Oracle® Enterprise Single Sign-on Universal Authentication Manager

Installation Guide

Release 11.1.1.5.0

E21030-01

March 2011

ORACLE®

Oracle Enterprise Single Sign-on Universal Authentication Manager, Installation Guide, Release 11.1.1.5.0

E21030-01

Table of Contents

Abbreviations and Terminology

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

Abbreviation or Terminology	Full Name
AD	Active Directory
ADAM	Active Directory Application Mode (Windows 2003 Server)
AD LDS	Active Directory Lightweight Directory Service (Windows 2008 Server)
Administrative Console	ESSO-LM Administrative Console
Agent	ESSO-LM Manager
BioAPI	Biometric Application Programming Interface
BSP	Biometric Service Provider
FTU	First Time Use Wizard
ESSO-PG	Oracle Enterprise Single Sign-on Provisioning Gateway
ESSO-LM	Oracle Enterprise Single Sign-on Logon Manager
ESSO-PR	Oracle Enterprise Single Sign-on Password Reset

Authentication Manager

Authentication Manager is a feature of ESSO-LM that adds the capability to enable multiple logon methods to authenticate the user. These logon methods can be the standard ESSO-LM supported logon methods such as LDAP and Windows Logon, or strong authenticators such as smart cards, proximity devices, and RSA SecurID tokens.

ESSO-LM installed with Strong Authenticators

ESSO-LM includes both standard logon methods such as LDAP and Windows Logon, and strong authenticators such as smart cards, proximity devices, and RSA SecurID tokens. The ESSO-UAM installer reacts differently based on which authenticators are installed with ESSO-LM. Refer to Step 7 during the ESSO-UAM Client installation.

Authenticator versus Primary Logon Method

An authenticator is a plug-in module to ESSO-LM. The Primary Logon Method is the authenticator you have selected to use with ESSO-LM. You can have multiple installed authenticators but can only have one Primary Logon Method.

About ESSO-UAM

Oracle Enterprise Single Sign-on Universal Authentication Manager (ESSO-UAM) enables Enterprises to replace the use of native password logon to Microsoft Windows and Active Directory networks with stronger and easier to use authentication methods. The ESSO-UAM system also enhances Enterprise security beyond traditional password authentication by providing two-factor authentication methods. ESSO-UAM enables users to rapidly and securely enroll credentials that will be used to identify and authenticate them. ESSO-UAM offers built-in and configurable authentication methods: smart cards, passive proximity cards, biometric fingerprint, and other biometric technologies compatible with the BioAPI standard. Native Windows Passwords are also supported.

Smart Cards

A smart card is a credit card-sized token containing a chip or embedded circuits that can store and process data securely. Information stored on a smart card can also be used for identification and authentication. ESSO-UAM enables enrolling and using smart cards for user logon and authentication without writing any data on a smart card chip. ESSO-UAM also supports the option to require a smart card PIN during logon to provide stronger two-factor authentication.

Proximity Cards

A passive proximity card or token is an identity object (such as a workplace ID badge) containing a circuit that a card-reading device can detect and decipher. When the proximity card is placed in close proximity to a reader, the reader detects the token's presence and recognizes identifying information that is associated with a specific user. This ESSO-UAM method includes the option to require a user to enroll a PIN that is associated with a proximity token enabling two-factor authentication. When so configured, ESSO-UAM prompts the user for the enrolled PIN associated with a token during logon, strengthening user authentication.

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 ESSO-UAM.

The BioAPI Logon Method leverages the BioAPI framework, thus enabling support of almost any third-party BioAPI-compliant Biometric Service Provider (BSP) module. In addition to fingerprint biometrics, this logon method can also support other biometric technologies that offer a BioAPI compatible BSP such as palm, facial, and iris recognition solutions.

ESSO-UAM Administration

ESSO-UAM leverages the ESSO-LM Administrative Console to configure a supported central repository to store and manage policies for users and user groups. The ESSO-LM Administrative Console contains ESSO-UAM settings that allow administrators to configure policies; these policies specify how authentication operates for different users and user groups. When you edit and publish a policy, the changes are applied to domain user accounts running in Enterprise mode each time the Client synchronizes with the repository, guaranteeing that the most up-to-date policies are enforced.

Installation Overview

ESSO-UAM consists of two components:

- ESSO-LM Administrative Console (for Enterprise functionality)
- ESSO-UAM Client

The installation process consists of:

- Installing the ESSO-LM Administrative Console

  The ESSO-LM Administrative Console installer supports both ESSO-UAM and ESSO-LM.

- Preparing the Repository

  You must create or select an ESSO-UAM Service Account in the repository to store user objects and containers. Select your repository:

  Active Directory

  Active Directory Application Mode

  Active Directory Lightweight Directory Service

  Microsoft Active Directory (AD) and Microsoft Active Directory Lightweight Directory Service (AD LDS or ADAM) are the only repositories supported by ESSO-UAM. For a full list of system requirements, see the *Oracle Enterprise Single Sign-on Suite Plus Release Notes*.

- Logon Method Prerequisites

  ESSO-UAM requires and supports various third-party software, hardware, and middleware for the logon methods. The general prerequisites are listed in this section. For a detailed list of supported products and versions for this release, refer to the *Oracle Enterprise Single Sign-on Suite Plus Release Notes*.

- Installing the ESSO-UAM Client

  The ESSO-UAM Client installer is a standalone installer for the ESSO-UAM Client only. It includes an adapter that enables ESSO-LM to offer ESSO-UAM as a Primary Logon Method during ESSO-LM's First-Time Use (FTU) Wizard operation. (For more information about enrolling with the FTU Wizard, see the *ESSO-UAM User Guide*.)

  The Client installer also automatically detects the presence of ESSO-LM on a Client workstation and adapts the installation accordingly.

  After installation you are required to restart your workstation in order for the settings to take effect. After you restart, the Microsoft Windows Log On dialog is replaced by the ESSO-UAM Log On dialog:

> It is possible in some scenarios that you will also receive a request to restart after installing other Oracle Enterprise Single Sign-on Logon Manager products.

- Configuring the ESSO-UAM Service Account

  The ESSO-UAM Service Account is a standard domain user account that is selected during deployment that is used to access Active Directory and ADAM containers, where ESSO-UAM data is centrally stored. Before deploying ESSO-UAM, you must create or designate a domain user account to serve as the ESSO-UAM Service Account.

  > This account must be a member of the Domain Users security group, which includes all domain users by default. Take precautions to ensure that no one can tamper with the account. Create a strong password and set a flag to prevent the password from expiring.

- Configure ESSO-UAM to use an ADAM or AD LDS Repository

  This step is for ADAM and AD LDS repository users only. You must configure ESSO-UAM to use this repository by creating two registry values on end-user workstations.

Installing the ESSO-LM Administrative Console

It is recommended that the ESSO-LM Administrative Console be installed and ESSO-UAM policies configured for the ESSO-UAM deployment prior to deploying ESSO-UAM on any client machines. The ESSO-LM Administrative Console can be found in this release package in the following location:

- ofm_esso_win_11.1.1.5.0_disk1_1ofn\ESSO Logon Manager 11.1.1.5.0\ESSO-LM Admin Console

Launch the installer and follow the on-screen instructions. Refer to the *ESSO-LM Installation and Setup Guide* for detailed information.

Oracle recommends against installing the ESSO-UAM Client on the same workstation as the ESSO-LM Administrative Console, to avoid lockout. You should have at least one workstation running the ESSO-LM Administrative Console without ESSO-UAM.

Preparing to use an Active Directory Repository

After installing the ESSO-LM Administrative Console, you need to prepare the Active Directory repository for use with ESSO-UAM. To do so, perform the following steps:

- Create an ESSO-UAM Service Account
- Extend the Schema
- Initialize ESSO-UAM Storage

Create an ESSO-UAM Service Account

By default, this account will be a member of the Domain Users security group, which includes all domain users by default. This is the only group/permission needed on this account.

On a workstation that you use to manage your Active Directory network, open **Active Directory Users and Computers**. Create a domain user account or select an existing account to designate as the ESSO-UAM Service Account. This is a standard domain user account. No elevated privileges are necessary.

This account is the central point used by all Clients to access Active Directory. Failure of this account for any reason will result in all Clients' inability to synchronize with Active Directory or possibly result in the inability of any user to log on to any client system. It is crucial that this account be protected against deletion or alteration of any kind. To ensure the integrity of this account:

- Set the "Password Never Expires" flag = True.
- Select a strong password.
- Ensure that the account is not changed or deleted.

For the procedure to recover the deployment in case of failure of this account, see the *ESSO-UAM Administrator Guide*.

Extend the Schema

Ensure the machine from which you are performing the extension is on the same domain as the directory and you must be logged on as a user in that same domain.

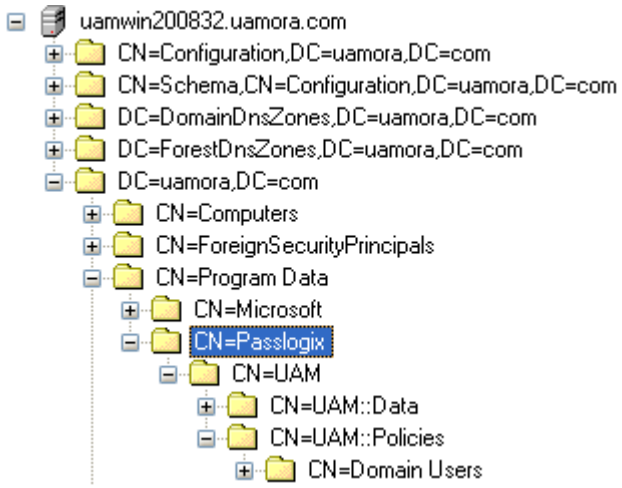
1. Launch the ESSO-LM Administrative Console.
2. From the **Repository** menu, select **Extend Schema**.
3. In the Connect to Repository dialog box, select **Microsoft Active Directory Server** from the dropdown menu, enter the **Server Name** and **Port** of the schema master Domain Controller, and the **Username/ID** and **Password** of an administrative account with Domain and/or Schema Administrator permissions. Click **OK** when finished. The Status window indicates progress and informs you when schema extension has been completed successfully.

Initialize ESSO-UAM Storage

1. From the Repository menu, select **Initialize UAM Storage**.
2. Verify the **Server Name** and **Port** field to ensure that you are connecting to a DC of the domain on which you are deploying ESSO-UAM. Then select **Microsoft Active Directory Server** from the dropdown menu, and enter a **Username/ID** and **Password** of an administrative account with Domain Administrator permissions or an account that has permissions to create objects under the CN=Program Data container.

The ESSO-UAM Storage Initialization alert displays to inform you that you will be selecting an Active Directory user account in the following step. If you have followed this procedure exactly, the ESSO-UAM Service Account exists already.

3. Click **OK** in the ESSO-UAM Storage Initialization dialog box.
4. In the Select User or Group dialog box, enter the name of the ESSO-UAM Service Account that you created, and click **OK**. The Status window indicates initialization progress and informs you when ESSO-UAM storage initialization has been completed successfully.
5. This creates new containers under CN=Program Data in which ESSO-UAM stores its data, according to the following hierarchy:



You should never modify anything under the CN=UAM::Data container.

Preparing to use an ADAM or AD LDS Repository

After installing the ESSO-LM Administrative Console, you need to prepare the ADAM / AD LDS repository for use with ESSO-UAM. To do so, perform the following steps:

- Install ADAM or AD LDS and Create an Instance and Application Directory Partition for ESSO-UAM
- Create an ESSO-UAM Service Account
- Specify the Default Naming Context for ESSO-UAM Repository
- Extend the Schema
- Initialize ESSO-UAM Storage

If using Windows Server 2003, the name of this repository is Active Directory Application Mode (ADAM).

If using Windows Server 2008, the name of this repository is Active Directory Lightweight Directory Services (AD LDS).

The instructions in this section are written for Windows 2008. There are slight variations for Windows 2003 that you will need to account for. For example, in Administrative Tools, the utility is called ADAM ADSI Edit rather than ADSI Edit.

Install ADAM or AD LDS and Create an Instance and Application Directory Partition for ESSO-UAM

If you have not already, you must install ADAM or AD LDS and create an instance for ESSO-UAM. It is recommended that you create a new instance for ESSO-UAM. You must also create an Application Directory Partition when creating the new instance. Refer to the Microsoft ADAM or AD LDS documentation for information on setting up the instance.

Create an ESSO-UAM Service Account

This account must be a member of the Domain Users security group, which includes all domain users by default.

On a workstation that you use to manage your Active Directory network, open **Active Directory Users and Computers**. Create a domain user account or select an existing account to designate as the ESSO-UAM Service Account. This is a standard domain user account. No elevated privileges are necessary.

This account is the central point used by all Clients to access Active Directory or ADAM/AD LDS. Failure of this account for any reason will result in all Clients' inability to synchronize with ADAM/AD LDS. It is crucial that this account be protected against deletion or alteration of any kind. To ensure the integrity of this account:

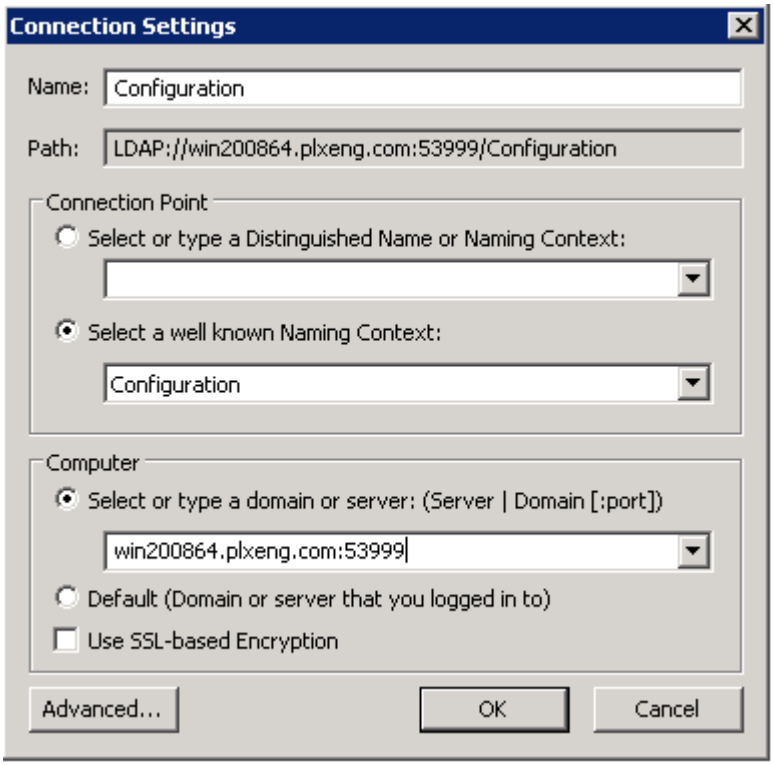
- Set the "Password Never Expires" flag = True.
- Select a strong password.
- Ensure that the account is not changed or deleted.

For the procedure to recover the deployment in case of failure of this account, see the *ESSO-UAM Administrator Guide*.

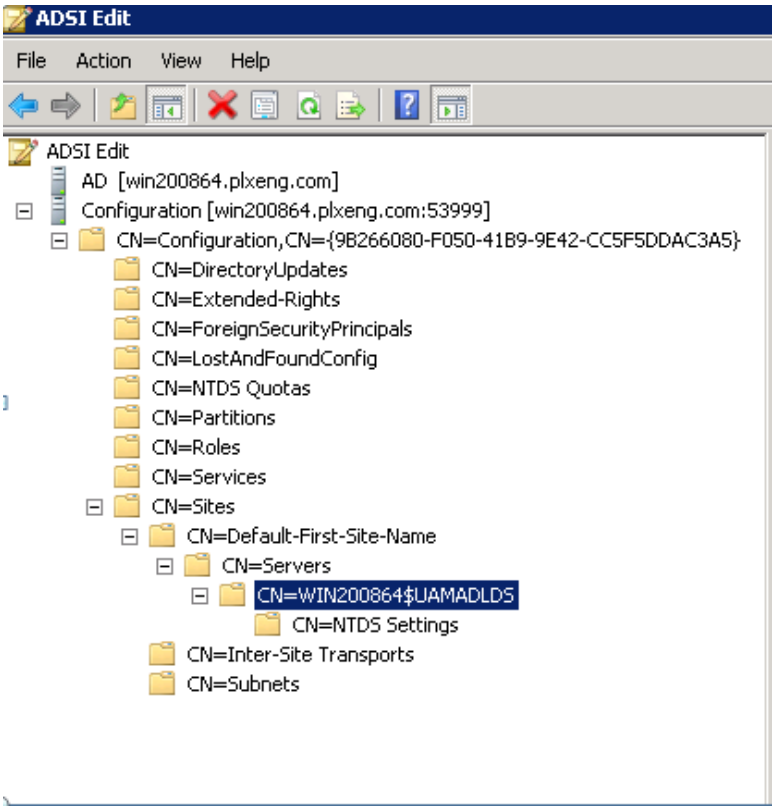
Specify the Default Naming Context for the ESSO-UAM Repository

1. On your server that you use to manage your AD LDS instance, from the Start menu, click **Administrative Tools** and then **ADSI Edit** to launch the ADSI Edit utility.
2. On the ASDI Edit snap-in, right-click **ADSI Edit** in the left pane and select **Connect to...**.

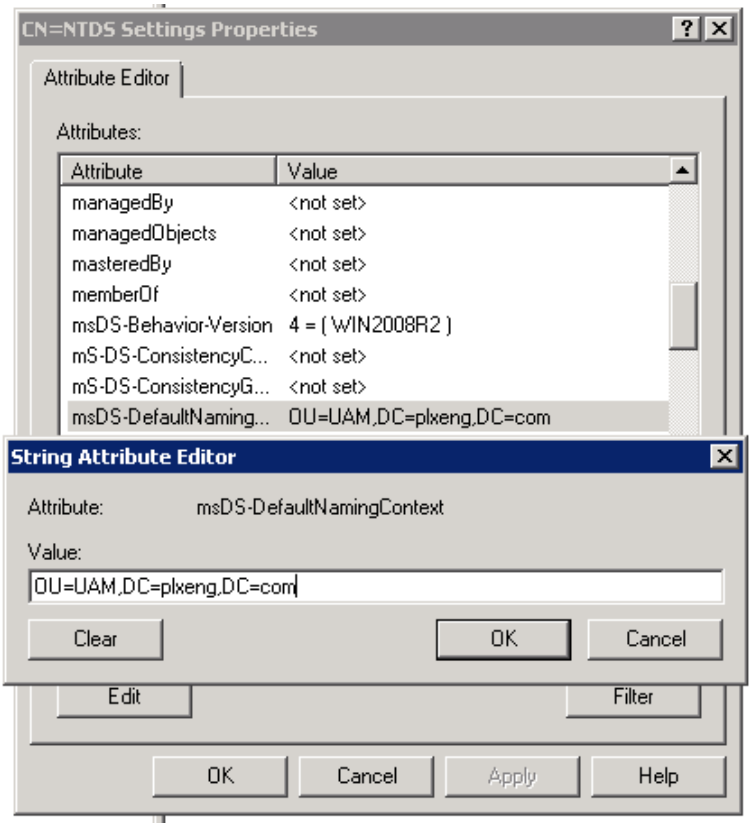
3. On the Connection Settings dialog, select **Configuration** from the Select a well known Naming Context dropdown. Select the option for **Select or type a domain or server**. In the **Select or type a domain or server** field, you must specify the machine name or IP of the machine running the AD LDS instance and the port number used when the instance was created. Click **OK**.



4. In ADSI Edit, navigate to and expand the tree node corresponding to the Configuration you added for the ESSO-UAM repository AD LDS instance and partition. Expand **CN=Sites, CN=Default-First-Site-Name, CN=Servers**. Expand the node for your AD LDS server and partition. The name should be in this format: `CN=[AD LDS computer name]$[UAM repository AD LDS instance name]`.



5. Expand the node and right-click on the **CN=NTDS Settings** sub node. Select **Properties**.
6. In the Properties dialog, locate and double-click the **msDS-DefaultNamingContext** attribute and enter the ESSO-UAM repository AD LDS Partition name in the **Value** field. You must specify the same partition name used when the instance was created. Click **OK**.



7. Click **OK** on the CN=NTDS Settings Properties dialog to close it.
8. From the Start menu, click **Administrative Tools** and then **Services** to launch the Services utility.
9. On Services, select the ESSO-UAM Repository AD LDS instance name, for example, `UAMADLDS`. Right-click and select **Restart**.

Extending the Schema

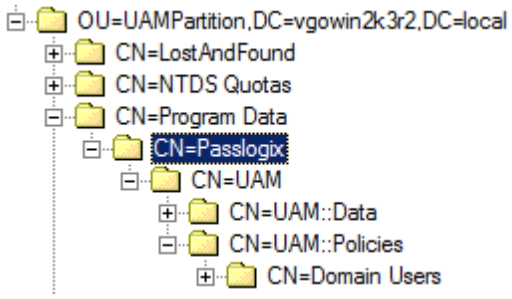
Ensure the machine from which you are performing the schema extension is on the same domain as the directory and you must be logged on as a user in that same domain.

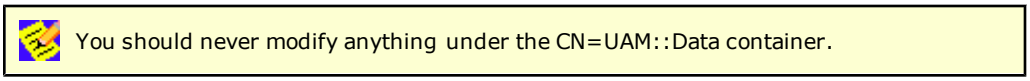
1. Launch the ESSO-LM Administrative Console.
2. From the **Repository** menu, select **Extend Schema**.
3. In the Connect to Repository dialog box, select **Microsoft ADAM** from the dropdown menu, enter the **Server Name** and **Port** of the ADAM or AD LDS instance, and the **Username/ID** and **Password** of an administrative account with ADAM or AD LDS Administrator permissions. Click **OK** when finished. The Status window indicates progress and informs you when schema extension has been completed successfully.

Initialize ESSO-UAM Storage

1. From the Repository menu, select **Initialize UAM Storage**.
2. Select **Microsoft ADAM** from the dropdown menu and verify the previously-created ADAM or AD LDS instance **Server Name** and **Port** are specified. Enter a **Username/ID** and **Password** of an administrative account with ADAM or AD LDS Administrator permissions.

   The ESSO-UAM Storage Initialization alert displays to inform you that you will be selecting an AD user account in the following step. If you have followed this procedure exactly, the ESSO-UAM Service Account account exists already.
3. Click **OK** in the ESSO-UAM Storage Initialization alert dialog box.
4. In the Select User or Group dialog box, enter the username of the ESSO-UAM Service Account that you created, and click **OK**. The Status window indicates initialization progress and informs you when ESSO-UAM storage initialization has been completed successfully.
5. This creates new containers in which ESSO-UAM stores its data, according to the following hierarchy:





Logon Method Prerequisites

ESSO-UAM requires and supports various third-party software, hardware, and middleware for the logon methods. The general prerequisites are listed below. For a detailed list of supported products and versions for this release, refer to the *Oracle Enterprise Single Sign-on Suite Plus Release Notes*.

Prerequisites for Smart Cards

The following third-party software and hardware components are required to use Smart Cards with ESSO-UAM:

- Supported Smart Card middleware software (PKCS#11, MiniDriver/Base CSP, .NET)
- Supported Smart Card readers
- Supported Smart Cards

Prior to use with ESSO-UAM, smart cards must be initialized to contain a valid serial number and PIN. ESSO-UAM 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.

Once the smart card middleware is installed, you must merge the appropriate registry file with it. The registry files are available in the ESSO-UAM installation zip file in the /SmartCard folder. Double-click the registry file to merge it. The following table displays the registry file for each supported smart card:

Card	Family/Type	Middleware	Registry File
RSA smart card 5200	PKCS11	RSA Authentication Client 2.0	smart_providers_pkcs11_rsa.reg
NetMaker Net iD - CardOS 1	PKCS11	NetMaker Net iD 4.6	smart_providers_pkcs11_netid.reg
ORGA JCOP21 v2.2	PKCS11	SafeSign/RaakSign Standard 3.0.23	smart_providers_pkcs11_safesign.reg
Oberthur ID-ONE Cosmo	PKCS11	SafeSign/RaakSign Standard 3.0.23	smart_providers_pkcs11_safesign.reg
Athena IDProtect	PKCS11	SafeSign/RaakSign Standard 3.0.23	smart_providers_pkcs11_safesign.reg
Athena ASECard Crypto	PKCS11	Athena ASECard Crypto 4.33	smart_providers_pkcs11_athena.reg
HID Crescendo 700	PKCS11	HID RaakSign Standard 2.3	smart_providers_pkcs11_raaksign.reg
IBM JCOP21id	PKCS11	SafeSign Identity Client 2.2.0	smart_providers_pkcs11_safesign.reg
DigiSign JCOP with MyEID Applet	PKCS11	Fujitsu mPollux DigiSign Client 1.3.2-34 (1671)	smart_providers_pkcs11_fujitsu.reg

Card	Family/Type	Middleware	Registry File
Gemalto Cyberflex 64K (v2c) SPE Required / SPE Optional	PKCS11	Gemalto Access Client 5.5 Xiring CCID Driver version 1.00.0002 or later / XI-SIGN reader Gemalto PC-PinPad version 4.0.7.5 or later / PC Pinpad reader	smart_providers_pkcs11_gemalto.reg
Oberthur ID-One Cosmo 64 v5.2D Fast ATR with PIV application SDK	PKCS11	ActivIdentity ActivClient 6.1	smart_providers_pkcs11_actividentity.reg
Cyberflex 64K	PKCS11	Gemalto Access Client 5.5	smart_providers_pkcs11_gemalto.reg
Sagem YpsID S1 and S2 (Sagem Mini-Driver cards are not supported.)	PKCS11	Sagem YpsID 3.2.1	smart_providers_pkcs11_sagem.reg
HID Crescendo 200	MS Base CSP/MiniDriver	HID Global MiniDriver for MS Base smart card CSP	smart_providers_basecsp.reg
Gemalto .NET v2+	MS Base CSP/MiniDriver	Gemalto MiniDriver for Microsoft Windows XP	smart_providers_basecsp.reg
Oberthur ID-ONE Cosmo	MS Base CSP/MiniDriver	Oberthur ID-ONE MiniDriver for MS Base smart card CSP	smart_providers_basecsp.reg
Athena ASECard Crypto ILM	MS Base CSP/MiniDriver	Athena ASECard Crypto ILM MiniDriver for MS Base smart card	smart_providers_basecsp.reg
Gemalto .NET v2 or v2+	.NET	Gemalto .NET smart cards PKCS#11 library 2.1.3	smart_providers_pkcs11_gemalto_dotnet.reg

Prerequisites for Proximity Cards

The following third-party hardware components are required to use Proximity Cards with ESSO-UAM.

- Supported Proximity Card readers
- Supported Proximity or Contactless Cards and tokens

Prerequisites for Biometrics

The following third-party hardware components are required to use Biometrics with ESSO-UAM.

- Supported Biometric devices
- For the Fingerprint logon method, BIO-key BioAPI BSP version 1.9 must be installed and a registry key must be created. See the manual configuration steps for BIO-key.
- For the BioAPI logon method, the BioAPI authenticator must be configured with a BioAPI BSP ID and a BioAPI compatible BSP must be installed. See the manual configuration steps for BioAPI.

Configuring the BIO-key BSP for the Fingerprint Logon Method

There are several manual steps required to properly configure the ESSO-UAM Fingerprint Logon Method to use the BIO-key BSP middleware and supported fingerprint readers.

This release of ESSO-UAM is compatible with BIO-key version 1.9. For the list of supported devices, and installation instructions, refer to the Bio-key documentation.

Configuring the BIO-key BSP for use with ESSO-UAM

Once BIO-key is installed, you must perform the following configuration steps:

Create Registry Key

In order for the ESSO-UAM to integrate with the BIO-key BSP, you must manually create registry values on end-user workstations.

1. Open the Windows registry and navigate to the `HKEY_LOCAL_MACHINE\SOFTWARE\BIO-key\Biometric Service Provider\Setting` key. If it does not already exist, create the `Setting` key.
2. Create the following values:

   `REG_DWORD: NumFingersToEnroll`. The **Value Data** field must be set to `00000001`.

   `REG_DWORD: ModelFormat`. The **Value Data** field must be set to `00000000`.

Adjust Permissions

In order for non-administrative users to be able to enroll with BIO-key BSP, you must manually adjust the folder permissions to grant 'Everyone' write/full permissions.

1. Navigate to `C:\WINDOWS\system32\BioAPIFFDB`.
2. Right-click on the BioAPIFFDB folder and click **Properties**.
3. Select the **Security** tab.
4. Grant FULL CONTROL permission to the `BioAPIFFDB` folder for "Everyone."

Configuring a Biometric Reader

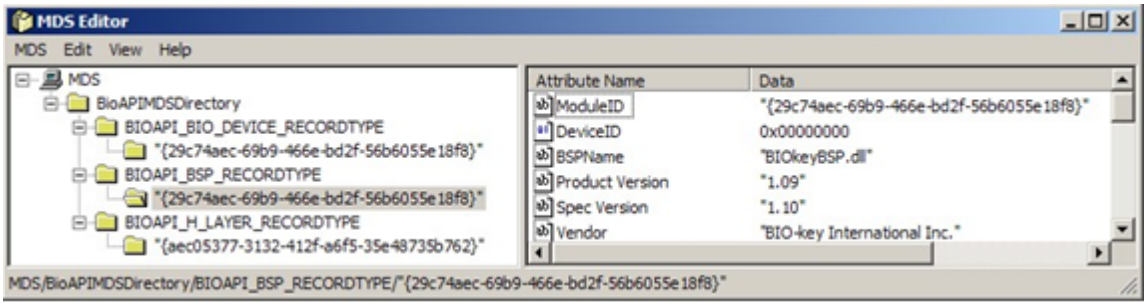
You must manually configure a biometric reader for use with BIO-key BSP.

For instructions, refer to the BIO-key User Guide. Refer to the section about the Control Panel applet, which is in the *Using the BIO-key BSP* section.

Configuring the BSP for the BioAPI Logon Method

In order for the user to be able to run the logon or client application, and successfully enroll and authenticate in BioAPI, you must copy the values from the MDS Editor into the Windows registry.

1. Install the BioAPI 1.1 Framework.
2. Run the mdsedit300.exe (provided with BioAPI Framework). The mdsedit300.exe is found inside the downloaded BioAPI Framework. Refer to the BioAPI documentation for the selected download package for the specific location and additional instructions.
3. Locate and copy the **ModuleID** value. See the screen shot below.



4. Open the Windows registry and navigate to the `HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix\UAM\Authenticators\{17875AD3-D203-4F07-BF48-788765-45AF4C}\Settings` key.
5. Edit the **Provider** setting registry key for the BioAPI BSP to replace the "uuid" in the "BIOAPI:{uuid}" registry value with the BSPID (i.e. ModuleID) of the BSP. For example, for BIO-key this value is "BIOAPI:{29c74aec-69b9-466e-bd2f-56b6055e18f8}".

Adjust Permissions

In order for non-administrative users to be able to enroll with BIO-key BSP, you must manually adjust the folder permissions to grant 'Everyone' write/full permissions.

1. Navigate to `C:\WINDOWS\system32\BioAPIFFDB`.
2. Right-click on the folder and click **Properties**.
3. Select the **Security** tab.
4. Grant FULL CONTROL permission to the `BioAPIFFDB` folder for "Everyone."

Configuring Additional BioAPI Logon Methods (Optional)

This section describes how to deploy an additional BioAPI BSP logical authenticator on a client. Once set up, the new custom logon method appears in ESSO-UAM and the user can enroll and authenticate through it.

1. Generate a new random GUID to be the authenticator ID, for example, using Visual Studio's Guidgen tool or any other GUID generator tool.
2. Ensure the GUID string is all uppercase, and in the following format: {6369E4DB-CEDE-4D3A-A00A-56441F5AC581}.
3. Clone the BioAPI Authenticator registry key and values, found under `HKLM\Software\Passlogix\UAM\Authenticators\{17875AD3-D203-4F07-BF48-78876545AF4C}`, into a new key named for the new random GUID. All other values are identical.

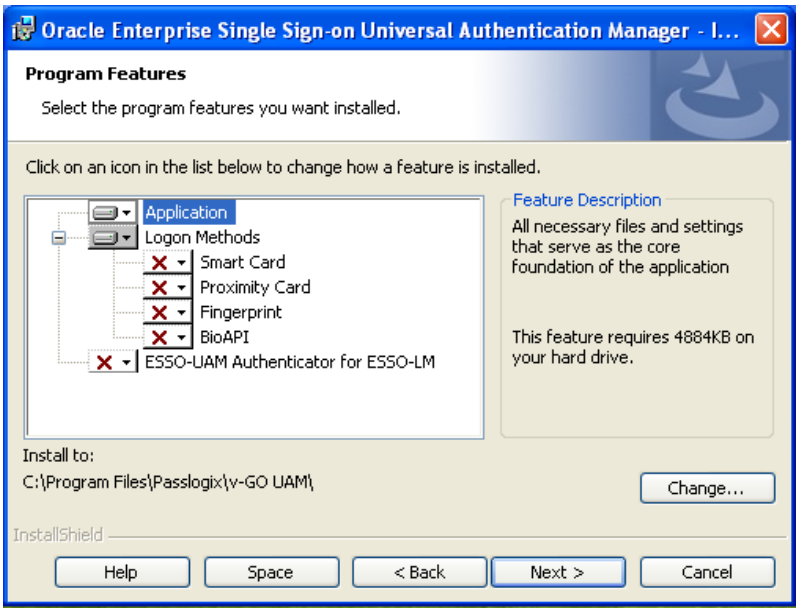
Installing the ESSO-UAM Client

> After installing the Client, you are required to restart your workstation. By default, when you log on after restarting, you will be prompted to enroll any installed logon methods. Oracle recommends that you install any hardware devices, middleware, and drivers prior to installing the Client.
>
> Installing the Client requires you to have local administrator permissions.
>
> Oracle recommends against installing the ESSO-UAM Client on the same workstation as the ESSO-LM Administrative Console, to avoid lockout. You should have at least one workstation running the ESSO-LM Administrative Console without ESSO-UAM.

To install and configure the ESSO-UAM Client:

1. Close all programs.
2. In the Release zip file, navigate to the ofm_esso_win_11.1.1.5.0_disk1_1ofn\ESSO Universal Authentication Manager 11.1.1.5.0\ folder. Double-click the setup file, **ESSO-UAM.msi**. Wait while the installer loads.
3. On the Welcome Panel, click **Next>**.

4. The Program Features dialog box prompts you to select the features to install. Select the features you want by clicking the red [**x**] next to the feature and clicking **This feature will be installed on local hard drive**. You must select at least one Logon Method to proceed with the installation.



Application

(*requires ~4580KB of space*)
This option installs all necessary files and settings that serve as the core foundation of the application.

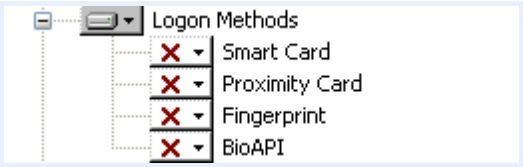
Logon Methods

(*requires ~215KB of space, ~1253KB including subfeatures*)
The logon methods are plug-ins supported by ESSO-UAM. Select the logon methods that you intend to use.

The available plug-ins are:

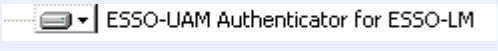
- Smart Card
- Proximity Card
- Fingerprint
- BioAPI

To avoid performance issues and potential conflicts, the recommended best practice is to install only the logon methods you intend to use.



ESSO-UAM Authenticator for ESSO-LM

(*requires ~105KB of space*)
The ESSO-UAM Authenticator plug-in integrates ESSO-UAM with ESSO-LM. If ESSO-LM is installed after ESSO-



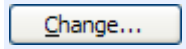
ESSO-UAM Authenticator for ESSO-LM

UAM, you can Modify the ESSO-UAM installation to install the ESSO-UAM Authenticator.

The ESSO-UAM Authenticator option is only available if you already have the ESSO-LM Agent installed on the workstation.

Change

Click this button to change the current installation destination folder for the Client. Browse to the location and click **OK**.

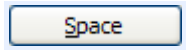


Help

Click the **Help** button to display Custom Setup tips.

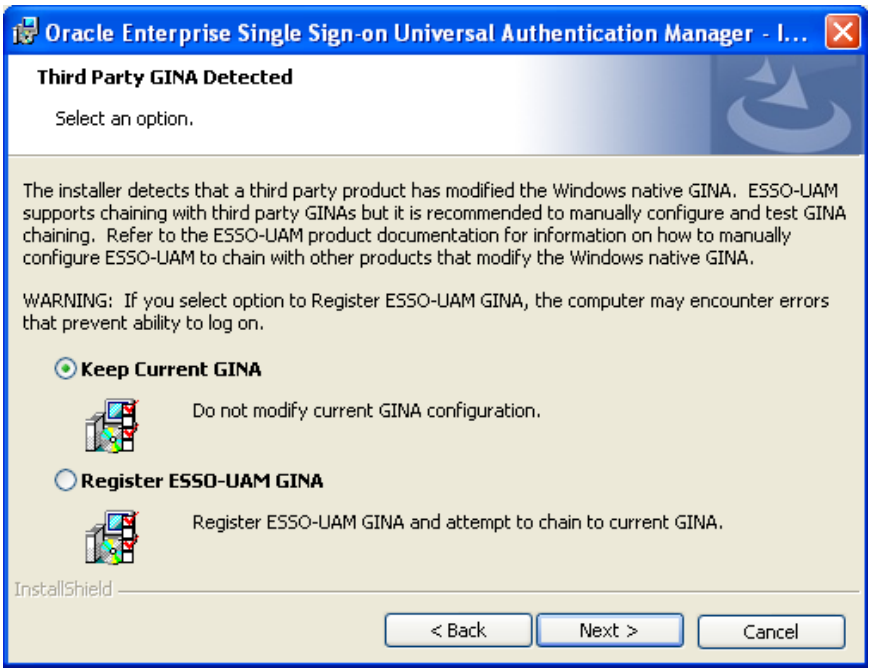
Space

Click **Space** to display the **Disk Space Requirements** for the installation of the selected features on local workstations. Click **OK**.



5. Select the Client Mode.
   - **Local Client Mode:** ESSO-UAM runs locally and does not synchronize with the repository.
   - **Enterprise Client Mode:** ESSO-UAM runs in an Enterprise environment and synchronizes with the repository.

6. If the installer detects a third-party GINA, it prompts you to choose between keeping the current GINA and registering the ESSO-UAM GINA. Oracle recommends that, if you choose to chain the GINAs, you verify in a test environment that the configuration is stable. See GINA Chaining for more information.



7. If you selected to install the ESSO-UAM Authenticator for ESSO-LM in step 4, the installer proceeds with the next step, depending on whether or not ESSO-LM is detected with any strong authenticators installed. The ESSO-UAM Authenticator for ESSO-LM allows for integration with ESSO-LM.

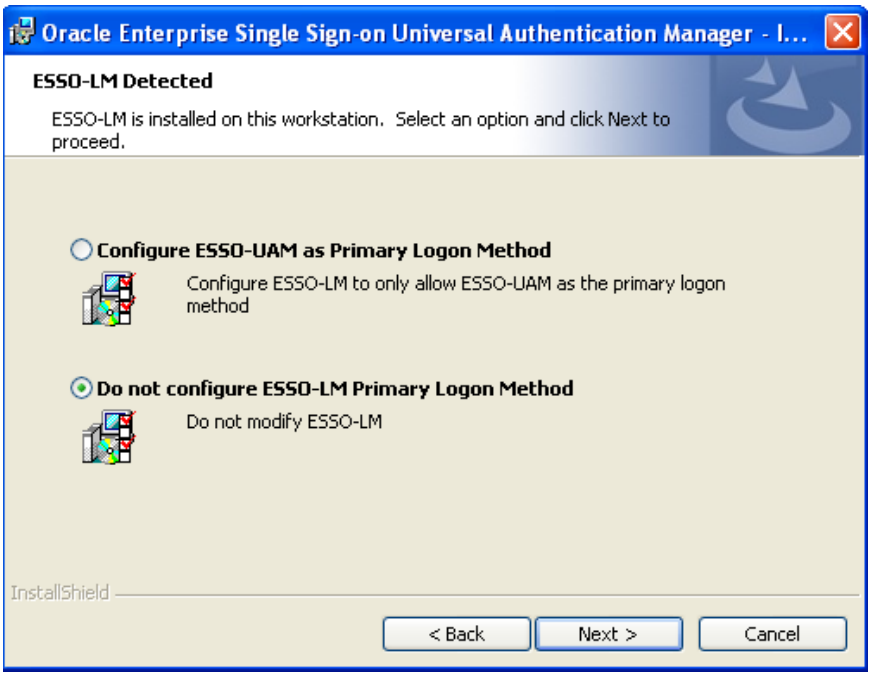
   ESSO-LM installed with Strong Authenticators

   When the installer detects that ESSO-LM is installed along with at least one strong authenticator and the ESSO-UAM Authenticator custom setup option has been enabled for installation, the installer will not ask if you want to configure ESSO-UAM as the ESSO-LM primary logon method.

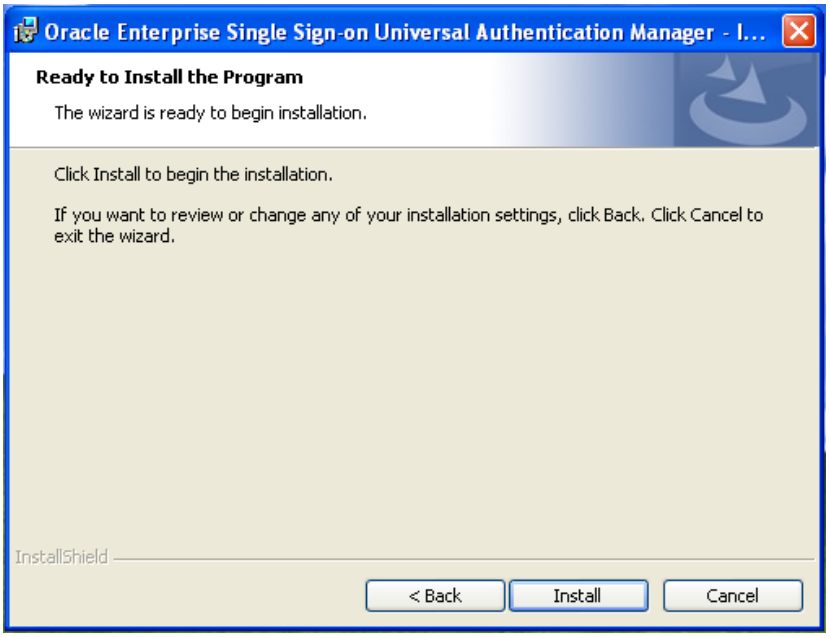
   ESSO-LM installed without Strong Authenticators

   When the installer detects that ESSO-LM is installed without any strong authenticators and the ESSO-UAM Authenticator custom setup option has been enabled for installation, the installer will ask if you want to configure ESSO-UAM as the ESSO-LM primary logon method. If you select to configure ESSO-UAM as the ESSO-LM primary logon method, **Universal Authentication Manager** will be the only available option in the Primary Logon dropdown of ESSO-LM First-Time Use (FTU) Wizard. For more information on the FTU Wizard, see the *ESSO-LM User Guide*.

   Make your selection and click **Next**.



8. The InstallShield Wizard is ready to begin the installation. Click **Install**.



9. Wait for the installation to complete. When the Completed screen appears, click **Finish**.

10. After installation is complete, you are prompted to restart your workstation.
    - If you installed the Client in Local Mode, click **Yes** now.
    - If you installed the Client in Enterprise Mode, click **No** and proceed to Configuring the ESSO-UAM Service Account.

Configuring the ESSO-UAM Service Account

When running the Client in Enterprise mode, you must follow the instructions in this section to configure each ESSO-UAM client so that they will be able to synchronize with an Enterprise repository.

> Some steps in this section need to only be performed once. Other steps must be performed every time ESSO-UAM is installed or upgraded.

Step 1: Installation or Upgrade

The ESSO-UAM Service Account must be a Local Administrator on each client system. This step only needs to be done once per client, and should be done immediately after the client has been installed. These steps can be done before or after rebooting the system. You can add the ESSO-UAM Service Account to the local Administrators group on each client. This is done through the Computer Management console:

1. Click **Start** > **Run** > and type **compmgmt.msc** and click **OK**. The Computer Management console opens.
2. Expand **Systems Tools** and then expand **Local Users and Groups** and click **Groups**.
3. In the right pane, right-click on **Administrators** and select **Add to Group...**.
4. Click **Add**. Enter the username of the ESSO-UAM Service Account that you created, and click **OK**.

Step 2: Configure the Service

The Windows Services console can be used to configure the service to run under the ESSO-UAM Service Account, and to automatically grant the account the Log On As Service local privilege. This step must be performed after *every* ESSO-UAM installation. This is done through the Windows Services console:

1. Click **Start** > **Run** > and type **services.msc** and click **OK**. The Services console opens.
2. Double-click the UAM Authentication Service. The Properties dialog will open.
3. On the Log On tab, select **This account**. Enter the username of the ESSO-UAM Service Account that you created into the **This account** field and enter and confirm the password.
4. Click **Apply**. The first time this step is done, you will receive a message that the Log On As Service right has been granted.

Step 3: Restart the Service

Restart the service to verify the new settings are working and the ESSO-UAM Service Account can start. If the ESSO-UAM Service Account is not working, you can try to revert to the Local System, restart the service, review and correct the settings, and try again.

To restart the service, right-click the service and click **Restart**.

> Do not leave the service in a stopped state. If the service is left in a stopped state, users may not be able to log on.

Uninstall

To undo these steps and return to a clean system:

1. Uninstall ESSO-UAM or set the ESSO-UAM Service Account back to Local System and restart.
2. Click **Start** > **Run** > and type **compmgmt.msc** and click **OK**. The Computer Management console opens.
3. Expand **Systems Tools** and then expand **Local Users and Groups** and click **Groups**.
4. In the right pane, right-click on **Administrators** and select **Add to Group...**.

5. Highlight the service user name and click **Remove**.
6. Click **Start** > **Run** > and type **secpol.msc** and click **OK**. The Local Security Policy console opens.
7. Double-click the ESSO-UAM Service Account. The Properties dialog will open.
8. Expand **Local Policies** and then expand **User Rights Assignment**.
9. Double-click the **Log on as a Service** policy.
10. Highlight the ESSO-UAM Service Account and click **Remove**.

Configure ESSO-UAM to use an ADAM or AD LDS Repository

This step only needs to be performed if you are using an ADAM or AD LDS repository. This step must be performed on each end-user workstation where ESSO-UAM will be syncing to ADAM or AD LDS.

1. Click **Start** > **Run** > and type **regedit.exe** and click **OK**.
2. Navigate to the `HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix\UAM\ Sync-Manager\Synchronizers\ADSI` registry key.
3. Create the following values:

   `REG_DWORD: StoreUserDataUnderProgramData`. The **Value Data** field must be set to 1.

   `REG_SZ: UAMProgramDataLocation`. Configure this value to store the location of the ESSO-UAM program data container in the form of LDAP ADsPath (LDAP://hostname:port/path_to_UAM_folder,default_naming_context).

   Examples:
   "`LDAP://win200864:53999/CN=UAM,CN=Passlogix,CN=Program Data,OU=U-AMPartition,DC=PLXENG,DC=COM`"

   In this example, win200864 is the AD LDS server name, 53999 is the AD LDS port number, and OU=UAMPartition,DC=PLXENG,DC=COM is the default naming context for the AD LDS ESSO-UAM instance.

   "`LDAP://server2003:50000/CN=UAM,CN=Passlogix,CN=Program Data,OU=U-AMPartition,DC=vgowin2k3r2,DC=local`"

   In this example, server2003 is the AD LDS server name, 50000 is the AD LDS port number, and OU=UAMPartition,DC=vgowin2k3r2,DC=local is the default naming context for the AD LDS ESSO-UAM instance.

Performing an Unattended (Silent) Installation

In order to install Oracle ESSO products successfully in unattended ("silent") mode, the Windows Management Instrumentation (WMI) service must be running before you execute the installer.

Verifying That the WMI Service Is Running

To check whether the WMI service is running, and start it if necessary, do the following on each target machine:

1. Click **Start** > **Run** > and type **services.msc** and click **OK** to open the Services snap-in.
2. Navigate to the Windows Management Instrumentation service and check its status and startup mode.
3. Depending on the status, do one of the following:
   - If the status is "Started," the WMI service is running; proceed to the next step.
   - If the status is blank, check the service's startup type and start it as follows:
     - If the startup type is "Disabled," do the following:
       a. Double-click the service.
       b. In the dialog box that appears, change the startup type to **Manual** or **Automatic**, as required by your environment.
       c. Click **Apply**.
       d. Click **Start** to start the service. The status changes to "Started."
     - If the startup type is not "Disabled," do the following:
       a. Double-click the service.
       b. In the dialog box that appears, click **Start** to start the service. The status changes to "Started."
       c. Click **OK**.
4. Click **OK** to close the service properties dialog box.

Command Line Syntax

ESSO-UAM supports standard MSIEXEC.exe command line parameters. The command line to perform an unattended installation uses the following sequence:

`MSIEXEC.exe [`*`Install Flag`*`] [MSI Installer `*`Filename`*`] [Custom Properties] [`*`User Interface Level Flag`*`]`

Where:

Install Flag: /i = install, /x = uninstall, /a = admin install

Filename: Name of the MSI package to install

Custom ESSO-UAM Installer Properties

The custom installer includes the ability to configure the following options:

- Option to select Local Client Mode (default) or Enterprise Client Mode
- Option to configure ESSO-LM to use ESSO-UAM as its Primary Logon Method
- Ability to select which GINA to use
- Ability to configure custom features to install

Use the following custom parameters to configure these installer options:

- **CLIENTMODE**
  - 0 = Local Client Mode (default)
  - 1 = Enterprise Client Mode
- **SSO_LOGONMETHOD**
  - Yes = Configure ESSO-UAM as the ESSO-LM Primary Logon Method
  - No = Do not configure ESSO-UAM as the only available ESSO-LM Primary Logon Method (default)
- **GINACHOICE**
  - 0 = Keep the current GINA (default)
  - 1 = Register ESSO-UAM GINA
- **ADDLOCAL**
  - "Application" (*Required*)
  - "SmartCard"
  - "ProximityCard"
  - "Fingerprint"
  - "BioAPI"
  - "UAMAuth"

  To configure which features are installed, use the standard "ADDLOCAL" command line option.

Do NOT use the ADDLOCAL property with Orca, which is command-line only.

Examples:

- `msiexec /i "ESSO-UAM.msi" ADDLOCAL ="Application,SmartCard,ProximityCard" CLIENTMODE=1 GINACHOICE=1`

  Installs ESSO-UAM with Smart Card and Proximity Card, in Enterprise Client mode, and using the ESSO-UAM GINA.
- `msiexec /qn /i "ESSO-UAM.msi" ADDLOCAL ="Application,SmartCard" CLIENTMODE=0 GINACHOICE=0`

  Installs ESSO-UAM with Smart Card only, in Local Client mode, and using the default GINA.
- `msiexec /qn /i "ESSO-UAM.msi" ADDLOCAL ="Application,Fingerprint" CLIENTMODE=0`

  Installs ESSO-UAM with Fingerprint only, in Local Client mode.
- `msiexec /i "ESSO-UAM.msi" ADDLOCAL="Application,ProximityCard,SmartCard,Fingerprint,BioAPI" CLIENTMODE=1 GINACHOICE=0`

  Installs ESSO-UAM with Proximity Card, Smart Card, Fingerprint, and BioAPI, in Enterprise Client mode, using the default GINA.

First-Time Logon for Enterprise Mode Users

It is recommended that you require Enterprise Mode users to perform their first-time logon in connected mode. If the workstation is not connected to the Active Directory Domain Controller, users will be able to log on but not enroll, because Windows cannot resolve the username while disconnected.

If users perform a first-time logon in disconnected mode, they might receive the following message when attempting to access to the Client application: "You cannot enroll in ESSO-UAM until you log on to Windows with the computer connected to the Windows network."

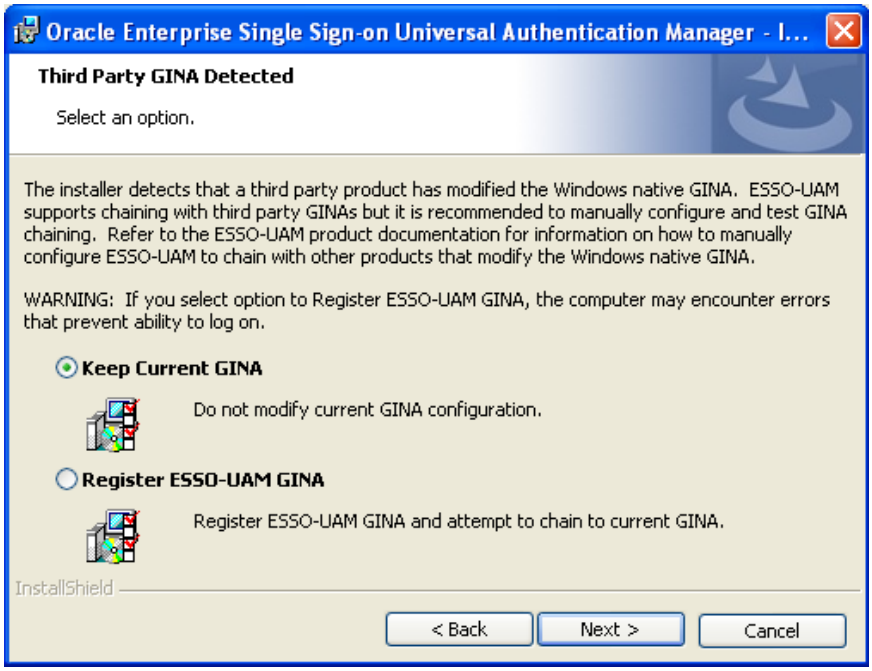
GINA Chaining

The ESSO-UAM GINA automatically chains with the ESSO-LM/ESSO-PR GINA and with the Microsoft GINA.

During installation or when performing maintenance, the ESSO-UAM installer resolves the GINA chain according to the following logic:

- If the current GINA is MSGINA, ESSO-UAM will automatically chain to it.
- If the current GINA is SSOGINA (used by ESSO-LM and ESSO-PR), ESSO-UAM configures SSO-GINA to chain to UAMGINA, which then chains to MSGINA.
- If the installer detects an unknown GINA, which was installed by a third-party product, it displays the "Third Party GINA Detected" screen, and prompts the administrator to choose between keeping the existing GINA configuration (default) or having ESSO-UAM attempt to register and chain with the third party GINA.

Using the third-party GINA will limit the functionality of the ESSO-UAM GINA to varying degrees, depending on the specific GINA. Oracle recommends replacing the third-party GINA with the ESSO-UAM GINA.



It is possible that choosing to chain the ESSO-UAM GINA with an unsupported GINA might result in an unrecoverable error. If you choose to attempt chaining to an unsupported GINA, be sure to verify that it will work by trying it in a test environment beforehand.

Recovering from Use of an Incompatible GINA

If the ESSO-UAM installer detects an unsupported GINA, it presents you with the following choices:

- Keep the current GINA
- Register ESSO-UAM GINA

If you opt to register the ESSO-UAM GINA, ESSO-UAM attempts to register UAMGINA and chain it to the unsupported GINA. If the third-party GINA is incompatible with UAMGINA, upon restart you might be unable to log on. In order to regain control of your workstation, perform the following steps to modify the registry manually:

1. Restart workstation, boot in Safe Mode and log on as a local administrator.

   Do not restart in Safe Mode with Networking or Safe Mode with Command Line. Refer to Microsoft documentation for more information about restarting your workstation in the different Safe Modes.

2. Click **Start** > **Run** > and type **regedit.exe** and click **OK** to launch the Registry Editor.
3. Select the GINA configuration that you want to use from the following list. If you plan to uninstall ESSO-UAM after recovery, deleting the `OrigGinaName` entry will prevent an unintended modification of the `GinaDLL` registry entry.
   - To restore the standard Windows logon:
     a. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` and delete the `GinaDLL` registry entry.
     b. Restart.
   - To configure for ESSO-UAM GINA only:
     a. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` and ensure that the GinaDLL registry entry is set to "UamGina.dll."
     b. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix\UAM\Gina` and delete any ChainToGinaName registry entry.
     c. Restart.
   - To restore any previously configured third-party GINA:
     a. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix\UAM\Gina` and copy the value of any `OrigGinaName` registry entry to `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GinaDLL`, or set `GinaDLL` to the name of the third-party GINA dll.
     b. Restart.

Migrating from ESSO-LM with Strong Authenticators to ESSO-UAM

Each client workstation with ESSO-LM may only be configured to use one primary logon method. ESSO-LM supports several native primary logon methods, including strong authenticators such as smart cards or proximity cards. If a strong authenticator is deployed and configured as the ESSO-LM primary logon method, each end user must convert to using ESSO-UAM as the primary logon method.

End users must manually change the ESSO-LM Primary Logon Method from the strong authenticator to the ESSO-UAM Authenticator using the ESSO-LM Agent Settings tab to Change Primary Logon Method.

Modifying ESSO-UAM

User data is preserved during a modification or upgrade (both local and roaming).

To modify this software:

1. Open the **Control Panel**.
2. Open **Add/Remove Programs**.
3. Scroll to the program name, select it, and click **Change**. The InstallShield Wizard welcome screen launches.
4. Click **Next>**.
5. On the Program Maintenance screen, select **Modify** and click **Next>**.
6. The InstallShield Wizard repeats the steps in the initial installation. Select the modifications you want to make, following the instructions in the installation section.

Refer to the appropriate section(s) of this guide to reconfigure ESSO-UAM as needed based on the modifications you choose to make.

7. Restart if necessary.

Repairing ESSO-UAM

User data is preserved during a repair (both local and roaming).

To modify this software:

1. Open the **Control Panel**.
2. Open **Add/Remove Programs**.
3. Scroll to the program name, select it, and click **Change**. The InstallShield Wizard welcome screen launches.
4. Click **Next>**.
5. On the Program Maintenance screen, select **Repair**and click **Next>**.
6. The InstallShield Wizard repeats the steps in the initial installation. Select the modifications you want to make, following the instructions in the installation section.

Refer to the appropriate section(s) of this guide to reconfigure ESSO-UAM as needed based on the modifications you choose to make.

7. Restart if necessary.

Authentication Service Repair Error

If you are working in Enterprise mode and your workstation has been configured so that the ESSO-UAM Authentication Service is logged on as the ESSO-UAM Service Account, you may see the following error message when you attempt to do a repair of the installation:

"Fatal error during installation."

The repair will not complete successfully.

To complete a repair:

1. Stop the UAM Authentication Service. From the Control Panel, launch Administrative Tools, and under Services, right-click the UAM Authentication Service and click **Stop**.
2. Right-click the UAM Authentication Service and click **Properties**. On the Log On tab, change the **Log On As** value from the ESSO-UAM Service Account user to the local system account.
3. Execute ESSO-UAM repair. From Control Panel, launch Add/Remove Programs, and start the ESSO-UAM installer.
4. Change the **Log On As** value back to the ESSO-UAM Service Account user.
5. Restart the UAM Authentication Service. From the Control Panel, launch Administrative Tools, and under Services, right-click the UAM Authentication Service and click **Start**.

Uninstalling ESSO-UAM

User data is preserved during an uninstall or upgrade, (both local and roaming).

To uninstall this software:

1. Click **Start**, point to **Settings**, and then click **Control Panel**.
2. Open **Add/Remove Programs**.
3. Scroll to the program name, select it, and click **Remove**.
4. A message appears asking if you are sure you want to remove Oracle Enterprise Single Sign-on Universal Authentication Manager from your computer. Click **Yes**.
5. Follow the prompts to uninstall the software.
6. Repeat to uninstall another component.
7. Restart if necessary.

Upgrade Notes

The previous version of this product, v-GO UAM version 7.0, is no longer supported and you cannot upgrade from this version.

If you have this version installed, the following cleanup steps are recommended:

1. In your current version of v-GO UAM, delete all the enrollments and synchronize the deletions using the v-GO UAM Client application. To do this, open the Client application and click the **Refresh** button.
2. Delete all the policy objects from the repository using the ESSO-LM Administrative Console. To do this:

   In the ESSO-LM Administrative Console tree on the left pane, click on **Repository**.

   On the right pane, click on the **Click here to connect** link.

   In the Connect to Repository dialog box, select **Microsoft Active Directory Server** from the dropdown menu, enter the **Server Name**, **Port**, and the **Username/ID** and **Password** . Click **OK** when finished.

   On the Repository AD LDS or ADAM instance on the right pane, navigate to **CN=Program Data** > **CN=Passlogix** > **CN=UAM** > **CN=Policies**.

   Delete all ESSO-UAM policies under this container.

The following steps are required:

1. Uninstall the v-GO UAM version 7.0 Client Application and any ESSO-LM Administrative Console versions earlier than 11.1.1.5.0.
2. Follow steps to install version 11.1.1.5.0.