Oracle® Fusion Middleware

Enterprise Single Sign-On Suite Release Notes

11g Release 2 (11.1.2.2)

E37689-03

April 2014

ORACLE®

Oracle Fusion Middleware Enterprise Single Sign-On Suite Release Notes, 11g Release 2 (11.1.2.2)

E37689-03

Contents

3 Technical Notes for 11g Release 2 (11.1.2.2)

Preface

This document describes the changes and additions to each component of the Oracle Fusion Middleware Enterprise Single Sign-On Suite since the last release, as well as open issues and their workarounds (if applicable) present in this release. Technical notes describing specific behavior in particular deployment scenarios are also included.

Audience

This document is intended for experienced administrators responsible for the planning, implementation, and deployment of Oracle Fusion Middleware Enterprise Single Sign-On Suite applications.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Enterprise Single Sign-On Suite 11g Release 2 (11.1.2.2) documentation set:

- *Oracle Enterprise Single Sign-On Suite Installation Guide*
- *Oracle Enterprise Single Sign-On Suite Administrator's Guide*
- *Oracle Enterprise Single Sign-On Suite Secure Deployment Guide*
- *Oracle Enterprise Single Sign-On Suite User's Guide*
- *Deploying Logon Manager with a Directory-Based Repository*
- *Configuring and Diagnosing Logon Manager Application Templates*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

1

Oracle Enterprise Single Sign-On Suite 11g Release 2 (11.1.2.2)

Oracle® is releasing version 11.1.2.2 of Oracle Enterprise Single Sign-On Suite. These release notes provide important information about this release. The information in this document supplements and supersedes information in the related product documents.

1.1 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 11.1.2.2. 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 Programs** 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.

1.2 What's New In Oracle Enterprise Single Sign-On Suite 11.1.2.2

A number of features and improvements have been incorporated into Oracle Enterprise Single Sign-On Suite Plus 11.1.2.2. 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.

1.2.1 Java-Based Help System (Requires 32-Bit Java Runtime Environment)

Oracle Enterprise Single Sign-On Suite applications have been upgraded to a more robust Java-based online help engine. Due to this change, you must install the latest 32-bit edition of the Java Runtime Environment before installing any of the Suite applications.

1.3 Administrative Console

The following features and functions have been added or improved in this release of the Oracle Enterprise Single Sign-On Suite Administrative Console.

1.3.1 Support for Configuring Access Portal Application Policies

The Console introduces support for configuring form-fill application policies for the Oracle Access Portal Service. These policies can be imported directly into Oracle Access Manager.

For more information on configuring these policies, see the *Oracle Enterprise Single Sign-On Administrator's Guide*.

For more information on the Oracle Access Portal Service, see the *Oracle Access Manager Administrator's Guide*.

1.3.2 Support for Mapping Logon Manager Application Templates to Oracle Privileged Account Manager Targets

The Console introduces support for mapping Logon Manager application templates to Oracle Privileged Account Manager targets via the new **OPAM** tab.

For more information, see the Oracle Enterprise Single Sign-On Administrator's Guide.

1.4 Logon Manager

The following features and functions have been added or improved in this release of Logon Manager.

1.4.1 Windows Authenticator v2 Support in Kiosk Environments

The Kiosk Manager component of Logon Manager now supports the Windows Authenticator v2.

For specific configuration instructions, see the section "Configuring the Windows Authenticator Version 2" in the *Oracle Enterprise Single Sign-On Suite Administrator's Guide.*

1.4.2 Secondary Authentication Support in LDAP Authenticator v2

The LDAP Authenticator Version 2 now support secondary authentication on par with the Windows Authenticator Version 2. Recovery is supported via user passphrase, Active Directory SID, and LDAP directory entryUUID. Custom secondary authentication libraries that utilize the Logon Manager Secondary Authentication API are also supported.

For specific configuration instructions, see the section "Configuring the LDAP Authenticator Version 2" in the *Oracle Enterprise Single Sign-On Suite Administrator's Guide.*

1.4.3 LDAP Authenticator Version 1 Has Been Deprecated

The LDAP Authenticator Version 1 has been deprecated and is now included solely for legacy migration purposes. Oracle recommends that all LDAPAuth v1 deployments migrate to LDAPAuth v2.

For specific configuration instructions, see the section "Configuring the LDAP Authenticator Version 2" in the *Oracle Enterprise Single Sign-On Suite Administrator's Guide.*

1.4.4 Customizable "Pause Logon Manager" System Tray Option

The behavior of the "Pause Logon Manager" system tray option can now be customized by the administrator. The administrator can decide whether the option is enabled for each individual user, as well as configure a time-out period after which the feature disengages after the user engages it.

For more information, see the *Oracle Enterprise Single Sign-On Suite Administrator's Guide.*

1.4.5 Enhanced Administrative Rights for Credential Delegation

The administrator can now delete and revoke credential delegations for individual Logon Manager users.

For more information, see the *Oracle Enterprise Single Sign-On Suite Administrator's Guide.*

1.5 Universal Authentication Manager

The following features and functions have been added or improved in this release of Universal Authentication Manager.

1.5.1 Individual Logon Methods Configurable as Primary Authenticator in Logon Manager

Universal Authentication Manager logon methods can now be individually selected as the primary authenticator in Logon Manager. Administrators can now also configure a graded authentication scheme assigning different weights to each Universal Authentication Manager logon method individually.

1.5.2 Windows 7 x64 Support

Universal Authentication Manager now supports the 64-bit edition of Windows 7.

1.5.3 Kiosk Manager Support on Windows 7

Universal Authentication Manager can now be used as an authentication method in Kiosk Manager environments.

1.6 Password Reset

The following features and functions have been added or improved in this release of Password Reset.

1.6.1 Windows Server 2012 Support

Password Reset is now fully compatible with Windows Server 2012.

For deployment instructions, see the *Oracle Enterprise Single Sign-On Suite Installation Guide*.

1.6.2 Mobile Browser Support

Password Reset now supports the default browsers on iOS and Android devices.

1.7 Provisioning Gateway

The following features and functions have been added or improved in this release of Provisioning Gateway.

1.7.1 Windows Server 2012 Support

Provisioning Gateway is now fully compatible with Windows Server 2012.

For deployment instructions, see the *Oracle Enterprise Single Sign-On Suite Installation Guide*.

1.8 Anywhere

The following features and functions have been added or improved in this release of Anywhere.

1.8.1 Windows Authenticator Version 2 Support

Anywhere deployments can now utilize the Windows Authenticator Version 2 as the primary authenticator.

2

Open Issues in 11g Release 2 (11.1.2.2)

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

2.1 Open Issues Applicable to All Suite Applications

This section describes open issues present in all Oracle Enterprise Single Sign-On Suite applications in this release.

2.1.1 Unicode Characters Not Supported

Oracle Enterprise Single Sign-On Suite applications currently do not support Unicode characters.

2.2 Administrative Console

This section describes open issues in the current release of the Oracle Enterprise Single Sign-On Administrative Console.

2.2.1 Incorrect Error Message Displayed when Invalid OPAM Credentials Are Used

When configuring OPAM connectivity in the Administrative Console, entering invalid OPAM credentials results in a generic "401 - Unuthorized" error message, rather than a message indicating invalid credentials.

2.3 Logon Manager

This section describes open issues in the current release of Logon Manager.

2.3.1 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.

2.3.2 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.

2.3.3 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.

2.3.4 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.

2.3.5 Logon Manager Does Not Support Checking Out OPAM-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.

2.3.6 LDAP Authenticator Version 1 Support for Active Directory

When configuring the LDAPAuth v1 authenticator, Active Directory will not be present in the "Directory Type" drop-down menu.

To work around this issue, select **LDAP-Compliant Server** from the drop-down menu and enable the **Enable Domain Name Support** option.

2.3.7 The "Process" Option in mfrmlist.ini Prevents Mainframe Application Detection

Setting the `Process` option in the `mfrmlist.ini` file to a value other than `shared` causes Logon Manager to no longer detect mainframe applications it previously detected correctly.

To ensure Logon Manager properly detects your mainframe applications, do not set this option to a value other than `shared`.

2.3.8 Network Provider Installable with Incompatible Authenticators

It is possible to install the Network Provider component required for Windows Authenticator Version 2 and the SmartCard authenticator with other Logon Manager authenticators, which are not compatible with the Network Provider component. This can result in users being unable to authenticate to Logon Manager.

To work around this issue, ensure that you only install the Network Provider component with either the Windows Authenticator Version 2 (WinAuth v2) or the SmartCard authenticator.

2.3.9 Silent Credential Capture Does Not Store Credentials for Some Web Applications

The silent credential capture function may not successfully capture credentials for some Web applications.

To work around this issue, always check that the credentials have been successfully captured and stored in Logon Manager.

2.3.10 Fine-Grain Password Policies Not Supported

Logon Manager currently does not support the detection of password expiration defined in fine-grain password policies utilized in Windows Server 2008 and subsequent Windows Server editions; only domain-level password policies are supported.

To work around this issue, users whose password expiration was defined in a fine-grain password policy will need to change their passwords without the use of Logon Manager.

2.3.11 Delegated Credentials Not Injected If Delegation End Time is 12:00AM

If the end time for a credential delegation is set to 12:00AM, Logon Manager will not inject the delegated credentials when a delegatee attempts to access the target application.

To work around this issue, set the delegation end time to a value other than 12:00AM.

2.4 Password Reset

This section describes the open issues in the current release of Password Reset.

2.4.1 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.

2.4.2 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.

2.4.3 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.

2.4.4 On Windows 7 Deployments in Norwegian, Some Dialogs Appear in English

On Windows 7, when Password Reset is deployed in Norwegian, the initial enrollment screen, the initial password reset screen, and the “Forgot your password?” link on the Windows 7 logon page appear in English instead of Norwegian.

There is currently no workaround for this issue.

2.5 Provisioning Gateway

This section describes the open issues in the current release of Provisioning Gateway

2.5.1 Unable to Check Out Account Delegated via Group Membership

Attempting to check out a delegated account whose delegation was granted via a group membership results in a 404 error.

There is currently no workaround for this issue.

2.5.2 Active Directory Users Must Use Full Name to Authenticate to the OPAM Server

Active Directory users must use their full name instead of their account name (user ID) to authenticate to the OPAM server; otherwise, authentication will fail.

There is currently no workaround for this issue.

2.5.3 Template Mapping List Appears Blank After Mapping a Template

In the Provisioning Gateway console, the "Template Mapping" list may appear blank after mapping a template.

To work around this issue, refresh the page after mapping a template to repopulate the "Template Mapping" list.

2.6 Universal Authentication Manager

This section describes the open issues present in the current release of Universal Authentication Manager.

2.6.1 BIO-Key Control Panel Does Not Open When No Reader Is Configured (64-Bit Systems Only)

On 64-bit systems, if no fingerprint reader has been configured and the user attempts to enroll with the Fingerprint logon method, Universal Authentication Manager will prompt the user to configure the reader, but acknowledging the prompt does not open the BIO-Key control panel. This issue does not affect 32-bit systems.

To work around this issue, ensure the fingerprint reader is correctly configured before enrolling with the Fingerprint logon method.

2.6.2 Reboot Required Immediately After Adding Or Removing a UAM-Enabled Machine To/From a Windows Domain

When adding or removing a machine that uses Universal Authentication Manager for strong authentication to or from a domain, you must reboot immediately after adding or removing the machine; otherwise, strong authentication will not function until you reboot.

3

Technical Notes for 11g Release 2 (11.1.2.2)

This section contains the technical notes for the current release of the Oracle Enterprise Single Sign-On Suite.

3.1 Administrative Console

This section contains the technical notes for the current release of the Enterprise Single Sign-On Suite Administrative Console.

3.1.1 Templates Exported to .INI File Must use Unicode Encoding if Imported into Oracle Access Manager

If you are exporting application templates or policies to an .INI file for import into Oracle Access Manager, you must select the **Unicode** (or **Unicode big endian)** encoding when saving the .INI file. Other encodings are not supported by Oracle Access Manager.

3.2 Logon Manager

This section contains the technical notes for the current release of Logon Manager.

3.2.1 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.

3.2.2 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.

3.2.3 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.

3.2.4 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.

3.2.5 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.

3.2.6 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.

3.2.7 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.

3.2.8 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]

3.2.9 "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.

Note: Clicking "End program" may result in credentials not being cleaned up (if the "Delete Local Cache" option is enabled).

3.2.10 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.

3.2.11 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.

3.3 Universal Authentication Manager

This section contains technical notes for the current release of Universal Authentication Manager.

3.3.1 Disable Kiosk Manager Credential Caching When Integrating with Kiosk Manager

In this release, Kiosk Manager defaults to using cached credentials to authenticate the user session (the **Use Cached Credentials** option in the Administrative Console now defaults to **Yes**).

If you are using Universal Authentication Manager as a logon method for authenticating to Kiosk Manager, you must explicitly set the **Use Cached Credentials** option to **No**; otherwise, authentication via Universal Authentication Manager will not be possible.

3.3.2 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):

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

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

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

Note: 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.

3.3.3 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.

3.3.4 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.

3.4 Anywhere

This section contains technical notes for the current release of Anywhere.

3.4.1 Anywhere Does Not Support Certain Logon Manager Features

The following Logon Manager features are not supported by Anywhere:

- 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.

Note: 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.

3.4.2 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

3.4.3 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.