Oracle® Enterprise Single Sign-On Suite Plus

Release Notes

Release 11.1.2.1

E27323-02

March 2013

ORACLE®

Oracle Enterprise Single Sign-On Suite Plus Release Notes, Release 11.1.2.1

E27323-02

Table of Contents

Oracle Enterprise Single Sign-On Suite Plus 11.1.2.1

Oracle® is releasing version 11.1.2.1 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.

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 11.1.2.1. Consider the following as you plan your installations:

- You must install Logon Manager prior to installing any other component.
- If you have a previous version of Kiosk Manager installed and are updating it with the Logon Manager 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' documentation for more detailed information.

What's New in Oracle Enterprise Single Sign-On Suite Plus 11.1.2.1

A number of features and improvements have been incorporated into Oracle Enterprise Single Sign-On Suite Plus 11.1.2.1. This section describes these additions. For more information on these features and settings, see the Oracle online documentation center and the online help systems for each suite component.

Supported Third-Party Software and Hardware Matrix

To determine which third-party software and hardware is supported in this release, please refer to the compatibility matrix accessible via the Oracle Support website at http://support.oracle.com.

Suite Documentation Has Been Streamlined

In this release, multiple guides containing information of a similar nature have been consolidated into larger guides. The following table describes this reorganization:

Previously Standalone Guide	*Target Guide in This Release*
Deploying Logon Manager with Microsoft Active Directory	*Deploying Logon Manager with a Directory-Based Repository*
Deploying Logon Manager with Microsoft AD LDS (ADAM)	
Deploying Logon Manager with an LDAP Directory	
Logon Manager Template Configuration and Diagnostics for Windows Applications	*Configuring and Diagnosing Logon Manager Application Templates*
Logon Manager Template Configuration and Diagnostics for Web Applications	
Logon Manager Template Configuration and Diagnostics for Mainframe Applications	

Logon Manager

Oracle Privileged Accounts Manager Integration

Logon Manager users can now check out privileged accounts managed by Oracle Privileged Account Manager, providing single sign-on functionality to systems accessed via Oracle Privileged Account Manager. For information on setting up this integration, see the "Oracle Privileged Account Manager Support in Logon Manager" section in the *Oracle Enterprise Single Sign-On Suite Plus Administrator's Guide.*

The AD LDS (ADAM) Synchronizer Now Supports Custom "People" Container Locations

The Logon Manager AD LDS (ADAM) synchronizer now permits you to specify a custom location for the "People" container. For more information on configuring this feature, see the guide *Deploying Logon Manager with a Directory-Based Repository*.

Google Chrome Support

Logon Manager now supports Web applications accessed via the Google Chrome browser, including resources protected by Oracle Access Manager.

ID Context Settings Added to Administrative Console

Settings that control the startup and refresh behaviors of the ID Context module have been added to the Oracle Enterprise Single Sign-On Suite Plus Administrative Console.

Universal Authentication Manager

Microsoft AD LDS (ADAM) Now Supported as a Data Repository

Microsoft AD LDS and Microsoft ADAM are now supported as data repositories by Universal Authentication Manager.

Instructions for deploying Universal Authentication Manager with either of these platforms are included in the *Universal Authentication Manager Administrator's Guide* and the Universal Authentication Manager section of the *Oracle Enterprise Single Sign-On Suite Plus Installation Guide*.

Universal Authentication Manager Client Language Selector

The Universal Authentication Manager client application now provides the ability to select the desired language from within the application. The appropriate language pack(s) must be installed for the languages to be available for selection.

Open Issues in Oracle Enterprise Single Sign-On Suite Plus 11.1.2.1

This section describes open issues in the current release of the Oracle Enterprise Single Sign-On Suite Plus and their workarounds, where applicable.

Logon Manager

Logon Manager May Not Respond On-The-Fly to Some Web Applications

Logon Manager may not respond on-the-fly to Web pages accessed via Google Chrome that contain multiple forms.

Additionally, Logon Manager may not respond on-the-fly to the following Web forms accessed via Mozilla Firefox and Google Chrome:

- Web pages where fields are not contained within a FORM element
- The netzero.net password change form

If you encounter this issue, create a Logon Manager application template for the affected Web application.

Logon Manager May Not Respond At All To Some Web Applications

Logon Manager may not respond at all to the following Web forms:

- **Google Chrome only:** Multi-frame Web pages to which the user navigated using the browser's **Back** button; refreshing the target page will allow Logon Manager to respond properly.
- **Google Chrome only:** The "Welcome to Google Chrome" sign-in page. Users must complete first time sign-in manually.
- **All browsers:** The papajohns.com logon form.

There are currently no workarounds for these issues, except as noted above.

Logon Manager Button Does Not Appear in Chrome's Title Bar

Logon Manager is currently unable to display its title bar button in the title bar of the Google Chrome browser.

There is currently no workaround for this issue.

Unable to Complete SmartCard Logon to a Kiosk Manager Session if Card Is Removed During PIN Entry

When logging on to a Kiosk Manager session with a PIN-protected SmartCard, removing the SmartCard while the PIN prompt is displayed causes the logon to fail. Entering the card PIN without the card present will result in an endless prompt for the PIN, requiring the user to cancel the logon in order to dismiss the PIN prompt.

There is currently no workaround for this issue.

Logon Manager Does Not Support Checking Out Oracle Privileged Account Manager-Protected Accounts That Have No Expiration Date

When Logon Manager is configured to integrate with Oracle Privileged Account Manager, checking out accounts that do not have a set expiration date is not supported.

There is currently no workaround for this issue.

Password Reset

On Windows 7, Password Reset Client Does Not Support Running Under Accounts Other than Local System

On Windows 7, Password Reset does not support modifying its configuration to run under a specified user account, rather than the Local System account. This feature is available on Windows XP only. Password Reset Server is not affected by this issue.

Installing the Password Reset Client on a 32-bit Windows 7 System Running Universal Authentication Manager and Configured for Automatic Logon Prevents Users From Logging On

On a workstation running Universal Authentication Manager and configured for automatic Windows logon, installing the Password Reset client prevents users from logging on to Windows. This issue only affects 32-bit editions of Windows 7.

If you are unable to log on in such a scenario, restart the machine in "Safe Mode" and disable the automatic logon feature.

Languages Missing From the Password Reset Tab in the Oracle Enterprise Single Sign-On Administrative Console

When setting up questions, the following languages are missing from the **Password Reset** tab in the Oracle Enterprise Single Sign-On Administrative Console:

- Chinese (Traditional)
- Danish
- Greek
- Hungarian
- Norwegian
- Portuguese (Portugal)
- Romanian
- Russian
- Slovak
- Swedish
- Thai
- Turkish

To work around this issue, access the questions configuration form using a Web browser at the following URL:

```
http://<server>:<port>/vgoselfservicereset/managementclient/questions.aspx
```

where `<server>` is the fully-qualified host name of the Password Reset Server machine and `<port>` is the number of the port on which Password Reset Server is listening for connections. If you have configured Password Reset Server for SSL connectivity, replace "`http://`" with "`https://`" in the above URL.

Password Reset Client: Reset Quiz Does Not Function on 64-bit Editions of Windows Server 2008 R2

On 64-bit editions of Windows Server 2008 R2 running the Password Reset Client, the password reset quiz does not function when accessed from the Windows logon screen.

There is currently no workaround for this issue.

Universal Authentication Manager

User Account Control Causes Challenge Questions Enrollment to Fail

When a non-administrative user attempts to enroll with the Challenge Questions logon method in a Kiosk Manager environment running on Windows 7 with default User Access Control settings, User Account Control will prevent the enrollment from completing.

To work around this issue, do one of the following:

- Disable User Account Control on the affected machine, or
- Enroll the affected user with the Challenge Questions logon method on the affected machine outside of the Kiosk Manager session (that is, terminate Kiosk Manager prior to initiating enrollment).

Technical Notes

The technical notes describe important technical information about this release.

Logon Manager

New User Setting Storage Schema (Active Directory Only)

Starting with version 11.1.2.1, when deployed on Microsoft Active Directory, Logon Manager configuration policies are now being stored in a repository location consistent with other user configuration objects of the class vGOSecret. Oracle highly recommends that you migrate to this new settings storage schema by enabling the **Use secure location for storing user settings** option found in the Active Directory synchronizer settings section of the Oracle Enterprise Single Sign-On Administrative Console.

When upgrading from a previous version of Logon Manager, **only** deploy this override after all instances of Logon Manager have been upgraded to version 11.1.2.1; otherwise, once Logon Manager 11.1.2.1 synchronizes with the repository, all previous versions will no longer be able to synchronize with the repository for that user.

Installing the Oracle Enterprise Single Sign-On Administrative Console on 64-Bit Windows May Fail If Older Version Is Present

If you're upgrading from an older version of the Oracle Enterprise Single Sign-On Administrative Console on 64-bit Windows, you must uninstall the older version before installing the latest version, otherwise the installation will fail.

Double Reboot Required when Upgrading a Kiosk Manager Installation

Due to an upgraded keyboard driver that ships with this version of Kiosk Manager, you will be prompted to reboot twice during the installation process - first to remove the old driver, and second to install the new driver.

Using Smart Cards with Logon Manager-Generated Keys

When the **Use default certificate for authentication** option (located in the Oracle Enterprise Single Sign-On Administrative Console under **Global Agent Settings > Authentication > Smart Card**) is set to **No**, users may be prompted to enter their PIN twice during the First Time Use (FTU) enrollment process. This is normal and necessary in order for Logon Manager to generate a keyset for the smart card. Subsequent authentications after FTU will only require a single PIN entry.

Event Manager

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

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.

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 since Citrix application windows are painted and no controls appear in 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

The NetManage NS/Elite emulator causes Logon Manager 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 the "Delete Local Cache" option is enabled).

Reflection 14 Sporadically Causes the Display of the Logon Manager Password Change Dialog Box on a Logon Screen

Logon Manager 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.

Win32/Injector.CFR Trojan Reported in the Agent Installer

Some MSI versions of the Logon Manager Agent installer exhibit false positives when scanned by anti-virus software during a Repair operation. The scan identifies the Win32/Injector.CFR trojan,

although in reality, no such virus is present in the installer.

Universal Authentication Manager

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:

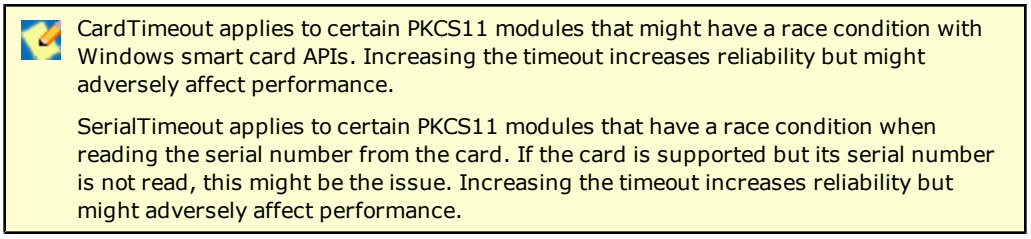
- The user can click **OK** and try inserting the card again.
- The administrator can add the following registry key and increase the timeout values:

  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.

Anywhere

Anywhere Does Not Support the Following Logon Manager Features

- **Oracle Access Manager integration.** Silent authentication to Oracle Access Manager is not supported.
- **Mozilla Firefox and Google Chrome.** Detection and response of Web applications accessed via the Mozilla Firefox and Google Chrome browsers is not supported.
- **Windows Authenticator v2 GINA**. The Windows Authenticator v2 GINA component is not supported. Anywhere does not support installing GINAs.
- **Windows Authenticator v2 Network Provider**. The Windows Authenticator v2 Network Provider component is not supported. Anywhere does not support installing Windows services.

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 7, and Windows Server 2008/2008R2 Prevents Anywhere from Running

Because Anywhere installs into the user's home folder, rather than the Program Files folder, the default security policy on Windows 7 and Windows Server 2008/2008 R2 deployments prevents 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 TechNet article: http://technet.microsoft.com/en-us/library/dd834830.aspx

Script Required for Microsoft IIS 6.0 Deployment

By default, Microsoft IIS 6.0 does not serve the three files types used by Anywhere (.application, .deploy, and .manifest). Administrators planning to deploy Anywhere using an IIS 6.0 Web Server must run the `IisAddMimeTypes.vbs` script included in the "Anywhere" folder of the Oracle Enterprise Single Sign-On Suite Plus master archive.

Attempting to deploy 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.