Oracle© Enterprise Single Sign-on Authentication Manager

Release Notes

Release 10.1.4.1.0

E12622-01

October 2008

Oracle Enterprise Single Sign-on Authentication Manager Release Notes, Release 10.1.4.1.0

E12622-01

Table of Contents

Oracle Enterprise Single Sign-on Authentication Manager 10.1.4.1.0

Oracle® is releasing version 10.1.4.1.0 of Oracle Enterprise Single Sign-on Authentication Manager (ESSO-AM). These release notes provide important information about this release. The information in this document supplements and supersedes information in the related product documents.

What's New in ESSO-AM 10.1.4.1.0

ESSO-AM integrates with most authentication methods and provides support for both primary logon and re-authentication requests (i.e., forced re-authentication, session timeout, or application-specific authentication request) for both connected and disconnected use.

The major new features of this product include:

Read-Only Smart Card Support

ESSO-AM now supports read-only smart cards. To install support for this authenticator, during installation select **Read-Only Smart Card** on the Custom Setup panel.

Advanced settings are available in the ESSO-LM Administrative Console. Open the console by clicking **Start** > **Programs** > **Oracle > ESSO-LM** > **ESSO-LM Console**. To access the read-only smart card settings, click **Global Agent Settings** > **Live** > **Primary Logon Methods** > **Read-Only Smart Card** > **Advanced**. See the Supported Authenticators section in this document for a list of supported read-only smart cards.

Refer to the *ESSO-AM Installation and Setup Guide* for additional information on configuring read-only smart cards.

Fujitsu mPollux DigiSign Client and ESSO-KM: Support for Fujitsu mPollux DigiSign Client used in conjunction ESSO-KM is available in preview-mode only. This functionality is considered Beta in the 10.1.4.1.0 release.

Enhanced Reset Certificate Configuration

Smart Card and Read-Only Smart Card authenticators now provide the ability to specify the certificate used for certificate-based reset through the use of an Object Identifier (OID). These authenticators search the "Enhanced Key Usage" attribute of each certificate on the smart card for this Object Identifier.

This feature is set in the ESSO-LM Administrative Console on the **Global Agent Settings** > **Live** > **Primary Logon Methods** > (**Read-Only Smart Card** and **Smart Card**) > **Advanced** panel. The setting is **Reset Certificate Object Identifier**

Refer to the *ESSO-AM Installation and Setup Guide* for additional information on configuring this setting.

Secondary Authentication API

Smart Card and Read-Only Smart Card Authenticators provide the option to enable a passphrase to authenticate the user in the case that the originally enrolled smart card is replaced. If the use of a passphrase is undesirable, the passphrase prompt can be eliminated by implementing an alternate solution through the use of the Secondary Authentication API.

This feature can only be invoked when the Smart Card or Read-Only Smart Card **Passphrase** is set to use **Enable (using a dialog box)** as the passphrase. This feature is set in the ESSO-LM Administrative Console on the **Global Agent Settings** > **Live** > **Primary Logon Methods** > (**Read-Only Smart Card** and **Smart Card**) > **Advanced** panel.

Support for Active Directory Application Mode with Smart Card and Read-Only Smart Card Authenticators

The Active Directory Application Mode (ADAM) repository is now supported when integrating with ESSO-KM and using Smart Card or Read-Only Smart Card authenticators.

What's Changed in ESSO-AM 10.1.4.1.0

Authenticator Technical Notes

In previous releases, technical notes about the supported authenticators were listed in the **Technical Notes** section of these Release Notes. With this release, they are listed in an Authenticator Configuration Settings section of the *ESSO-AM Installation and Setup Guide*.

Smart Card and ESSO-KM Integration

The **Store Synchronization Credentials** setting configures whether to store the user's synchronization repository credentials on the smart card. It should be set to "Store credentials" when using Smart Card authenticator with ESSO-KM. Previously, the synchronization credentials were always stored on the card.

This setting is set to "Do not store credentials" by default and is located on the **Global Agent Settings** > **Live** > **Primary Logon Methods** > **Smart Card** > **Advanced** panel in the ESSO-LM Administrative Console.

.

Resolved Issues

Issues that were reported in earlier releases of ESSO-AM that have been resolved in this release include:

Tracking Number	Description of Issue
a11007	When using the Proximity Card authenticator with the ADAM synchronizer, if the name of the ADAM partition name reflects a domain other than the user's domain, the authenticator cannot locate the user. The issue is that the authenticator attempts to use the domain referenced in the ADAM partition name, and not the user's actual domain.
a10519	Proximity card with ESSO-KM: When starting a new ESSO-KM session with a proximity card, the user receives an "Invalid PIN" message and ESSO-KM does not unlock.
a10571	The user is unable to complete the First Time Use (FTU) enrollment process in the Smart Card authenticator when using a Cryptoflex e-gate smart card in an Axalto 5.2 or Schlumberger 4.4.3 environment when **Use default certificate for authentication** is set to **Use SSO-generated keys**.
a10640	The version information for the built InstallShield 2008 setup.exe file gets truncated at different lengths. This information can be viewed when right-clicking the setup.exe and checking the **Version** tab. Fields such as **Product Name** and **Product Version** are affected.
a10554	Extended proximity card functionality to work with two additional proximity readers: RF IDeas pcProx USB RDR-6382AKU for Indala Flexcard and RF IDeas pcProx USB RDR-6E82AKU for EM Compatible devices.
a10813	Users going through the FTU wizard using the RSA SecurID authenticator in a RSA LAC environment will see a message that indicates "Authentication Failed". This message displays when a standard user is logged into the machine.

Open Issues

This section describes issues that remain open in this release.

Tracking Number	Description
a11487	After using read-only smart cards or proximity cards to start a new session in ESSO-KM, ESSO-LM does not respond to pre-defined applications until a synchronization event occurs. To work around this issue, disable the ESSO-KM Cached Credentials feature, located on the **Global Agent Settings** > **Live** > **Kiosk Manager** > **Cached Credentials** panel.
a11542	When using Read-Only Smart Card authenticator with Fujitsu mPollux DigiSign Client and ESSO-KM, you may experience a delay of up to 20 seconds after a card is inserted into the reader, before being prompted for the PIN.

Hardware and Software Requirements

The ESSO-AM hardware and software requirements are listed under the following sections:

Supported Operating Systems

The ESSO-AM components are supported on the following operating systems:

Operating System	Versions Supported
Microsoft® Windows® 2000	SP4
Microsoft Windows XP	SP2
Microsoft Windows Server 2003	SP1

System Requirements

The ESSO-AM components system requirements are as follows:

Disk Space Requirements

Disk space requirements for the Agent:

	Minimum, excluding temporary space and runtime expansion	Temporary disk space (/tmp) needed during installation	For runtime expansion (configuration data and logs)
MSI	15 MB	30 MB	20 MB
EXE	20 MB	40 MB	25 MB

Other Disk Space Requirements

The following components require additional disk space requirements:

- Microsoft .NET Framework 2.0: 20 MB hard drive space (if not present)
- Microsoft Windows Installer: 20 MB hard drive space (if not present and if used)

A note about the MSI installer and EXE installer

The disk space requirements are different for the MSI and EXE installers as there are differences in the capabilities of these installers:

- The EXE installer file can be run in multiple languages. The MSI file is English-only.

Software Prerequisites

The ESSO-AM Agent requires the following software prerequisites:

ESSO-LM

- This release requires ESSO-LM 10.1.4.0.5 Agent and Administrative Console with Fix Pack 3 applied.

ESSO-KM

- If integrating with ESSO-KM, this release requires ESSO-KM 10.1.4.0.4 with Fix Pack 3 applied.

Authenticator Software

- The client software for each authenticator must be installed. Strong authenticator clients are likely to have their own system requirements, which may differ from the requirements of ESSO-AM. Please refer to the strong authenticator's documentation to review the system requirements.

Windows Installer

- Windows Installer 2.0 is required for the MSI installer file.

Microsoft .NET Framework

- Microsoft .NET Framework 2.0 is required for the ESSO-LM Administrative Console.

Supported Authenticators

ESSO-AM supports the following authenticators:

Authenticator	Authenticator brand and version supported
Smart Card	• GemSafe Libraries 4.2.0 • GemSafe GXPPro-R3.x STD PTS smart cards • GemSafe GXPPro-R3.x FIPS PTS smart cards • Schlumberger Cyberflex Access 4.3 • Axalto Access Client Software 5.2 • Cryptoflex e-gate 32K smart cards • RSA Authentication Client 2.0 / Smartcard Middleware 2.0 • RSA Smart Card 5200 smart cards • RSA Smart Key 6200 • RSA SecurID SID800 hardware authenticator • NetMaker Net iD 4.6 • NetMaker Net iD - CardOS 1 smart cards • SafeSign/RaakSign Standard 2.3 • ORGA JCOP21 v2.2 smart cards • Microsoft Base Smart Card CSP • Gemalto Cryptoflex .NET smart cards • HID Crescendo 200 • HID Crescendo 700 • HID C700 middleware • HID C200 mini-driver for MS BASE Smart Card CSP
Read-Only Smart Card	• SafeSign Identity Client 2.2.0 • IBM JCOP21id • Fujitsu mPollux DigiSign Client 1.3.2-34(1671) • DigiSign JCOP with MyEID Applet
Xyloc	• Ensure Tech lock • Ensure Tech Xyloc XC-2 badges • Xyloc client 8.4.6 • Xyloc Active Directory Schema Extension 4.2.6 • Xyloc Active Directory UI Extension 4.2.0
Sphinx	• OmniKey Cardman 5121 reader • HID iClass 16k CL proximity cards • Sphinx Logon Manager v3.2.36 • Sphinx CardMaker v3.2.36
SAFLink	• Precise Biometrics 100 series reader • SAFsolution(R) Enterprise Edition Version 1.3
Entrust	• Entrust Desktop Solutions 6.1
Proximity Card	• OmniKey Cardman 5125 reader o HID Proximity 125 kHz Credentials ▪ 1386 ISOProx II ▪ 1336 DuoProx II ▪ 1346 ProxKey II • OmniKey Cardman 5121 reader • OmniKey Cardman 5321 reader

Authenticator	Authenticator brand and version supported
	o iClass Contactless 13.56 MHz Credentials ▪ 2080 ICLASS Clamshell Card o FlexSmart Series /MIFARE / DESFire - 13.56 MHz Credentials ▪ 1430 MIFARE ISO Card ▪ 1450 DESFire ISO Card • RF IDeas pcProx USB RDR-6382AKU o Indala FlexCard • RF IDeas pcProx USB RDR-6E82AKU o EM wristband
RSA SecurID	• RSA Authentication Agent 6.1 for Windows • RSA Local Authentication Toolkit (LAT) • RSA SecurID SID800 hardware authenticator • RSA SecurID SID700 hardware authenticator
SoftID Helper	• RSA SecurID Software Token 3.0.3 • RSA Authentication Client 2.0 • RSA SecurID SID800 hardware authenticator • RSA SecurID SID700 hardware authenticator

Product Documentation

The following documentation supports this product:

- *ESSO-AM Installation and Setup Guide*
- *ESSO-LM Administrative Console Help*
- *ESSO-LM Agent Help*