

Oracle® Fusion Middleware

Release Notes for Enterprise Single Sign-On Suite

11g Release 2 (11.1.2.3)

E55058-01

April 2015

E55058-01

Copyright © 1998, 2015, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

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

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware 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 that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

The information contained in this document is for informational sharing purposes only and should be considered in your capacity as a customer advisory board member or pursuant to your beta trial agreement only. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle Master Agreement, Oracle License and Services Agreement, Oracle PartnerNetwork Agreement, Oracle distribution agreement, or other license agreement which has been executed by you and Oracle and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced, or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

Contents

Audience.....	vii
Documentation Accessibility	vii
Related Documents	vii
Conventions	viii
1 Oracle Enterprise Single Sign-On Suite 11g Release 2 (11.1.2.3)	
1.1 Installation and Upgrade Notes.....	1-1
1.2 What's New In Oracle Enterprise Single Sign-On Suite 11.1.2.3.....	1-1
1.2.1 Windows XP and Windows Server 2003 No Longer Supported.....	1-1
1.2.2 Windows 8 and Windows 8.1 Support.....	1-1
1.3 Administrative Console	1-2
1.3.1 Oracle Access Portal Form Masking Settings	1-2
1.4 Logon Manager	1-2
1.4.1 Microsoft User Interface Automation API Support.....	1-2
1.5 Universal Authentication Manager	1-2
1.5.1 Windows Server 2012 R2 Repository Support	1-2
1.5.2 Windows 8/8.1 Virtual Smart Card Support	1-2
1.5.3 Required BIO-Key Middleware Version Increased to 1.12.....	1-2
1.5.4 SmartCard PIN Mode Enhancements.....	1-2
1.5.5 Morpho ypsID 6.4.0 Support.....	1-3
1.5.6 Token Settings Enhancements	1-3
1.5.7 New Language: French (Canada).....	1-3
2 Open Issues in 11g Release 2 (11.1.2.3)	
2.1 Open Issues Applicable to All Suite Applications	2-1
2.1.1 Unicode Characters Not Supported.....	2-1
2.2 Administrative Console	2-1
2.2.1 Incorrect Error Message Displayed when Invalid OPAM Credentials Are Used.....	2-1
2.3 Logon Manager	2-1
2.3.1 Logon Manager May Not Respond On-the-Fly to Some Web Applications	2-1
2.3.2 Logon Manager May Not Respond At All to Some Web Applications.....	2-2
2.3.3 Unable to Complete SmartCard Logon to a Kiosk Manager Session if Card Is Removed During PIN Entry	2-2
2.3.4 Logon Manager Does Not Support Checking Out OPAM-Protected Accounts That Have No Expiration Date	2-2
2.3.5 The "Process" Option in mfrmlist.ini Prevents Mainframe Application Detection ...	2-2

2.3.6	Network Provider Installable with Incompatible Authenticators.....	2-2
2.3.7	Silent Credential Capture Does Not Store Credentials for Some Web Applications	2-2
2.3.8	Fine-Grain Password Policies Not Supported.....	2-3
2.3.9	Delegated Credentials Not Injected If Delegation End Time is 12:00AM	2-3
2.4	Password Reset.....	2-3
2.4.1	On Windows 7, Password Reset Client Does Not Support Running Under Accounts Other than Local System	2-3
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	2-3
2.4.3	Password Reset Client: Reset Quiz Does Not Function on 64-bit Editions of Windows Server 2008 R2	2-3
2.4.4	On Windows 7 Deployments in Norwegian, Some Dialogs Appear in English.....	2-4
2.5	Provisioning Gateway	2-4
2.5.1	Unable to Check Out Account Delegated via Group Membership.....	2-4
2.5.2	Active Directory Users Must Use Full Name to Authenticate to the OPAM Server .	2-4
2.5.3	Template Mapping List Appears Blank After Mapping a Template	2-4
2.6	Universal Authentication Manager.....	2-4
2.6.1	Prompted Enrollment Requires Disabling The Sign-On Animation on Windows 8/8.1 Systems	2-4
2.6.2	Blank Passwords Cause Authentication Failure	2-4
2.6.3	On Windows 8/8.1, Metro Authentication Dialogs May Appear On the Desktop ...	2-5

3 Technical Notes for 11g Release 2 (11.1.2.3)

3.1	Administrative Console	3-1
3.1.1	Templates Exported to .INI File Must use Unicode Encoding if Imported into Oracle Access Manager	3-1
3.2	Logon Manager	3-1
3.2.1	New User Setting Storage Schema (Active Directory Only)	3-1
3.2.2	Double Reboot Required when Upgrading a Kiosk Manager Installation	3-1
3.2.3	Using Smart Cards with Logon Manager-Generated Keys.....	3-2
3.2.4	Logon Manager May Not Respond to Some Applications Running with Elevated Privileges	3-2
3.2.5	Event Manager	3-2
3.2.6	Backup/Restore	3-2
3.2.7	Citrix Published Applications Using SendKeys: Cannot Use "Set Focus" Feature	3-2
3.2.8	Citrix Published Applications: SendKeys Does Not Process "Enter" or "Tab" Properly... 3-2	
3.2.9	"End Program" Message Displayed	3-3
3.2.10	Reflection 14 Sporadically Causes the Display of the Logon Manager Password Change Dialog Box on a Logon Screen	3-3
3.2.11	Win32/Injector.CFR Trojan Reported in the Client Installer	3-3
3.3	Universal Authentication Manager.....	3-3
3.3.1	Reboot Required Immediately After Adding Or Removing a UAM-Enabled Machine To/From a Windows Domain	3-3
3.3.2	Error When Using RSA Authentication Client 2.0 Smart Card Middleware	3-3
3.3.3	PKCS11 Card Failure with Remote Desktop Lock.....	3-4
3.3.4	Incompatibility Between Crescendo C700 Proximity Card and Omnikey 5X25 Proximity Card Reader	3-4

3.4	Anywhere.....	3-4
3.4.1	Anywhere Does Not Support Certain Logon Manager Features	3-4
3.4.2	Default Security Policy on Windows 7, and Windows Server 2008/2008R2 Prevents Anywhere from Running	3-5
3.4.3	Script Required for Microsoft IIS 6.0 Deployment.....	3-5

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 that have purchased support 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 (11.1.2.3) documentation set:

- *Installing Oracle Enterprise Single Sign-On Suite*
- *Administering Oracle Enterprise Single Sign-On Suite*
- *Securing Oracle Enterprise Single Sign-On Suite*
- *Accessing Applications with Oracle Enterprise Single Sign-On Suite*
- *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.
<i>italic</i>	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.

Oracle Enterprise Single Sign-On Suite 11g Release 2 (11.1.2.3)

Oracle® is releasing version 11.1.2.3 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 11.1.2.3. Consider the following as you plan your installations:

- Installation on Windows XP is no longer possible.
- 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 11.1.2.3

A number of features and improvements have been incorporated into Oracle Enterprise Single Sign-On Suite 11.1.2.3. 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 Windows XP and Windows Server 2003 No Longer Supported

The Windows XP operating system is no longer supported; installing the Oracle Enterprise Single Sign-On Suite 11.1.2.3 on Windows XP is no longer possible.

1.2.2 Windows 8 and Windows 8.1 Support

Oracle Enterprise Single Sign-On Suite now supports the Windows 8 and Windows 8.1 operating systems.

1.3 Administrative Console

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

1.3.1 Oracle Access Portal Form Masking Settings

The Proxy tab within a Web application template's form definition now contains settings to enable form masking in Oracle Access Portal. For more information, see the guides *Configuring and Diagnosing Logon Manager Application Templates* and *Administering Oracle Enterprise Single Sign-On Suite*.

1.4 Logon Manager

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

1.4.1 Microsoft User Interface Automation API Support

Logon Manager now supports the Microsoft User Interface Automation (MS UIA) API, allowing detection and interaction with Java, SAP, and Windows 8/8.1 Metro ("Modern UI") applications. The MS UIA API to programmatically access the fields and controls of those applications.

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 Windows Server 2012 R2 Repository Support

Universal Authentication Manager can now store data in an Active Directory or AD LDS repository running on the Windows Server 2012 R2 operating system. For configuration instructions, see the guide *Installing Oracle Enterprise Single Sign-On Suite*.

1.5.2 Windows 8/8.1 Virtual Smart Card Support

On Windows 8/8.1 systems, Universal Authentication Manager now allows the use of hardware-backed virtual smart cards. To utilize this functionality, the target machine must have a functional Trusted Platform Module.

1.5.3 Required BIO-Key Middleware Version Increased to 1.12

Universal Authentication Manager now requires version 1.12 of the BIO-Key middleware. Prior versions are not supported and must be removed before installing Universal Authentication Manager.

1.5.4 SmartCard PIN Mode Enhancements

The PIN mode for the Smart Card authentication method has been enhanced as follows

- Certificates that do not allow "Key Encipherment" key usage are now allowed by default. A new setting, "Strict Key Cipher," has been added to revert to the old (strict) behavior.

- The “Session Key | Prompt Always” option is now enabled by default.

1.5.5 Morpho ypsID 6.4.0 Support

Universal Authentication Manager now supports the Morpho ypsID 6.4.0 (formerly Sagem) middleware, which enables fingerprint-on-smart-card (substituting a fingerprint for the PIN) functionality. A .REG configuration file is now included to facilitate this. For more information, see the guide *Administering Oracle Enterprise Single Sign-On Suite*.

1.5.6 Token Settings Enhancements

The smart card and proximity token settings each have been enhanced to include a new "Authenticator token description" setting (a "Global Branding" setting). These descriptions are now also enabled by default. For more information, see the guide *Administering Oracle Enterprise Single Sign-On Suite*.

1.5.7 New Language: French (Canada)

Universal Authentication Manager now supports the Canadian variant of the French language. For configuration instructions, see the guide *Installing Oracle Enterprise Single Sign-On Suite*.

Open Issues in 11g Release 2 (11.1.2.3)

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 - Unauthorized" 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 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.

2.3.4 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.

2.3.5 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`.

2.3.6 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.

2.3.7 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.

2.3.8 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.

2.3.9 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 Prompted Enrollment Requires Disabling The Sign-On Animation on Windows 8/8.1 Systems

On Windows 8/8.1 systems, a "Welcome" animation plays the first time a user logs on to the target system. Because this animation severely interferes with Universal Authentication Manager's "Prompted Enrollment" feature, the Universal Authentication Manager installer will disable it using the local policy registry settings. However, certain environments may require that you manually disable the animation using your organization's group policy configuration.

2.6.2 Blank Passwords Cause Authentication Failure

The "Limit local account use of blank passwords to console logon only" windows security policy prevents Windows authentication of users with blank passwords. Even though Universal Authentication Manager itself can initially authenticate such users, potentially allowing them to enroll, re-authentication and subsequent strong (Universal Authentication Manager-based) authentication attempts of such a user

account will fail. To restore normal operation, assign a Windows password to the affected user account.

Oracle severely discourages disabling this Windows policy as doing so will severely compromise the security of your environment.

2.6.3 On Windows 8/8.1, Metro Authentication Dialogs May Appear On the Desktop

When authenticating to a Metro application on a Windows 8/8.1 system, the authentication dialog may appear on the desktop instead of over the target Metro application. To work around this issue, use the Alt+Tab key combination to switch to the authentication dialog.

Technical Notes for 11g Release 2 (11.1.2.3)

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 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.

3.2.3 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.

3.2.4 Logon Manager May Not Respond to Some Applications Running with Elevated Privileges

Logon Manager may be unable to respond to some applications running with highly elevated privileges. For example, when logged in as the built-in Administrator account, and the local security policy is set to disable Admin Approval Mode for the built-in Administrator account, the resulting privilege elevation prevents Logon Manager, which itself is a medium-privilege application, from hooking into the target applications running with elevated privileges.

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 Client Installer

Some MSI versions of the Logon Manager 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 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.

3.3.2 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.

