBM Tivoli Directory Server 5.2	✓	✓		✓		
Novell eDirectory 8.8 SP1	✓			✓		
Open LDAP Directory Server 2.4.x	✓					

Repository	ESSO-LM	Kiosk Manager	ESSO-UAM	ESSO-PG Server	ESSO-PR Server	Reporting
Open LDAP Directory Server 2.2	✓					
Open LDAP Directory Server 2.0.27	✓					
Siemens DirX Directory 8.0	✓					

Web Servers

The following Oracle Enterprise Single Sign-on Suite Plus components require one of the following web servers to be installed:

Web Server	ESSO-PG Server	ESSO-PR Server	Reporting Console
Microsoft Internet Information Server 7.5	✓	✓	✓
Microsoft Internet Information Server 7.0	✓	✓	✓
Microsoft Internet Information Server 6.0	✓	✓	✓

Browsers

The Oracle Enterprise Single Sign-on Suite Plus components support the following browsers:

Browser	ESSO-LM	ESSO-PG Server	ESSO-PR Server	Reporting Console
Microsoft Internet Explorer 8.0	✓	✓	✓	✓
Microsoft Internet Explorer 7.0	✓	✓	✓	✓
Mozilla Firefox 4.0	✓			
Mozilla Firefox 3.6	✓	✓		✓
Mozilla Firefox 3.5	✓	✓		✓

Microsoft .NET Framework

The table below lists Oracle Enterprise Single Sign-on Suite Plus components that require Microsoft .NET Framework, and the .NET versions they require:

Version	ESSO-LM Administrative Console	Kiosk Manager	ESSO-PG Server	ESSO-PR Server	ESSO-Anywhere Administrative Console	Reporting Console
Microsoft .NET Framework 4.0	✓					
Microsoft .NET Framework 3.5 SP1						✓
Microsoft .NET Framework 2.0 SP1				✓		
Microsoft .NET Framework 2.0		✓	✓		✓	

ESSO-UAM Supported Third-Party Cards, Middleware, and Hardware

The following tables list the specific third-party cards, middleware, and reader pairings that are tested and officially supported. ESSO-UAM does not ship with cards, middleware, or hardware; you must obtain them separately.

Smart Cards

The ESSO-UAM Smart Card Logon Method supports a variety of smart card technologies, including cards used with Microsoft Base CSP (MiniDriver) and cards that are used with a PKCS#11-compliant smart card middleware. It also supports the Gemalto .NET smart card.

Prior to use with ESSO-UAM, smart cards must be initialized to contain a valid serial number and PIN. ESSO-UAM does not provide any smart card initialization 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.

For PKCS#11 compliant cards and middleware, cards must be initialized with a standard PKCS#11-compatible applet that provides a serial number and a user PIN. MS Base CSP (MiniDriver) compliant cards must be initialized with a standard MS Base CSP "\cardid" (serial number) file and a user PIN.

The corresponding registry file is available on the ESSO-UAM installation ISO image in the /SmartCard folder. The appropriate file must be merged (by double-clicking it) after the middleware and ESSO-UAM are installed. If ESSO-UAM is re-installed or upgraded, the file must be merged again.

Oracle recommends that you always obtain the latest drivers and firmware from the reader manufacturer.

Card	Family/Type	Middleware	Registry File
RSA smart card 5200	PKCS11	RSA Authentication Client 2.0	smart_providers_pkcs11_rsa.reg
NetMaker Net iD - CardOS 1	PKCS11	NetMaker Net iD 4.6	smart_providers_pkcs11_netid.reg
ORGA JCOP21 v2.2	PKCS11	SafeSign/RaakSign Standard 3.0.23	smart_providers_pkcs11_safesign.reg
Oberthur ID-ONE Cosmo	PKCS11	SafeSign/RaakSign Standard 3.0.23	smart_providers_pkcs11_safesign.reg
Athena IDProtect	PKCS11	SafeSign/RaakSign Standard 3.0.23	smart_providers_pkcs11_safesign.reg
Athena ASECard Crypto	PKCS11	Athena ASECard Crypto 4.33	smart_providers_pkcs11_athena.reg
HID Crescendo 700	PKCS11	HID RaakSign Standard 2.3	smart_providers_pkcs11_raaksign.reg
IBM JCOP21id	PKCS11	SafeSign Identity Client 2.2.0	smart_providers_pkcs11_safesign.reg
DigiSign JCOP with MyEID Applet	PKCS11	Fujitsu mPollux DigiSign Client 1.3.2-34 (1671)	smart_providers_pkcs11_fujitsu.reg

Card	Family/Type	Middleware	Registry File
Gemalto Cyberflex 64K (v2c) SPE Required / SPE Optional	PKCS11	Gemalto Access Client 5.5 Xiring CCID Driver version 1.00.0002 or later / XI-SIGN reader Gemalto PC-PinPad version 4.0.7.5 or later / PC Pinpad reader	smart_providers_pkcs11_ gemalto.reg
Oberthur ID-One Cosmo 64 v5.2D Fast ATR with PIV application SDK	PKCS11	ActivIdentity ActivClient 6.1	smart_providers_pkcs11_ actividentity.reg
Cyberflex 64K	PKCS11	Gemalto Access Client 5.5	smart_providers_pkcs11_ gemalto.reg
Sagem YpsID S1 and S2 (Sagem Mini-Driver cards are not supported.)	PKCS11	Sagem YpsID 3.2.1	smart_providers_pkcs11_ sagem.reg
HID Crescendo 200	MS Base CSP/MiniDriver	HID Global MiniDriver for MS Base smart card CSP	smart_providers_ basecsp.reg
Gemalto .NET v2+	MS Base CSP/MiniDriver	Gemalto MiniDriver for Microsoft Windows XP	smart_providers_ basecsp.reg
Oberthur ID-ONE Cosmo	MS Base CSP/MiniDriver	Oberthur ID-ONE MiniDriver for MS Base smart card CSP	smart_providers_ basecsp.reg
Athena ASECard Crypto ILM	MS Base CSP/MiniDriver	Athena ASECard Crypto ILM MiniDriver for MS Base smart card	smart_providers_ basecsp.reg
Gemalto .NET v2 or v2+	.NET	Gemalto .NET smart cards PKCS#11 library 2.1.3	smart_providers_pkcs11_ gemalto_dotnet.reg

Proximity Cards

The ESSO-UAM Proximity Card Logon Method supports many standard HID, Mifare and iClass proximity cards and tokens that are used for physical access security. Currently, ESSO-UAM supports several Omnikey and RFIDeas card reader devices.

> The Crescendo C700 Card is not supported as a Proximity Card with any Omnikey 5X25 Card Reader.
>
> Omnikey dual readers require a manufacturer's proximity reader driver.
>
> RFIdeas readers do not require a special driver.

Card	Family/Type	Reader
HID 1336 DuoProx II	Prox 125 KHz	Omnikey Cardman 5125/5325
HID 1346 ProxKey II-Key fob token	Prox 125 KHz	Omnikey Cardman 5125/5325
HID ProxCard II	Prox 125 KHz	Omnikey Cardman 5125/5325
HID 2080 ICLASS Clamshell	RFID 13.56 MHz	Omnikey Cardman 5121/5321
HID 1430 MIFARE ISO	RFID 13.56 MHz	Omnikey Cardman 5121/5321
HID 1450 DESFire ISO	RFID 13.56 MHz	Omnikey Cardman 5121/5321
HID C700	RFID 13.56 MHz	Omnikey Cardman 5121/5321
HID iCLASS Px E6L	RFID 13.56 MHz	Omnikey Cardman 5121/5321
Indala FlexCard	Prox 125 KHz	RFIDeas pcProx USB RDR-6382AKU
Indala FlexPass	Prox 125 KHz	RFIDeas pcProx USB RDR-6382AKU
iCLASS and MIFARE contactless Most iCLASS and MIFARE contactless cards are supported	RFID 13.56 MHz	RFIDeas AIR ID RDR-7582AKU
HID C700	RFID 13.56 MHz	RFIDeas AIR ID RDR-7582AKU
EM Wristband	Prox 125 KHz	RFIDeas pcProx USB RDR-6E82AKU

Biometrics

The Fingerprint Logon Method supports the use of numerous external and embedded laptop biometric fingerprint devices to provide a convenient and secure fingerprint authentication mechanism to ESSO-UAM. This release of ESSO-UAM is compatible with BIO-key version 1.9. For the list of supported devices, refer to the Bio-key documentation.

The BioAPI Logon Method leverages the BioAPI framework , thus enabling support of almost any third-party BioAPI-compliant Biometric Service Provider (BSP) module. In addition to fingerprint biometrics, this logon method can also support other biometric technologies that offer a BioAPI compatible BSP such as palm, facial, and iris recognition solutions. Refer to the BioAPI BSP documentation for supported biometric devices.

Optional Software Support for ESSO-LM

Java

- Java support: Java Runtime Environment (JRE) version 1.6, 1.5, 1.4, 1.3.

Host Emulators

- Support for virtually any HLLAPI, EHLLAPI or WinHLLAPI-based emulator

  See "ESSO-LM Supported Emulators" on page 35 or visit myoraclesupport for a list of supported emulators.

Windows Event Logging

- Windows event logging requires Microsoft Windows Server configured for Event Logging when being redirected to a central server.

Citrix Presentation Server/XenApp

- Citrix XenApp version 6.0: Windows Server 2008 R2 64-bit
- Citrix XenApp version 5.0: Windows Server 2008 64-bit, Windows Server 2003 64-bit, Windows Server 2003 32-bit
- Citrix Presentation Server version 4.5: Windows Server 2003 32-bit

SAP

- SAP support: version 7.2, 7.1, 6.40.

ESSO-LM Supported Emulators

The ESSO-LM mfrmlist.ini file includes the following host emulators:

Emulator	Versions Supported
Attachmate Extra!	X-treme 8.0 SP1, 2000, 6.5, 6.4, 6.3
Attachmate IRMA for the Mainframe	4.01, 4
Attachmate myExtra! Presentation Services	7.1, 7.0
Attachmate/WRQ Reflection	15.0, 14.0, 10.0, 9.0, 8.0, 7.0
BOSaNOVA TCP/IP	6.0, 5.0
Ericom PowerTerm Interconnect	9.1.0, 8.2.0
G&R Glink	6.0
Hummingbird Exceed	11.0, 10.0, 9.0
Hummingbird HostExplorer	11.0, 10.0, 9.0
IBM WebSphere Host On-Demand	10.0.03, 9.0, 8.0, 4.0
IBM Personal Communications	5.8, 5.6, 5.5, 4.3
Jolly Giant QWS3270 PLUS	4.4 SP5, 4.3 SP10
NetManage NS/ElitePlus for Mainframe	3.12
NetManage Rumba	7.5, 7.1, 6.0
Newhart Systems BLUES 2000	6.0.0.35
PuTTY	0.60
ScanPak (Eicon) Aviva	9.1, 9.0, 8.1
Seagull BlueZone	4.0, 3.4
Zephyr PASSPORT PC TO HOST	2005
Zephyr PASSPORT WEB TO HOST	2005

ESSO-LM Supported Applications

ESSO-LM supports the following applications out-of-the-box:

Windows Application	Versions Supported
Adobe Reader	9.1, 8.13, 6.0, 5.1, 5.05, 4.05
AIM (AOL instant Messenger)	6.9, 6.8, 5.5, 5.2
Citrix ICA Client / Program Neighborhood	0.200.2650, 9.15, 9.0
Entrust	7.0, 6.1, 6.0, 5.5, 5.0, 4.0
Eudora	7.1, 6.1, 5.2, 5.1.1, 5.0.2, 4.2
GoldMine	6.7, 6.5, 6.2, 5.7, 5.0, 4.0
ICQ	6.5.1, 2002a, 4.0
Lotus Notes	8.0.1, 8.0, 6.5, 6.0, 5.0
Lotus Organizer	6.1, 6.0, 5.0, 4.1
Lotus Sametime	8.0.2, 8.0
Meeting Maker	8.0, 7.3, 7.2, 7.1, 7.0, 6.0, 5.5.2
Microsoft FrontPage	2007, 2003, XP, 2000
Microsoft Outlook	2007, 2003, XP, 2000
Microsoft Word	2007, 2003, XP, 2000
MSN Messenger	9.0, 7.5, 6.2, 5.0
Novell Client	4.91 SP5, 4.91 SP4, 4.91 SP1, 4.90, 4.83
Novell GroupWise	6.5, 6.0, 5.5
Oracle	11g, 10g
Oracle ESSO-LM Administrative Console	11.1.1.2.0, 10.1.4.1.0 Fix Pack 6
PKZip	12.2, 12.1, 12.0, 11.2, 11.0, 10.0, 9.0, 8.0, 5.0
QuickBooks Pro	2009, 2004, 2003, 2002, 2001, 2000
QuickBooks Pro (Password-Only)	2009, 2004, 2003, 2002, 2001, 2000
Sage ACT!	2009 (11.0), 6.0, 5.0, 4.0, 3.0
Siebel Sales CRM	8.1.1, 5.0
Visual Source Safe	2008, 2005
Windows Logon	8.0
WinZip	12.0, 11.2, 11.0, 10.0, 9.0, 8.1, 8.0, 7.0
Yahoo! Messenger	9.0, 5.6, 5.5

Additional ESSO-PG Requirements

Microsoft Internet Information Server

If Active Directory or ADAM is used, the anonymous account used in Microsoft IIS must have administrative privileges and the server must be joined to the domain.

Microsoft Web Services Enhancements

Microsoft Web Services Enhancements 3.0 (WSE 3.0) is required. (installed by ESSO-PG)

Installer Requirements

To install ESSO-PG, you must have administrative privileges for the ESSO-PG/IIS server.

Certificate Requirements

- An X.509 Certificate for SSL must be obtained from a Certificate Authority.
- A Trusted Root CA Certificate should also be downloaded from your Certificate Authority into the list of trusted root CAs on the local computer.

For more information, see the "Enable SSL" section in the *ESSO-PGInstallation and Setup Guide.*

A certificate setup guide is provided with the ESSO-PG documentation suite. If you have not set up a certificate authority and want to use Microsoft Certificate Services to obtain certificates, refer to the *ESSO-PG Certificate Setup Guide* which walks you through obtaining the necessary certificates using Microsoft Certificate Services.

Technical Notes

The technical notes describe important technical information about this release.

ESSO-UAM

Error When Using RSA Authentication Client 2.0 Smart Card Middleware

Due to race conditions and variations in polling times, it is possible that users will receive the error message, "Card is either not enrolled or not supported,"when using RSA Authentication Client 2.0 Smart Card middleware with some Smart Cards.

There are two possible remedies for this scenario:

- The user can click **OK** and try inserting the card again.
- The administrator can add the following registry key and increase the timeout values:

  Smart Card Authenticator card and serial timeout settings (PKCS11 race conditions):

  Key: HKLM\SOFTWARE\Passlogix\UAM\Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}\Settings

  Value: CardTimeout = DWORD (0-5000 ms; 2000 ms (default))

  Value: SerialTimeout = DWORD (0-5000 ms; 500 ms (default))

> CardTimeout applies to certain PKCS11 modules that might have a race condition with Windows smart card APIs. Increasing the timeout increases reliability but might adversely affect performance.
>
> SerialTimeout applies to certain PKCS11 modules that have a race condition when reading the serial number from the card. If the card is supported but its serial number is not read, this might be the issue. Increasing the timeout increases reliability but might adversely affect performance.

PKCS11 Card Failure with Remote Desktop Lock

If a workstation is locked due to a Remote Desktop session, a user may not be able to unlock the workstation using an enrolled smart card with certain PKCS11 middleware. This is due to the limitations of the smart card middleware.

To unlock the workstation, the user can use Windows Password.

Incompatibility Between Crescendo C700 Proximity Card and Omnikey 5X25 Proximity Card Reader

The Crescendo C700 Card does not function as a Proximity Card with any Omnikey 5X25 Card Reader. For a list of supported cards, middleware, and hardware, refer to that section in this document.

ESSO-LM

Using ESSO-LM 11.1.1.5.0 with Oracle Internet Directory 11.1.1.2.0 and 11.1.1.5.0

You must configure Oracle Internet Directory (OID) 11g to enable Anonymous Binding for use with ESSO-LM 11.1.1.5.0. Follow this procedure:

1. Launch a browser and open **Oracle Directory Services Manager**.
2. Log on to ODSM as the OID super user, orcladmin.
3. Click **Connect to a directory** and select an OID instance.

4. Click the **Data Browser** tab.
5. Go to: DN: cn=oid1,cn=osdldapd,cn=subconfigsubentry.
6. Note that the "orclanonymousbindsflag" flag is set to "2." This entry only allows anonymous binding to the server's "RootDSE," but nothing else.
7. Change the entry from "2" to "1." Click **Apply** in the upper-right hand corner.
8. Ensure the OID "Enable Access Control Check" option is disabled:

   a. Locate the appropriate OID server instance in the Oracle Enterprise Manager Fusion Middleware Control application.

   b. From the Oracle Internet Directory menu, select **Administration > Server Properties**.

   c. On the Server Properties screen, locate the "Enable Access Control Check" option and make sure it is switched off.

   d. Click **Apply** in the upper-right hand corner.

Using ESSO-LM 11.1.1.5.0 with Oracle Virtual Directory 11.1.1.2.0 and 11.1.1.5.0

You must configure Oracle Virtual Directory (OVD) 11.1.1.2.0 and 11.1.1.5.0 to enable anonymous binding and disable the access check for use with ESSO-LM 11.1.1.5.0. Follow this procedure:

1. Ensure that the user containers of all LDAP servers are mapped to the same subtree of the OVD directory information tree. For example, Following is the correct layout for DSEE and OID servers mapped to the same OVD instance:

   ou=dsee,ou=users,dc=corp,dc=com (for Oracle DSEE user entries)

   ou=oid,ou=users,dc=corp,dc=com (for OID users entries)

   This ensures that the SSO locator-based user lookup mechanism is able to locate users from different servers.
2. Ensure anonymous binding is enabled on the mapped LDAP server. Grant search permissions for user list entries to the anonymous user.
3. Ensure the OVD "Enable Access Control Check" option is disabled:

   a. Locate the appropriate OVD server instance in the Oracle Enterprise Manager Fusion Middleware Control application.

   b. From the Oracle Virtual Directory menu, select **Administration > Server Properties**.

   c. On the Server Properties screen, locate the "Enable Access Control Check" option and make sure it is switched off.

   d. Click **Apply** in the upper-right hand corner.

Synchronization

Database support requires that client connectivity support be installed for the specific database(s).

Event Manager

The XML log file plug-in continually expands/appends file. The log file should be cleaned up periodically (from the user's AppData\Passlogix folder) if it is used as part of a solution.

Logon Support

Embedded browser support, such as from within Lotus Notes, requires that IE 6.0 be installed. It is not consistent with previous versions of the browser.

Under Windows Server 2003 (as well as Windows XP SP2), browser helper object support is (or can be) turned off; this security setting is no longer required to be on for ESSO-LM to function properly and can be turned off if it is no longer needed.

Backup/Restore

Conflicts may occur when using Backup/Restore functionality in conjunction with synchronizer usage. It is not suggested that a deployed solution utilize both mechanisms and that Backup/Restore only be used in standalone installations.

You must restore a backup from a local drive. It is not possible to restore from a network drive.

Java Sun Plug-in Applets

The Java Applet using Java Sun Plug-in 1.1.3 must be clicked on before the Agent responds to it. The plug-in loads the JHO only after the user clicks into the applet UI.

Oracle JInitiator 1.1.8.X functions without this problem.

Citrix Published Applications Using SendKeys: Cannot Use 'Set Focus' Feature

When using SendKeys with Citrix published applications, the SendKeys 'Set Focus' feature cannot be used. The reason this feature cannot be used is because Citrix application windows are painted, so there are no controls on the window. In order for 'Set Focus' to function, it needs to reference a window's controls.

Citrix Published Applications: SendKeys Does Not Process 'Enter' or 'Tab' Properly

When setting up a Citrix published application using regular SendKeys with 'Enter' or 'Tab' characters in between each field, those characters are not processed correctly. They are processed in a random order.

The issue is that the separator characters submitted between fields (typically 'Enter' or 'Tab' characters) are not processed by the Citrix application in the correct sequence resulting in inconsistent behavior.

The solution is to modify the application template to add a delay between the fields. For example, if the current application template is configured like this:

[Username]
[Tab]
[Password]
[Tab]
[Enter]

delays should be added in between fields:

[Username]
[Delay 0.1 sec]
[Tab]
[Password]
[Delay 0.1 sec]
[Tab]
[Enter]

"End Program" Message Displayed

NetSoft's NS/Elite emulator causes ESSO-LM to display an 'End Program' message when logging off or restarting a machine. This behavior is only seen intermittently.

> Clicking 'End program' may result in credentials not being cleaned up (if 'Delete Local Cache' is turned on in the Administrative Console).

Using the Hidden Window Utility

For information on using the Hidden Window Utility, which is located in the Utility folder on the CD, refer to the Oracle online documentation center.

Reflection 14 Sporadically Causes the Display of the ESSO-LM Password Change Dialog Box on a Logon Screen

ESSO-LM sporadically displays the Password Change dialog box on a Reflection 14 logon screen. If this dialog box displays, click the **Cancel** button and begin to enter text. The expected logon dialog box displays.

Configuring Java to Accept Application Credentials

> Also see the related article (1140293.1) at myoraclesupport.com.

The flags are located in HKLM\SOFTWARE\Passlogix\Extensions\AccessManager and are as follows:

JhoHierarchyProcessing

Determines which Java hierarchy events are recognized. Set the flag as follows:

HIERARCHY_EVENT_CHANGED = 0x1

The above value instructs the JHO to recognize all hierarchy events.

JhoEventWaitTimeout

Determines the event processing timeout for JHO controls (in milliseconds). The default value of 0 instructs the JHO to wait indefinitely.

JhoWindowEventProcessing

Determines which Java window events are recognized. This flag is a combination of the following values:

WINDOW_EVENT_OPENED = 0x1
WINDOW_EVENT_CLOSED = 0x2
WINDOW_EVENT_ACTIVATED = 0x4
WINDOW_EVENT_DEACTIVATED = 0x8
WINDOW_EVENT_CLOSING = 0x10
WINDOW_EVENT_ICONIFIED = 0x20
WINDOW_EVENT_DEICONIFIED = 0x40

By default, all window events are recognized.

JhoComponentProcessing

Determines which Java component events are recognized. This flag is a combination of the following values:

COMPONENT_EVENT_SHOWN = 0x1
COMPONENT_EVENT_HIDDEN = 0x2
COMPONENT_EVENT_ADDED = 0x4
COMPONENT_EVENT_REMOVED = 0x8

By default, all component events are recognized.

JhoInjectType

Determines the injection type used by the JHO to submit data to the controls. This flag takes one of the following values:

INJECT_TYPE_DEFAULT = 0
INJECT_TYPE_METHOD = 1
INJECT_TYPE_ACCESSIBLE = 2
INJECT_TYPE_NONACCESSIBLE = 3
INJECT_TYPE_ROBOT = 4

By default this flag is set to INJECT_TYPE_DEFAULT.

If you set JhoInjectType to INJECT_TYPE_DEFAULT, the JHO attempts injection using each of following methods, in the order shown, until injection is successful:

INJECT_TYPE_METHOD (if an appropriate set method had been found for the control)
INJECT_TYPE_ACCESSIBLE (if the control supports accessibility)
INJECT_TYPE_NONACCESSIBLE
INJECT_TYPE_ROBOT

> For combo and list boxes, the JHO always uses INJECT_TYPE_METHOD.

Oracle recommends the following default settings on new installations of ESSO-LM:

JhoWindowEventProcessing=0x3
JhoComponentProcessing=0xB
JhoHierarchyProcessing=0x0

These values instruct the JHO to recognize the following events:

WINDOW_EVENT_OPENED (0x1)
WINDOW_EVENT_CLOSED (0x2)
COMPONENT_EVENT_SHOWN (0x1)
COMPONENT_EVENT_HIDDEN (0x2)
COMPONENT_EVENT_REMOVED (0x8)

Removing the ssolauncher/nossoshutdown Key from the Registry

1. Install SSO+NetworkProvider+msp and modify SSO Sens Svc to start automatically in Services.
2. Remove all ssoLauncher/ssoShell from HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\UserInit and HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AppSetup
3. Change published Application command line to:
   "C:\Program Files\Passlogix\v-GO SSO\wts\ssolauncher.exe" /application "c:\WINDOWS\notepad.exe" /SSOSHUTDOWNSSOAUTH
4. Set Shell:LogonOnStartup to 1:
   In Administrative Console: End-User Experience\Response\Logon to waiting applications upon startup -> Logon At Startup.

Win32/Injector.CFR Trojan Reported in the Agent Installer

Some MSI versions of the ESSO-LM Agent installer exhibit false positives when scanned by antivirus software during a Repair operation. The scan identifies the Win32/Injector.CFR trojan, although in reality, no such virus is present in the installer.

Kiosk Manager Administrative Console Notes

The ESSO-LM Administrative Console must be closed in order to run the Kiosk Manager Session Agent. If you start the Session Agent while the Administrative Console is still running, an error message displays saying, "Cannot run Kiosk Manager until Administrative Console is closed."

> It is recommended that you do not use the ESSO-LM Administrative Console on a machine running Kiosk Manager.

Save Data Before Locking a Session

If a user locks a session or leaves the kiosk while an application has a dialog open, (such as the "Save As" dialog) and Kiosk Manager is unable to dismiss that dialog, the application may be terminated.

As such, it is strongly recommended that users save data before locking a session or leaving the kiosk.

ESSO-Anywhere

ESSO-Anywhere Does Not Support the Following ESSO-LM Features

- **Windows Authenticator v2 GINA**. The Windows Authenticator v2 GINA component is not supported. ESSO-Anywhere does not support installing GINAs.
- **Windows Authenticator v2 Network Provider**. The Windows Authenticator v2 Network Provider component is not supported. ESSO-Anywhere does not support installing Windows services.

> ESSO-Anywhere supports all Windows Authenticator v2 functionality except the GINA and Network Provider. There is no workaround to enable the unsupported Windows Authenticator v2 functionality.

Default Security Policy on Windows Vista, Windows 7, and Windows 2008 Prevents ESSO-Anywhere from Running

Because ESSO-Anywhere installs into the user's home folder, rather than the Program Files folder, the default security policy on Windows Vista deployments prevents ESSO-Anywhere from executing due to insufficient permissions. (By default, the Program Files folder is recognized as a secure location, while the user's home folder is not.)

To solve this issue, do the following:

1. Modify the Group Policy Object (GPO) and disable the setting **User Account Control: Only elevate UIAccess applications that are installed in secure locations**. The location of this setting in the GPO is: `Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\`.
2. Apply the modified policy to the domain using standard group policy practices.

You will still be protected from unauthorized code access since applications must also pass the PKI signature check in order to execute, regardless of the state of the above setting.

For more information on this security setting, see the following Microsoft Vista TechCenter article: http://technet2.microsoft.com/WindowsVista/en/library/c6c673db-0e8b-43da-95ad-2280cb0a7ab01033.mspx?mfr=true

Script Required for Microsoft IIS 6.0 Deployment

By default, Microsoft IIS 6.0 does not serve the three files types used by ESSO-Anywhere (.application, .deploy,and .manifest). Administrators planning to deploy ESSO-Anywhere using an IIS 6.0 Web Server must run thescript included on the ESSO-Anywhere CD. To run this script, double-click the file `IisAddMimeTypes.vbs` in the `(CD Root)\Utility` folder and follow the prompts.

Attempting to deploy ESSO-Anywhere without running this script results in the error HTTP 404. For a complete discussion of IIS 6.0 and unsupported MIME types, see the Microsoft Web site.

ESSO-Anywhere Creates Non-Functional Deployments with ESSO-PG 10.1.4.0.2 Installed

ESSO-Anywhere is designed for out-of-the-box compatibility with ESSO-PG 11.1.1.5.0. If you install ESSO-PG 10.1.4.0.2 on your master ("template") machine, the support6.dll file is overwritten with a version that is incompatible with ESSO-Anywhere. A deployment package created via ESSO-Anywhere in this scenario will result in a non-functional deployment on the end-user machine.

To reinstall the correct file, do the following on your master machine:

1. Delete the support6.dll file from the ESSO-LM installation directory. The default path is `\Program Files\Passlogix\v-GO SSO`.
2. Open the **Add/Remove Programs** applet, launch the ESSO-LM installer, and repair the ESSO-LM installation by following the installer prompts. The repair process reinstalls the correct version of the support6.dll file.

ESSO-PR

Excluding Users and Groups from Forced Enrollment

ESSO-PR does not support forced enrollment exclusion with primary groups. Only non-primary Active Directory groups are supported. For more information on using this feature, see the Service Settings section in the *ESSO-PR Administrator's Guide*.

Active Directory Schema Error

Schema error (code 35) occurs when applying Active Directory storage settings in ESSO-PR under IIS 5.0 (Windows 2000 Server).

This error occurs when ESSO-PR Server v6.0 is installed in an environment that uses Windows 2000 Server (which uses IIS 5.0) and AD as the storage container. The security settings for VgoSelfServiceReset are configured under IIS 5.0.

On the System tab of the ESSO-PR Management Console, if a schema is configured to use AD as ESSO-PR's storage settings, once the Submit button is clicked the following schema error is returned:

"Error saving changes: Error saving schema: 0x35."

Error code 35 indicates that AD did not allow an update to the schema. You must enable "Write" access to the schema to correct this error. For more information about resolving this problem, see Microsoft's "Schema Updates Require Write Access to Schema in Active Directory" support article Q285172 for more information (http://support.microsoft.com/default.aspx?kbid=285172).

Upgrade Notes

If you are performing an upgrade from any previous version of ESSO-PR to version 11.1.1.5.0, perform the following upgrade steps:

1. Install ESSO-PR Server 11.1.1.5.0. See the section, Installing the ESSO-PR Server in the *ESSO-PR Server Installation and Setup Guide*.
2. After installation, apply the storage settings for the existing repository (created by the previous version of ESSO-PR) through the ESSO-PR Management Console’s Storage page (under the System tab).

   See the section, Configuring Service Storage in the *ESSO-PR Administrator's Guide* for more information. Once this is done, the old user base and enrollment and reset logs will continue to be used.
3. Reset the Anonymous Access Account.

During installation, the Windows User account for anonymous access in IIS Manager may be reset to the default IUSR_<computer name> account. If this occurs, it must be reset back to the Administrator account (or the previous account used).

To do this:

1. Open the IIS Manager on the ESSO-PR Server machine.
2. In the left tree pane, expand Internet Information Services > Web sites >Default Web sites.
3. Right-click on vGOSelfServiceReset and select Properties.
4. Select the Directory Security tab. Under Authentication and Access Control, click Edit.
5. Change the Windows User account for anonymous access back to the appropriate account, for example, the Administrator account.

Upgrading for SQL Server Users

Versions of ESSO-PR prior to 10.1.4.0.2 Fix Pack 1 did not adhere to case sensitivity when submitting Users page queries to SQL databases, which would result in an error message. See Installation and Configuration Notes in the *ESSO-PR Server Installation and Setup Guide* for a workaround for this issue that requires changing a design table heading manually.

ESSO-PR 10.1.4.0.2 Fix Pack 1 resolved this issue. However, depending on your upgrade path, your installation might still require this manual change. The following table illustrates the various upgrade paths for ESSO-PR and what to do based on the path you have taken.

Version/Upgrade Path	Issue	Workaround
11.1.1.2.0/New installation	Issue resolved	Not necessary
11.1.1.2.0/ Upgrade from 10.1.4.0.2 Fix Pack 1	Issue resolved	Not necessary
11.1.1.2.0/ Upgrade from 10.1.4.0.2 or prior	SQL Case Sensitivity	Rename Design Table(see the *ESSO-PR Server Installation and Setup Guide*.)

Product Documentation and Support

Documentation

The following documentation supports Oracle Enterprise Single Sign-on Suite Plus. For the latest versions of printed documentation, see the Oracle online documentation center.

Oracle Enterprise Single Sign-on Universal Authentication Manager

- *Oracle Enterprise Single Sign-on Universal Authentication Manager Administrator's Guide*
- *Oracle Enterprise Single Sign-on Universal Authentication Manager Installation Guide*
- *Oracle Enterprise Single Sign-on Universal Authentication Manager User Guide*
- *How-To: Using the ESSO-UAM Deployment Tools*

Oracle Enterprise Single Sign-on Logon Manager

- *Oracle Enterprise Single Sign-on Logon Manager Installation and Setup Guide*
- *Oracle Enterprise Single Sign-on Logon Manager User Guide*
- *Oracle Enterprise Single Sign-on Logon Manager Global Agent Settings Reference Guide*
- *Oracle Enterprise Single Sign-on Logon Manager Kiosk Manager Configuration Guide*
- *Deploying ESSO-LM with Microsoft Active Directory*
- *Deploying ESSO-LM with Microsoft ADAM*
- *Deploying ESSO-LM with an LDAP Directory*
- *Configuring the ESSO-LM Agent*
- *Packaging ESSO-LM for Mass Deployment*
- *Template Creation and Diagnostics for Windows Applications*
- *Template Creation and Diagnostics for Web Applications*
- *Template Creation and Diagnostics for Mainframe Applications*
- *Deploying ESSO-LM with the Windows Authenticator Version 2*
- *Using the Hidden Windows Response Utility*
- *Configuring ESSO-LM Event Logging with the IBM DB2 Database*
- *Configuring ESSO-LM Event Logging with MS SQL Server 2005*
- *Understanding the ESSO-LM Event Notification Service API*
- *Understanding the ESSO-LM Secondary Authentication API*
- *Using the Trace Controller Utility*
- *Strong Authenticator Configuration Guide*

Oracle Enterprise Single Sign-on Provisioning Gateway

- *Oracle Enterprise Single Sign-on Provisioning Gateway OIM User Guide*
- *Oracle Enterprise Single Sign-on Provisioning Gateway Certificate Setup Guide*
- *Oracle Enterprise Single Sign-on Provisioning Gateway Java SDK Guide*
- *Oracle Enterprise Single Sign-on Provisioning Gateway .NET SDK Guide*
- *Oracle Enterprise Single Sign-on Provisioning Gateway CLI Guide*
- *Oracle Enterprise Single Sign-on Provisioning Gateway Administrator's Guide*
- *Oracle Enterprise Single Sign-on Provisioning Gateway Installation and Setup Guide*
- *Oracle Enterprise Single Sign-on Provisioning Gateway SIM Integration and Installation Guide*
- *Oracle Enterprise Single Sign-on Provisioning Gateway TIM Integration and Installation Guide*

- *Oracle Enterprise Single Sign-on Provisioning Gateway NIM Integration and Installation Guide*
- *Oracle Enterprise Single Sign-on Provisioning Gateway Minimum Permissions Guide*

Oracle Enterprise Single Sign-on Anywhere

- *Oracle Enterprise Single Sign-on Anywhere Administrator's Guide*
- *Oracle Enterprise Single Sign-on Anywhere Installation and Setup Guide*
- *Oracle Enterprise Single Sign-on Anywhere User Guide*
- *Creating and Exporting an SSL Certificate for ESSO-Anywhere*

Oracle Enterprise Single Sign-on Suite Plus Reporting

- *Oracle Enterprise Single Sign-on Suite Plus Reporting Database Configuration Guide*
- *Oracle Enterprise Single Sign-on Suite Plus Reporting Installation and Setup Guide*
- *Oracle Enterprise Single Sign-on Suite Plus Reporting Administrator's Guide*
- *Oracle Enterprise Single Sign-on Suite Plus Reporting Event Table Guide*
- *Oracle Enterprise Single Sign-on Suite Plus Reporting Oracle Database Configuration Guide*
- *Configuring Enterprise Single Sign-on to Log Events for Reporting*

Oracle Enterprise Single Sign-on Password Reset

- *Oracle Enterprise Single Sign-on Password Reset User Guide*
- *Oracle Enterprise Single Sign-on Password Reset Administrator's Guide*
- *Oracle Enterprise Single Sign-on Password Reset Client Installation and Setup Guide*
- *Oracle Enterprise Single Sign-on Password Reset Server Installation and Setup Guide*
- *Oracle Enterprise Single Sign-on Password Reset Schema Extension Guide*
- *Configuring an Oracle 10g Database Instance for ESSO-PR*
- *Configuring SSL Support for the ESSO-PR Web Interface*
- *Configuring the Minimum Required Permissions for ESSO-PR*
- *Understanding the ESSO-PR Database Schema*

Support

For Oracle Enterprise Single Sign-on Suite Plus product support, see http://www.oracle.com/support/index.html.

To open a support request, see http://www.myoraclesupport.com.