Oracle® Enterprise Single Sign-On Suite Plus

Release Notes

Release 11.1.2

E27323-02

August 2012

ORACLE®

Oracle Enterprise Single Sign-On Suite Plus Release Notes, Release 11.1.2

E27323-02

Table of Contents

Oracle Enterprise Single Sign-On Suite Plus 11.1.2

Oracle® is releasing version 11.1.2 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. 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

A number of features and improvements have been incorporated into Oracle Enterprise Single Sign-On Suite Plus 11.1.2. 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.

Now Shipping Reports for Oracle Business Intelligence Publisher

The Oracle Enterprise Single Sign-On Suite Plus Reporting Console has been removed in favor of integration with Oracle Business Intelligence Publisher; report files supporting this integration are now shipping with the Suite.

Reporting Now Captures Session (IDContext) Parameter Events

The Oracle Enterprise Single Sign-On Suite Plus Reporting Service now captures and stores client session attributes such as the machine's operating system version, IP address, firewall state, anti-virus software state, if installed, and others. For more information, see the *Oracle Enterprise Single Sign-On Suite Plus Administrator's Guide*.

Connector Plug-Ins No Longer Distributed with Oracle Enterprise Single Sign-On Suite Plus

Connector plug-ins for interfacing Provisioning Gateway with Oracle Identity Manager, IBM Tivoli Identity Manager, and Sun Identity Manager are no longer being shipped as part of the Oracle Enterprise Single Sign-On Suite Plus. The connectors can be found at the following locations:

- **Oracle Identity Manager connector:** download patch ID 14006614 from Oracle Support.
- **IBM Tivoli Identity Manager and Sun Identity Manager connectors:** retrieve from the "ESSO Provisioning Gateway 11.1.1.5.1" folder in the Oracle Enterprise Single Sign-On Suite Plus Release 11.1.1.5.1 ZIP archive available via Oracle eDelivery.

Expanded List of Supported Languages

Language support for the Oracle Enterprise Single Sign-On Suite Plus applications has been expanded to the following languages:

- English
- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Danish
- Dutch
- Finnish
- French
- German
- Greek
- Hungarian
- Italian
- Japanese

- Korean
- Norwegian
- Polish
- Portuguese (Brazil)
- Portuguese (Portugal)
- Romanian
- Russian
- Slovak
- Spanish
- Swedish
- Thai
- Turkish

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*
Oracle Enterprise Single Sign-On Logon Manager Installation and Setup Guide	*Oracle Enterprise Single Sign-On Suite Plus Installation Guide*
Oracle Enterprise Single Sign-On Provisioning Gateway Server Installation and Setup 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 Universal Authentication Manager Installation and Setup Guide	
Oracle Enterprise Single Sign-On Anywhere Console Installation and Setup Guide	
Configuring SSL Support for the Password Reset Web Interface	
Packaging Logon Manager for Mass Deployment	
Oracle Enterprise Single Sign-On Provisioning Gateway Administrator's Guide	*Oracle Enterprise Single Sign-On Provisioning Gateway Administrator's Guide*
Oracle Enterprise Single Sign-On Provisioning Gateway Certificate Setup Guide	
Oracle Enterprise Single Sign-On Provisioning Gateway Minimum Permissions Guide	

Previously Standalone Guide	*Target Guide in This Release*
Understanding the Password Reset Database Schema	*Oracle Enterprise Single Sign-On Suite Plus Administrator's Guide*
Configuring Logon Manager Event Logging with the IBM DB2 Database	
Configuring Logon Manager Event Logging with Microsoft SQL Server 2005	
Creating and Exporting an SSL Certificate for Anywhere	
Using the Hidden Window Response Utility	
Understanding the Logon Manager Secondary Authentication API	
Configuring the Logon Manager Agent	
Oracle Enterprise Single Sign-On Logon Manager Administrative Console Online Help	
Oracle Enterprise Single Sign-On Password Reset Management Console Guide	
Oracle Enterprise Single Sign-On Anywhere Administrator's Guide	
Oracle Enterprise Single Sign-On Suite Plus Reporting Configuration Guide	
Oracle Enterprise Single Sign-On Logon Manager Global Agent Settings Reference Guide	
Oracle Enterprise Single Sign-On Password Reset Schema Extension Guide	
Oracle Enterprise Single Sign-On Provisioning Gateway Administrator's Guide	
*Deploying Logon Manager with Windows Authenticator Version 2 **	
Understanding the Logon Manager Event Notification API	
Using the Trace Controller Utility	
Configuring an Oracle 10g Database Instance for Password Reset	
Oracle Enterprise Single Sign-On Suite Plus Secure Deployment Guide	New in this release.
Oracle Enterprise Single Sign-On Provisioning Gateway CLI Guide	*Oracle Enterprise Single Sign-On Provisioning Gateway Command Line Interface Guide*

Previously Standalone Guide	*Target Guide in This Release*
Oracle Enterprise Single Sign-On Provisioning Gateway Java CLI Guide	*Oracle Enterprise Single Sign-On Logon Manager User's Guide*
Oracle Enterprise Single Sign-On Provisioning Gateway .NET CLI Guide	
Oracle Enterprise Single Sign-On Logon Manager User's Guide	
Oracle Enterprise Single Sign-On Password Reset User's Guide	
Oracle Enterprise Single Sign-On Anywhere User's Guide	
Oracle Enterprise Single Sign-On Logon Manager Getting Started Guide	No longer shipped.
Oracle Enterprise Single Sign-On Password Reset Getting Started Guide	
Oracle Enterprise Single Sign-On Universal Authentication Manager Getting Started Guide	
Oracle Enterprise Single Sign-On Provisioning Gateway Getting Started Guide	
Oracle Enterprise Single Sign-On Anywhere Getting Started Guide	
Oracle Enterprise Single Sign-On Suite Plus Reporting Getting Started Guide	

* Some information from this guide has also been incorporated into the new *Oracle Enterprise Single Sign-On Suite Plus Secure Deployment Guide*.

Logon Manager

Transparent Session Integration with Oracle Access Manager and Identify Context Now Supported

Logon Manager now silently authenticates to Oracle Access Manager and initiates a session propagated to the user's Web browser (Internet Explorer and Mozilla Firefox are supported). Logon Manager supplies Identify Context client claims as part of this session. For more information, see the "Oracle Access Manager Support in Logon Manager" section of the *Oracle Enterprise Single Sign-On Suite Plus Administrator's Guide*.

Mozilla Firefox Now Supported via an Extension Plug-In

Logon Manager now interfaces with the Mozilla Firefox browser via an .xpi extension rather than a Gecko-based programmatic hook, providing forward compatibility and extensibility.

Smart Cards Now Supported on Windows 7

Logon Manager's smart card authenticator now supports Windows 7.

Siemens Smart Cards Now Supported

Logon Manager's smart card authenticator now supports Siemens smart cards.

A Utility Has Been Added for Interfacing Kiosk Manager with Caregiver Mobility and Oracle VDI Environments

The Kiosk Manager plug-in for Logon Manager now supports a utility that interfaces with Caregiver Mobility and Oracle VDI environments, allowing health-care professionals to log on to kiosk systems to access location-specific information, such as patient data or other local resources pertinent to the kiosk system's location.

Repository Authentication via Smart Card Certificate Now Supported (Active Directory and ADAM/AD-LDS Only)

When deployed on Microsoft Active Directory or Microsoft ADAM/AD-LDS, Logon Manager now allows the user to authenticate to the repository with the certificate stored on the smart card with which they already authenticate to Logon Manager.

Local User Settings Now Stored in a Location Consistent with Other Logon Manager User Data (Active Directory)

When deployed with Microsoft Active Directory, Logon Manager now stores its configuration and other user settings in a location consistent with all other user objects of class vGoSecret.

Windows Authenticator Version 1 (WinAuth v1) Deprecated

The Windows Authenticator version 1 (WinAuth v1) authenticator plug-in has been deprecated in this release and is now provided for legacy migration purposes only. Do **not** use this authenticator unless explicitly instructed to do so by Oracle Support.

AES (MS CAPI) Is Now the Default Encryption Algorithm; Legacy Algorithms Deprecated

The AES (MS CAPI) encryption algorithm is now the default and standard encryption algorithm used by Logon Manager and is supported on Window XP / Windows Server 2003 and all later Windows editions. All other algorithms previously supported by Logon Manager have been deprecated and are now provided for legacy migration purposes only. Do **not** use any of the legacy algorithms unless explicitly instructed to do so by Oracle Support.

Roaming Profiles Deprecated

The support for roaming profiles has been deprecated and is now provided for legacy migration purposes only. Do **not** install this feature unless explicitly instructed to do so by Oracle Support.

Password Reset

Password Reset Client-Side Software Is Now Part of the Logon Manager Installer

The Password Reset client-side software has been merged into the Logon Manager installer package and is no longer provided as a separate installer. It is, however, still possible to install the Password Reset client-side software standalone (that is, without installing Logon Manager); for instructions, see the *Oracle Enterprise Single Sign-On Suite Plus Installation Guide.*

Password Reset Administration Now Part of the Oracle Enterprise Single Sign-On Administrative Console

All Password Reset administrative tasks have been merged into the Oracle Enterprise Single Sign-On Administrative Console and are now available under the **Password Reset** tab of the Console.

Provisioning Gateway

Credential Delegation

Users can now securely delegate their credentials to other Oracle Enterprise Single Sign-On Suite Plus users for a specific period of time, for example, when going on vacation or an extended medical leave.

Universal Authentication Manager

Windows 7 Now Supported (32-Bit Only)

Universal Authentication Manager now supports Windows 7 in 32-bit environments, including a new Microsoft Credential Provider-compliant logon mechanism.

Knowledge-Based Authentication Now Supported via the Challenge Questions Logon Method

Universal Authentication Manager now includes the Challenge Questions logon method, a knowledge-based authenticator that allows users to authenticate to Universal Authentication Manager by answering a series of quiz questions. In enterprise mode, Universal Authentication Manager can also synchronize with Password Reset, providing portability to the quiz enrollment data as well as the ability to customize the quiz questions and their weights.

For more information, see the *Universal Authentication Manager Administrator's Guide*.

Kiosk Manager Integration

You can now use Universal Authentication Manager logon methods (except Challenge Questions; unless user has previously enrolled in Challenge Questions prior to authenticating to Kiosk Manager) to lock/unlock Kiosk Manager sessions. You can also enroll with Universal Authentication Manager logon methods (except Challenge Questions) when first logging on to a Kiosk Manager session as well as when you launch Universal Authentication Manager from within a Kiosk Manager session.

For more information, see the *Universal Authentication Manager Administrator's Guide*.

Roaming Credentials Now Supported; Repository Data Storage, Synchronization, and Security Now Consistent with Logon Manager

Universal Authentication Manager now supports full portability of user enrollment data in enterprise mode. Universal Authentication Manager also now shares the same data storage and synchronization mechanism with Logon Manager and can use the same repository as Logon Manager.

Repository preparation and configuration steps have changed in this release; for more information, see the *Universal Authentication Manager Administrator's Guide*.

Simple Auditing

New simple auditing solution based on logging added for authentication event auditing.

BIO-key Support Upgraded to Version 1.10

The Fingerprint logon method has been upgraded to support BIO-key 1.10. Version 1.9 is no longer supported.

BioAPI Support Removed

The BioAPI logon method is no longer supported and has been removed.

New Policy Settings for the Fingerprint Logon Method

The Fingerprint logon method now allows you to require a PIN, set a minimum PIN length, and specify characters allowed in the PIN via respective policy settings.

Universal Authentication Manager PIN Mode for the Fingerprint Logon Method (Required by Default)

The Fingerprint logon method now supports the use of a Universal Authentication Manager-generated PIN. Additionally, a PIN is now required by default.

Cherry Dual-Mode Card Readers Now Supported with MIFARE-Compliant Proximity Tokens)

The Proximity Card logon method now supports Cherry dual-mode card readers when used with MIFARE-compliant proximity tokens.

PIN Is Now Mandatory for Smart Cards

The Smart Card logon method now requires a PIN at all times; the "No PIN" option has been removed.

New Policy Settings for Smart Cards

The Smart Card logon method now allows you to specify a PIN type (card-based or Universal Authentication Manager-generated), a minimum PIN length, and the characters allowed in the PIN. The "PIN Required" setting has been removed as PIN is now mandatory for smart cards.

Security Strengthened for Smart Cards in Card PIN Mode

In order to use the Smart Card logon method in Card PIN mode, a certificate is now required. Additionally, PKI operations are now used to protect the logon method's authenticator key.

System-Wide Policy Security Improvements

Universal Authentication Manager user policy settings are now fully portable. Administrative settings have been removed and user policies are now enforced in local mode.

Open Issues in Oracle Enterprise Single Sign-On Suite Plus 11.1.2

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

When Upgrading from a Previous Version of Logon Manager on a 64-Bit System, the Installation Cannot Continue if the Microsoft Visual C++ 2008 Redistributable is Not Installed

When upgrading from a previous version of Logon Manager on a 64-bit edition of Windows, the Logon Manager installer erroneously checks for the presence of the Microsoft Visual C++ 2008 Redistributable libraries, even though Logon Manager requires the Microsoft Visual C++ 2010 Redistributable library to function. If the Microsoft Visual C++ 2008 is not present on the target machine, the installation will not continue. This issue does not occur on 32-bit editions of Windows.

To work around this issue, install the Microsoft Visual C++ 2008 Redistributable before running the Logon Manager installer. You can then uninstall the 2008 version of the redistributable, as it is not required by Logon Manager to function.

Failed Logons to the Repository Are Counted Twice by Active Directory when Not Using a Fully Qualified User Name

When a user, while authenticating to the repository, enters an incorrect password and a user name that is not fully qualified (i.e., does not include the domain name), the failed logon attempt will be counted as two bad logons by Active Directory. This is because Logon Manager attempts to authenticate to the repository twice, using both the legacy NT4 "domain/user" format and the principal "user@domain" format to resolve the ambiguity in the user name.

If enough bad logon attempts are made, the user's account will be locked out in only half the number of attempts set as the account lockout threshold in the domain policy.

There is currently no workaround for this issue.

Synchronization with the Repository Fails When Logon Manager Is Configured to Use Smart Card Certificate for Repository Authentication and Card Is Unavailable

When Logon Manager is configured to use a smart card certificate to authenticate to the repository, fallback to a user name and password will not occur when the card is removed/unavailable or the card reader is disconnected from the system.

There is currently no workaround for this issue. You may choose to configure Logon Manager to use another repository authentication method.

Warning Dialogs Appear and Repository Synchronization Fails When Kiosk Manager Session Is Locked by Removing the Smart Card

When Logon Manager is configured to authenticate to the repository using a smart card certificate and the Kiosk Manager session is locked by removing the Smart Card, the "Insert

Smart Card" dialog appears. The user must click "Cancel" to dismiss the dialog. Then a "Logon Manager Failed to Log On to Directory" warning appears, which the user must also dismiss.

If any modifications are made to the user's credentials and Logon Manager is configured to use the card's certificate to authenticate to the repository, synchronization with the repository fails and the changes are not stored in the repository.

There is currently no workaround for this issue.

When Network Traffic Is High, Credential Modifications and Deletions May Not Immediately Synchronize to the Repository

When deployed on a network with high amounts of traffic to/from the repository, credential modifications and deletions performed on an end-user workstation may not be immediately synchronized to the repository.

To work around this issue, wait a few minutes before refreshing the credential list in Logon Manager.

Silent Credential Capture Intermittently Fails to Capture Network Share Credentials on Windows 7 and Windows Server 2008/2008 R2

On Windows 7 and Windows Server 2008/2008 R2 systems, the silent credential capture feature intermittently fails to capture credentials from a Windows network share authentication dialog. If the user attempts to cancel the credential capture process, Logon Manager freezes.

There is currently no workaround for this issue.

Member Templates in a Credential Sharing Group Become Corrupted if Not Published Together

If you individually publish a template that is a member of a credential sharing group, other member templates in that group may become corrupted.

To prevent this issue from occurring, always import all member templates from the repository and republish them together after making your changes to any of the member templates.

Disabling the Kiosk Manager Setting "Lock session when screen saver times out" Has No Effect when Session Is Unlocked via Smart Card

Even when the Kiosk Manager setting "Lock session when screen saver times out" is set to "No," Kiosk Manager still locks the session when the screen saver timeout expires if the session was unlocked using a smart card.

There is currently no workaround for this issue.

First Time Use Wizard Cannot Be Completed If the Kiosk Manager Session Is Unlocked with a Siemens Smart Card

If you log on to a Kiosk Manager machine for the first time by unlocking the session with a Siemens smart card, you will not be able to complete the First Time Use wizard.

There is currently no workaround for this issue.

When Using Mozilla Firefox, Logon Manager Does Not Respond to Web Pages in Which Credential Field Elements Are Not Enclosed by a Form Element

When using the Mozilla Firefox browser, Logon Manager fails to detect and respond to Web pages in which the field elements comprising the logon form are not enclosed by a form element.

To work around this issue, specify the value of -1 instead of the form element's name or ordinal ID when configuring field matching. This will cause Logon Manager to treat the HTML document body as the form container and thus correctly detect the target field elements. A template configured this way will work in both Internet Explorer and Mozilla Firefox.

Logon Manager Does Not Respond to hotmail.com When Accessed via Internet Explorer

Logon Manager fails to detect and respond to the hotmail.com logon form when accessed via Internet Explorer.

To work around this issue, use the Mozilla Firefox browser.

Application Title Bar Remains Hidden After Configuring Logon Manager to Display It

Sometimes, the application title bar remains hidden even though the "Display Title Bar" option is enabled.

To work around this issue, restart Logon Manager.

On 64-bit Editions of Windows 7, Enabling the "Allow Forced Verification" Feature Does Not Eliminate Double PIN Prompt

When using a smart card with a PIN in card PIN mode on a 64-bit edition of Windows 7, the "Allow Forced Verification" option does not eliminate the double PIN prompt.

There is currently no workaround for this issue.

First Time Use Wizard Appears to Freeze When Logon Manager Is Configured to Use Smart Card Certificate to Authenticate to Repository and Card Is Not Present

When Logon Manager is configured to use a smart card certificate to authenticate to the repository and fall back to a username and password if smart card authentication fails, the First Time Use wizard appears to freeze if the user does not insert their smart card or the smart card reader is disconnected from the system.

This is because the fallback to a user name and password only occurs once the user clicks "Cancel" in the "Insert Smart Card" dialog that appears behind the First Time Use wizard window and may not be noticed by the user.

To work around this issue, switch to the "Insert Smart Card" dialog and click "Cancel," then complete the First Time Use wizard.

When Using RSA Soft ID with WinAuth v2 and Interactive Passphrase, the Passphrase Prompt Is Displayed Behind the Target Application

When using the RSA SoftID logon method with WinAuth v2 configured for interactive passphrase, the passphrase prompt appears behind the target application.

To work around this issue, switch to the passphrase prompt, enter it, and click "OK."

Last Minute Documentation Changes for the "Credential Delegation" Feature Exist in the User's Guide but Not in the Online Help

Last minute updates have been made to the documentation of the "Credential Delegation" feature that could not be included in the Logon Manager online help.

Changes have been made to:

- The icon functionality description table.
- The paragraph under the heading, "Updating Delegated Credentials."

These updates are present in the *Oracle Enterprise Single Sign-On Suite Plus User's Guide.*

Provisioning Gateway

Provisioning Gateway Server Cannot Function in the Same IIS Application Pool as Password Reset Due to .NET Framework Version Mismatch

When deploying Provisioning Gateway Server on a Windows Server 2003/2003 R2 machine that's also running Password Reset Server, Provisioning Gateway Server will not function if it is placed in the same IIS application pool as Password Reset Server due to the .NET Framework version mismatch between the two server applications.

To work around this issue, create an IIS application pool that is separate from the Password Reset Server application pool and place Provisioning Gateway Server in that pool.

Password Reset

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.

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.

For Languages with Multiple Variants, Editing Questions for One of the Variants Overwrites Questions for the Other Variant

If you create or edit a question in a language that exists in multiple variants, for example, Portuguese (Portugal) and Portuguese (Brazil), saving the question in one variant will overwrite its counterpart in the other variant. For example, editing a question in Portuguese (Portgual) will overwrite the question's Portuguese (Brazil) translation.

The affected languages are Chinese (Simplified), Chinese (Traditional), Portuguese (Brazil), and Portuguese (Portugal).

There is currently no workaround for this issue.

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

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

There is currently no workaround for this issue.

Password Reset Banner Missing from Windows XP Logon Screen on Danish and Turkish Systems

The Password Reset banner is missing from the Windows XP logon screen on Danish and Turkish systems due to an incorrect registry setting.

To resolve this issue, please contact Oracle Support for a hotfix.

"Forgot Your Password?" Link Appears in English on the Windows 7 Logon Screen on Some Non-English Systems

The "Forgot Your Password?" link used to access the password reset quiz from the Windows 7 logon screen appears in English on some non-English systems.

The following languages are affected on 32-bit editions of Windows 7:

- Danish
- Turkish

The following languages are affected on 64-bit editions of Windows 7:

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

To work around this issue, modify the `LinkText` registry value with link text correct for your target language. The value can be found at the following location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix\SSPR\WindowsInterface\xx
```

where `xx` is the two-character code of the affected language. (A list of supported languages and their codes can be found in the *Oracle Enterprise Single Sign-On Suite Plus Installation Guide*.)

Universal Authentication Manager

Administrative Console Allows Assignment of the Unsupported "Domain Users" Group to a Policy

When assigning users and user groups in the Assignments tab of a Universal Authentication Manager logon method policy in the Oracle Enterprise Single Sign-On Administrative Console, it is possible to assign the unsupported "Domain Users" group, even though this group will be ignored by Universal Authentication Manager.

To work around this issue, do not assign the "Domain Users" group to policies. Instead, always use custom user groups tailored specifically to the requirements of the individual policy, or assign users individually, as appropriate for your environment.

When Enrolling with a Logon Method at Windows Logon After Grace Period Has Expired, User Is Returned to the Logon Screen

If you attempt to enroll with a logon method at Windows logon when the enrollment grace period for that logon method is enabled but has expired, you will be returned to the Windows logon dialog upon completing enrollment instead of being logged on to Windows.

To work around this issue, log on to Windows with any valid logon method when you are returned to the Windows logon screen.

The Challenge Questions Logon Method Is Not Supported in Kiosk Manager Environments

The Challenge Questions logon method does not support Kiosk Manager environments in this release. This is because the Challenge Questions logon method requires more privileges than are granted to the limited-privilege session account used by Kiosk Manager.

There is currently no workaround for this issue.

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

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

Operating System	Logon Manager	Logon Manager Strong Authenticators	Kiosk Manager	Universal Authentication Manager	Provisioning Gateway Server	Provisioning Gateway Client	Password Reset Server
Microsoft Windows XP Professional SP3 (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)	✓	✓	✓		✓	✓	✓

Logon Manager includes both standard logon methods such as LDAP and Windows Logon v2, 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	Oracle Enterprise Single Sign-On Administrative Console	Logon Manager	Kiosk Manager	Universal Authentication Manager	Provisioning Gateway Server	Provisioning Gateway Client	Password ResetServer	Password Reset Client	Anywhere	Oracle Business Intelligence Publisher Reports**
Disk Space	22 MB	135 MB	20 MB	30 MB	7 MB	25 MB	44 MB	10 MB	5 MB	20MB

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

** Consult the Oracle Business Intelligence Publisher release notes for more information on the current release of Oracle Business Intelligence Publisher.

Repositories

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

Repository	Logon Manager	Universal Authentication Manager	Provisioning Gateway Server	Password Reset Server	Reporting
Oracle Directory Server Enterprise Edition 11.1.1.5 and above	✓		✓	✓	
Oracle Internet Directory 11.1.1.5 and above	✓		✓	✓	
Oracle Unified Directory 11.1.1.5 and above	✓		✓	✓	
Oracle Virtual Directory 11.1.1.5 and above	✓		✓	✓	
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 2.0.27/2.2/2.4.x	✓				

Web Servers

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

Web Server	Provisioning Gateway Server	Password Reset Server
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	Logon Manager	Provisioning Gateway Server	Password Reset Server
Microsoft Internet Explorer 7.0 and later	✓	✓	✓
Mozilla Firefox 6.0 and later	✓	✓	

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	Oracle Enterprise Single Sign-On Administrative Console	Kiosk Manager	Provisioning Gateway Server	Universal Authentication Manager*	Password Reset Server	Anywhere Console
Microsoft .NET Framework 4.0	✓	✓		✓	✓	
Microsoft .NET Framework 2.0			✓			✓

* Universal Authentication Manager only requires the .NET framework when using the Challenge Questions logon method.

Universal Authentication Manager 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. Universal Authentication Manager does not ship with cards, middleware, or hardware; you must obtain them separately.

Smart Cards

The Universal Authentication Manager 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.

Prior to use with Universal Authentication Manager, smart cards must be initialized to contain a valid serial number and PIN. Universal Authentication Manager 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 in the /SmartCard folder in the Universal Authentication Manager folder in the Oracle Enterprise Single Sign-On Suite Plus master archive. The appropriate file must be merged (by double-clicking it) after the middleware and Universal Authentication Manager are installed. If Universal Authentication Manager 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.

Middleware	Example Card	Family/Type
RSA Authentication Client 2.0	RSA smart card 5200	PKCS11
NetMaker Net iD 4.6	NetMaker Net iD - CardOS 1	
SafeSign/RaakSign Standard 3.0.23	ORGA JCOP21 v2.2 Oberthur ID-ONE Cosmo Athena IDProtect	
Athena ASECard Crypto 4.33	Athena ASECard Crypto	
HID RaakSign Standard 2.3	HID Crescendo 700	
SafeSign Identity Client 2.2.0	IBM JCOP21id	
Fujitsu mPollux DigiSign Client 1.3.2-34 (1671)	DigiSign JCOP with MyEID Applet	
Xiring CCID Driver version 1.00.0002 or later (with XI-SIGN reader)	Gemalto Cyberflex 64K (v2c) SPE Required / SPE Optional	
Gemalto PC-PinPad version 4.0.7.5 or later (with PC-PinPad reader)	Gemalto Cyberflex 64K (v2c) SPE Required / SPE Optional	
ActivIdentity ActivClient 6.1	Oberthur ID-One Cosmo 64 v5.2D Fast ATR with PIV application SDK	
Gemalto Access Client 5.5	Cyberflex 64K Gemalto Cyberflex 64K (v2c) SPE Required / SPE Optional	
HID Global MiniDriver for MS Base smart card CSP	HID Crescendo 200	MS Base CSP/MiniDriver
Gemalto MiniDriver for Microsoft Windows XP	Gemalto .NET v2+	
Oberthur ID-ONE MiniDriver for MS Base smart card CSP	Oberthur ID-ONE Cosmo	
Athena ASECard Crypto ILM MiniDriver for MS Base smart card	Athena ASECard Crypto ILM	

Proximity Cards

The Universal Authentication Manager Proximity Card Logon Method supports many standard HID, MIFARE and iCLASS proximity cards and tokens used for physical access security.

Reader Family	Family/Type	Example Reader	Example Card/Token
Omnikey Cardman	Prox 125 KHz	Omnikey Cardman 5125/5325	HID 1336 DuoProx II HID 1346 ProxKey II-Key fob token HID ProxCard II
	RFID 13.56 MHz	Omnikey Cardman 5121/5321	HID 2080 ICLASS Clamshell HID 1430 MIFARE ISO HID 1450 DESFire ISO HID C700 HID iCLASS Px E6L
RFIDeas pcProx	Prox 125 KHz	RFIDeas pcProx USB RDR-6382AKU	Indala FlexCard Indala FlexPass
		RFIDeas pcProx USB RDR-6E82AKU	EM Wristband
RFIDeas AIR ID	RFID 13.56 MHz	RFIDeas AIR ID RDR-7582AKU	Most iCLASS-compliant and MIFARE-compliant proximity tokens
		RFIDeas AIR ID RDR-7582AKU	HID C700
Cherry Dual-Mode (SmartCard/ Contactless)	RFID 13.56 MHz	Cherry ST-1275 Smart Terminal	Most MIFARE-compliant proximity tokens

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.

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 Universal Authentication Manager. This release of Universal Authentication Manager is compatible with BIO-key version 1.10. For the list of supported devices, refer to the BIO-key documentation.

Optional Software Support for Logon Manager

Java

- Java support: Java Runtime Environment (JRE) version 1.7, 1.6, 1.5, 1.4, 1.3.

Host Emulators

- Support for virtually any HLLAPI, EHLLAPI, or WinHLLAPI-compliant emulator. See the Supported Emulators section or contact Oracle Support 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.x: 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.

Logon Manager Supported Emulators

The Logon Manager mfrmlist.ini file includes the following host emulators:

Emulator	Versions Supported
Attachmate Accessory Manager	8.1
Attachmate Extra!	9.1, 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	2011, 15.0, 14.0, 10.0, 9.0, 8.0, 7.0 **Note:** Requires HLLAPI-compatible version; non-HLLAPI versions (such as the UNIX version) are not supported.
BOSaNOVA TCP/IP	6.0, 5.0
Dynacomm Series 8	
Ericom PowerTerm Interconnect	9.1.0, 8.2.0
G&R Glink	6.0
Hummingbird Exceed	11.0, 10.0
Hummingbird HostExplorer	14.0, 13.0, 12.0, 11.0, 10.0
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 Chameleon Hostlink	
NetManage NS/ElitePlus for Mainframe	3.12
NetManage Rumba	7.5, 7.1, 6.0
Newhart Systems BLUES 2000	6.0.0.35
Novell LAN Workplace Pro	5.2
PuTTY	0.60

Emulator	Versions Supported
ScanPak (Eicon) Aviva	9.1, 9.0, 8.1
SDI Limited TN3270 Plus	
Seagull BlueZone	4.0, 3.4
Seagull Rio	
Zephyr PASSPORT PC TO HOST	2005
Zephyr PASSPORT WEB TO HOST	2005

Logon Manager Supported Applications

Logon Manager 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
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
Lotus Notes	8.5.2, 8.5, 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
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 Enterprise Single Sign-On Administrative Console	11.1.2.0.0, 11.1.1.5.x, 11.1.1.2.x
PKZip	12.2, 12.1, 12.0, 11.2, 11.0, 10.0, 9.0, 8.0, 5.0
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

Additional Provisioning Gateway Requirements

Microsoft Internet Information Server

If Active Directory or ADAM/AD-LDS is used as a repository, 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 the Provisioning Gateway server installer).

Installer Requirements

To install Provisioning Gateway, you must have administrative privileges for the Provisioning Gateway/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 "Enabling SSL" section of the "Installing Provisioning Gateway" chapter in the *Oracle Enterprise Single Sign-On Suite Plus Installation Guide.*

If you have not set up a certificate authority and want to use Microsoft Certificate Services to obtain certificates, refer to the "Obtaining a Certificate" section of the *Provisioning Gateway Administrator's 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.

Logon Manager

New User Setting Storage Schema (Active Directory Only)

Starting with version 11.1.2, 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; otherwise, once Logon Manager 11.1.2 synchronizes with the repository, all previous versions will no longer be able to synchronize with the repository for that user.

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:

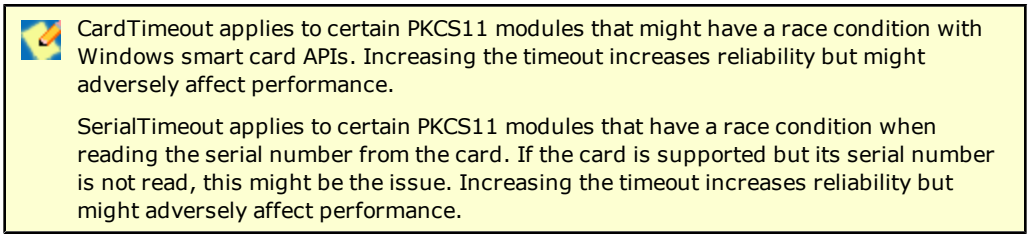
- The user can click **OK** and try inserting the card again.
- The administrator can add the following registry key and increase the timeout values:

  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. For a list of supported cards, middleware, and hardware, refer to that section in this document.

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.** Detection and response of Web applications accessed via the Mozilla Firefox browser are 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 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 Vista 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 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 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.