Oracle© Enterprise Single Sign-on Authentication Manager

Release Notes

Release 11.1.1.2.0

E15707-02

November 2010

ORACLE®

Oracle Enterprise Single Sign-on Authentication Manager Release Notes, Release 11.1.1.2.0

E15707-02

Table of Contents

Abbreviations and Terminology

Following is a list of commonly-used abbreviations and terminology.

Abbreviation or Terminology	Full Name
Administrative Console	ESSO-LM Administrative Console
Agent	ESSO-LM Manager
FTU	First Time Use Wizard
ESSO-AM	Oracle Enterprise Single Sign-on Authentication Manager
ESSO-ODE	Oracle Enterprise Single Sign-on On Demand Edition
ESSO-PG	Oracle Enterprise Single Sign-on Provisioning Gateway
ESSO-KM	Oracle Enterprise Single Sign-on Kiosk Manager
ESSO-LM	Oracle Enterprise Single Sign-on
ESSO-PR	Oracle Enterprise Single Sign-on Password Reset

Oracle Enterprise Single Sign-on Authentication Manager 11.1.1.2.0

Oracle® is releasing version 11.1.1.2.0 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 11.1.1.2.0

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 feature of this product is:

Polish Language Support

ESSO-AM now includes support for the Polish language.

To install the Polish language pack, during installation select a **Custom** install, expand **Language Packs**, and select **Polish**.

What's Changed

Authenticator Support Removed

ESSO-AM no longer includes or supports the following logon methods: Xyloc, SAFLink, and Sphinx authenticators.

Resolved Issues

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

s4513	Simultaneously updating the Logon Certificate and the Encryption Certificate used for Certificate-based Passphrase on the smart card results in the user not being able to authenticate with their smart card to ESSO-LM.
s5537	Support has been added for Schlumberger Cyberflex Access 4.5.
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.

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 XP	SP3
Microsoft Windows Server 2003	SP2

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 version 11.1.1.2.0 Agent and Administrative Console.

ESSO-KM

- If integrating with ESSO-KM, this release requires ESSO-KM version 11.1.1.2.0.

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 4.5 • 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
Entrust	• Entrust Desktop Solutions 6.1
Proximity Card	• OmniKey Cardman 5125 reader ○ HID Proximity 125 kHz Credentials ■ 1386 ISOProx II ■ 1336 DuoProx II ■ 1346 ProxKey II • OmniKey Cardman 5121 reader • OmniKey Cardman 5321 reader ○ iClass Contactless 13.56 MHz Credentials ■ 2080 ICLASS Clamshell Card ○ FlexSmart Series /MIFARE / DESFire - 13.56 MHz Credentials ■ 1430 MIFARE ISO Card ■ 1450 DESFire ISO Card • RF IDeas pcProx USB RDR-6382AKU ○ Indala FlexCard • RF IDeas pcProx USB RDR-6E82AKU ○ 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

This note applies to smart cards only: Prior to use with ESSO-AM, smart cards must be initialized and contain a valid PIN. If ESSO-AM is configured to use smart card certificates, smart cards must contain a valid PKI certificate. If the smart cards are also to be used with ESSO-KM, they must have a serial number.

ESSO-AM does not provide any smart card initialization, configuration, 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.

Technical Notes

The technical notes describe important technical information about this release.

Authenticator Technical Notes

The technical notes for ESSO-AM supported authenticators, such as how they need to be configured to work with ESSO-AM and to integrate with ESSO-KM, are now located in the*ESSO-AM Installation and Setup Guide* in the Authenticator Configuration Settings section.

Read-Only Smart Card and Fujitsu

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.

ESSO-AM and ESSO-KM Integration Considerations

This situation occurs when using proximity devices, smart cards, and read only smart cards.

- **Active Directory.** An error message displays saying "Unable to connect to network ...".
- **ADAM**. ESSO-KM stops responding and requires a restart.

There are 2 workarounds to this issue:

1. Users can manually start a ESSO-KM session by authenticating with a username and new password within the password lifetime period.
2. Administrators can change the lifetime period of an old password to decrease the probability that this issue will occur. Please refer to Microsoft Help and Support for more details - http://support.microsoft.com/kb/906305.

Hardware Reassignment

If a hardware device, such as a smart card, is ever reassigned to another user, it is possible that ESSO-KM will logon as the original user. This occurs because ESSO-KM keeps a device-to-username mapping.

It is strongly recommended that these devices not be reassigned to avoid this issue.

Product Documentation

The following documentation supports this product:

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