

**Oracle© Enterprise Single Sign-on  
Authentication Manager**

Release Notes

Release 11.1.1.2.0

**E15707-02**

November 2010

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

E15707-02

Copyright © 2006 - 2010, Oracle. All rights reserved.

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

## Table of Contents

Table of Contents.....	3
Abbreviations and Terminology.....	4
Oracle Enterprise Single Sign-on Authentication Manager 11.1.1.2.0.....	5
What's New in ESSO-AM 11.1.1.2.0.....	6
What's Changed.....	6
Resolved Issues.....	7
Hardware and Software Requirements.....	8
Supported Authenticators.....	10
Technical Notes.....	12
Product Documentation.....	13

## 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 <b>Global Agent Settings &gt; Live &gt; Kiosk Manager &gt; Cached Credentials</b> panel.

## Hardware and Software Requirements

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

- Supported Operating Systems
- System Requirements
- Software Prerequisites
- Supported Authenticators

### 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	<ul style="list-style-type: none"> <li>• GemSafe Libraries 4.2.0</li> <li>• GemSafe GXPPro-R3.x STD PTS smart cards</li> <li>• GemSafe GXPPro-R3.x FIPS PTS smart cards</li> <li>• Schlumberger Cyberflex Access 4.5</li> <li>• Axalto Access Client Software 5.2</li> <li>• Cryptoflex e-gate 32K smart cards</li> <li>• RSA Authentication Client 2.0 / Smartcard Middleware 2.0</li> <li>• RSA Smart Card 5200 smart cards</li> <li>• RSA Smart Key 6200</li> <li>• RSA SecurID SID800 hardware authenticator</li> <li>• NetMaker Net ID 4.6</li> <li>• NetMaker Net ID - CardOS 1 smart cards</li> <li>• SafeSign/RaakSign Standard 2.3</li> <li>• ORGA JCOP21 v2.2 smart cards</li> <li>• Microsoft Base Smart Card CSP</li> <li>• Gemalto Cryptoflex .NET smart cards</li> <li>• HID Crescendo 200</li> <li>• HID Crescendo 700</li> <li>• HID C700 middleware</li> <li>• HID C200 mini-driver for MS BASE Smart Card CSP</li> </ul>
Read-Only Smart Card	<ul style="list-style-type: none"> <li>• SafeSign Identity Client 2.2.0</li> <li>• IBM JCOP21id</li> <li>• Fujitsu mPollux DigiSign Client 1.3.2-34(1671)</li> <li>• DigiSign JCOP with MyEID Applet</li> </ul>
Entrust	<ul style="list-style-type: none"> <li>• Entrust Desktop Solutions 6.1</li> </ul>
Proximity Card	<ul style="list-style-type: none"> <li>• OmniKey Cardman 5125 reader</li> <li>◦ HID Proximity 125 kHz Credentials <ul style="list-style-type: none"> <li>■ 1386 ISOProx II</li> <li>■ 1336 DuoProx II</li> <li>■ 1346 ProxKey II</li> </ul> </li> <li>• OmniKey Cardman 5121 reader</li> <li>• OmniKey Cardman 5321 reader</li> <li>◦ iClass Contactless 13.56 MHz Credentials <ul style="list-style-type: none"> <li>■ 2080 ICLASS Clamshell Card</li> </ul> </li> <li>◦ FlexSmart Series /MIFARE / DESFire - 13.56 MHz Credentials <ul style="list-style-type: none"> <li>■ 1430 MIFARE ISO Card</li> <li>■ 1450 DESFire ISO Card</li> </ul> </li> <li>• RF IDEas pcProx USB RDR-6382AKU</li> <li>◦ Indala FlexCard</li> <li>• RF IDEas pcProx USB RDR-6E82AKU</li> <li>◦ EM wristband</li> </ul>
RSA SecurID	<ul style="list-style-type: none"> <li>• RSA Authentication Agent 6.1 for Windows</li> <li>• RSA Local Authentication Toolkit (LAT)</li> <li>• RSA SecurID SID800 hardware authenticator</li> <li>• RSA SecurID SID700 hardware authenticator</li> </ul>
SoftID Helper	<ul style="list-style-type: none"> <li>• RSA SecurID Software Token 3.0.3</li> <li>• RSA Authentication Client 2.0</li> <li>• RSA SecurID SID800 hardware authenticator</li> <li>• RSA SecurID SID700 hardware authenticator</li> </ul>



**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*