Oracle® Enterprise Single Sign-on Universal Authentication Manager

Administrator's Guide

Release 11.1.1.5.0

E21029-01

March 2011

ORACLE®

Oracle Enterprise Single Sign-on Universal Authentication Manager, Administrator's Guide, Release 11.1.1.5.0

E21029-01

Table of Contents

Abbreviations and Terminology ... 5
About ESSO-UAM ... 6
  About this Guide ... 6
Administration Overview ... 7
Integrating with the ESSO-LM Administrative Console ... 8
  Configuring ESSO-LM to Use ESSO-UAM for Logon ... 8
Client Overview ... 9
  Local Client Mode ... 9
  Enterprise Client Mode ... 9
  Configuring the Client ... 9
ESSO-UAM Enterprise Synchronization ... 10
  How Synchronization Works ... 10
  Repository Functions ... 10
Logon Methods ... 11
  Fingerprint Logon Method ... 11
  BioAPI Logon Method ... 11
  Smart Card Method ... 12
  PIN Options for Account Security ... 12
  Proximity Card Method ... 13
  PIN Options for Account Security ... 13
About ESSO-UAM Policies ... 14
  Logon Method Enabled Policy ... 14
  Enrollment Prompt Policy ... 16
  Enrollment Grace Period Policy ... 18
Managing Policies in the ESSO-LM Administrative Console ... 20
Creating a New ESSO-UAM Policy ... 21
  The General Tab and Security Tab ... 21
  Logon Method Settings ... 22
Fingerprint Settings ... 23
BioAPI Settings ... 25
Proximity Card Settings ... 27
Smart Card Settings ... 29
Windows Password Settings ... 31
  General Tab (for a Selected Policy) ... 32
  Security Tab (for a Selected Policy) ... 32
Publishing an ESSO-UAM Policy ... 33
  Publishing a Policy ... 33
Modifying an ESSO-UAM Policy ... 43
  Copying and Modifying a Policy from the Repository ... 44
Compatibility with Windows Default Domain Policies ... 45
Authenticator Preferred Display Order ... 47
Troubleshooting ... 48
  Recovery from Deletion of the Service Account ... 48
  Authentication Service Repair Error ... 50
  AutoLogon Condition is Incorrectly Configured ... 51
  Avoid Using Dual Purpose Cards with Dual Purpose Readers ... 51
Configuring Your System with Settings and Registry Keys ... 52
  Managing Settings Configured in Multiple Locations ... 52

Global Client Settings 53
Global Branding Settings 59
Per-Computer Administrative Settings 62
Per-User Administrative Settings 64

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

About ESSO-UAM

Oracle Enterprise Single Sign-on Universal Authentication Manager 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.

At its core, ESSO-UAM offers a flexible, adaptable, and truly universal authentication solution, capable of integrating with a wide variety of authentication methods through its framework and APIs. Out-of-the-box, ESSO-UAM currently supports built-in and configurable authentication methods: smart cards, passive proximity cards, biometric fingerprint, BioAPI compatible biometric, and native Windows Password. ESSO-UAM associates an easily obtainable piece of data from a smart card or proximity card with a user account, so that the card or token can be used to identify and authenticate a user.

About this Guide

This guide is intended for experienced administrators responsible for the planning, implementation, and deployment of ESSO-UAM. Administrators are expected to understand single sign-on concepts and be familiar with Internet Information Services, Windows Registry settings, the ESSO-LM Administrative Console, and the process of creating users and user groups in Active Directory. Persons completing the installation and configuration procedure should also be familiar with their company's system standards.

Administration Overview

ESSO-UAM administrators can configure and apply ESSO-UAM policy settings from a central location using the ESSO-LM Administrative Console. The ESSO-LM Administrative Console contains ESSO-UAM settings that allow administrators to configure policies; these policies specify how various logon methods operate for different users and user groups.

A policy is simply a collection of settings that controls how a user or user group authenticates to the system. You can create as many policies as you need in order to establish secure authentication for all users throughout your enterprise, but you can only apply one policy per user or user group.

After you create a policy, you publish it to the supported repository and select which users it will govern. See Publishing an ESSO-UAM Policy for details.

Using the ESSO-LM Administrative Console, an administrator can perform the following tasks:

Manage ESSO-UAM Policies

- Create and configure new Policies
- Publish policies to users and user groups

Manage the Deployment

- Configure the centralized data repository. See the *ESSO-UAM Installation Guide* for information on performing this procedure.

Integrating with the ESSO-LM Administrative Console

Administrative functionality for ESSO-UAM is fully integrated within the ESSO-LM Administrative Console.

Configuring ESSO-LM to Use ESSO-UAM for Logon

You can configure ESSO-LM to use ESSO-UAM as its primary logon method. ESSO-UAM supports integration with ESSO-LM version 11.1.1.5.0.

When the ESSO-UAM installer detects that ESSO-LM is installed, the ESSO-UAM Authenticator custom setup option is displayed, allowing you to choose to install the adapter to enable integration with ESSO-LM. If you choose to install the adapter, the installer will ask if you want to configure ESSO-UAM as the only available ESSO-LM logon method. For details on installation, see the *ESSO-UAM Installation Guide*.

Client Overview

During installation, you can select whether to install the ESSO-UAM Client in either Local Client mode or Enterprise Client mode.

Local Client Mode

The Client runs on the local workstation and is not connected to the repository. In Local Mode, credentials and settings are stored and managed through the Client's local cache repository. If the Client is switched from Local Client to Enterprise Client mode to sync with the repository, any policy settings configured by the administrator will be enforced, and will override any local settings. User credentials are stored locally on the system that they were enrolled.

Password Security in Local Client Mode

In Local Client Mode, a security policy exists which limits the local account use of blank passwords to workstation logon only. When this setting is enabled (which is the default), local accounts with blank passwords can be used to log on to Windows, but not for reauthentication (that is, not for ESSO-LM authentication or ESSO-UAM enrollment operations). Oracle recommends that you always set (strong) passwords on all accounts.

Enterprise Client Mode

The Client runs as part of the enterprise and synchronizes to the repository. In Enterprise mode, the Client will operate while connected or disconnected from the repository domain.

- When the Client is connected to the repository domain and can synchronize with the repository, it synchronizes any policy changes during initial logon. After that, the Client performs periodic synchronizations.
- When a Client is disconnected from the repository domain and/or unable to synchronize with the repository, it utilizes its local cache repository. Any policy updates will not be effective until synchronization occurs.

Configuring the Client

Using the ESSO-LM Administrative Console, you create policies, which include Client configuration settings that specify how users enroll and manage logon methods.

You can also configure certain Client settings through registry keys. See Configuring Your System with Settings and Registry Values for a table of registry keys and their functions.

ESSO-UAM Enterprise Synchronization

ESSO-UAM leverages Microsoft Active Directory and ADAM/AD LDS, for centralized storage of ESSO-UAM policies. When an ESSO-UAM Client is configured to utilize a repository, it periodically performs a synchronization of policies.

Synchronization only takes place when a client workstation is configured in Enterprise Client mode to utilize a centralized repository. The repository itself must be properly configured to support ESSO-UAM synchronization (for information on preparing the repository, see the *ESSO-UAM Installation Guide*).

How Synchronization Works

Policy synchronization is "pull-down-only," meaning only the latest roaming policies published to each user are pulled down from the repository during synchronization.

ESSO-UAM synchronizes at a number of locations and times, depending on how you have configured your system. Data may be out-of-date at any given time; this is necessary to provide the highest level of performance for the typical cases where data does not change very often and thus no synchronization is required. By default, synchronization will occur at most once every five minutes, and will occur asynchronously, that is, in the background. You can customize synchronization settings using registry keys.

Repository Functions

- Stores ESSO-UAM policies.
- Manages storage leveraging the existing repository schemas used by other Oracle Enterprise Single Sign-on Suite Plus products.
- Secures data stored in repository; access is controlled.
- Maintains ESSO-UAM data separately from other Oracle Enterprise Single Sign-on Suite Plus product data.

Client Synchronization Functions

- Retrieves ESSO-UAM policies from the repository to local data cache.
- Reconciles data updated during offline operations from repository.
- Parses and transfers policy data to the registry.
- Enforces security for proper access rights to repository data.

Logon Methods

ESSO-UAM supports enrollment using a number of logon methods that permit users to enroll credentials. When you create a policy, you specify:

- Whether the logon method is enabled.
- Whether to require users to enroll.
    - If enrollment is required, whether there is an enrollment grace period, and how long the grace period should be.
- Other settings specific to each logon method.

Fingerprint Logon Method

ESSO-UAM enables you to enroll and use third party USB biometric fingerprint readers and readers embedded in laptops as an authentication mechanism to ESSO-UAM.

Administrators can configure up to ten fingerprint samples to be enrolled.

This logon method requires a supported biometric reader device and the BIO-key BioAPI BSP to be installed and configured on each user's system using this logon method. If this is not installed, users will get an error message.

To use the Fingerprint logon method, users must manually choose to log on with that method from the Logon dialog.

BioAPI Logon Method

ESSO-UAM enables you to enroll and use any third-party BioAPI-compliant Biometric Service Provider (BSP) module as an authentication mechanism to ESSO-UAM. In addition to fingerprint biometrics, this logon method may also support other biometric technologies that offer a BSP such as palm, facial, and iris recognition solutions.

This logon method requires a supported biometric reader device and BioAPI compatible BSP middleware on each user's system. If the BioAPI BSP is not installed and properly configured with a compatible biometric reader device, users will get an error. Refer to the BSP documentation for installation instructions.

To use the BioAPI logon method, users must manually choose to log on with that method from the Logon dialog.

There are several manual steps required to properly configure the BioAPI Logon Method for use with ESSO-UAM. These steps are detailed in the *ESSO-UAM Installation Guide*.

Smart Card Method

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 to the smart card. ESSO-UAM also supports the option to require a smart card PIN during logon for stronger user authentication.

User logon and unlock can be initiated by card detection, or a user can manually choose to logon or unlock using this method. Users will insert an enrolled card to an attached reader to initiate a logon or unlock.

ESSO-UAM supports two smart card authentication methods:

- Smart card alone
- Smart card plus PIN (default value)

PIN Options for Account Security

Smart cards have associated PINs for stronger account security. By default, users are required to enter the PIN during enrollment and authentication.

Oracle strongly recommends always using PINs associated with smart cards as a best practice for increased security.

Smart cards issued to users have an associated PIN that is stored and managed on each card. ESSO-UAM provides the options to use the smart card alone for enrollment and authentication, or to challenge users to supply a smart card's PIN. You can specify whether users are prompted to enter a card's PIN with the **PIN Required** setting.

A policy setting controls whether ESSO-UAM will utilize and prompt for a card's PIN.

During card enrollment, a user must correctly submit a smart card's PIN value before a card can be enrolled as a security measure to ensure that the user knows the associated PIN value. When the card is used for authentication, the user will be prompted for the card's PIN in order to successfully authenticate.

Proximity Card Method

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 logon method includes the option to require a user to enroll a PIN that is associated with a proximity token. When so configured, ESSO-UAM prompts the user for the enrolled PIN associated with a token during logon, strengthening user authentication.

User logon and unlock can be initiated by card detection, or a user can manually choose to logon or unlock using this method. Users will insert or tap an enrolled card on an attached reader to initiate a logon or unlock.

When presenting a proximity card, users must tap-and-hold the proximity card until the software noticeably responds to the event. You can adjust the minimum token presence required before a proximity token is recognized by using the MinPresence setting in the registry. See the Configuring Your System with Settings and Registry Keys section for more information on this setting.

Like smart cards, proximity cards will be enrolled by retrieving each card's unique serial number and securely associating its value with a single repository user account.

ESSO-UAM supports two proximity card authentication methods:

- Proximity card alone
- Proximity card plus ESSO-UAM PIN (default value)

PIN Options for Account Security

Proximity cards can have associated PINs for stronger account security. By default users are required to create the PIN during enrollment, and supply the PIN for authentication.

Oracle strongly recommends always using PINs associated with proximity cards as a best practice for increased security.

PINs for proximity cards are created by the user and stored by ESSO-UAM (as opposed to smart card PINs, which are stored and managed on the card). An ESSO-UAM PIN feature is integrated into the proximity card authenticator, enabling users to enroll an optional PIN value that is linked and stored with each enrolled card.

A policy controls whether a card's ESSO-UAM PIN is required for user authentication. When an ESSO-UAM PIN is required, a PIN prompt dialog will appear after the card is presented to and detected by a reader.

If a policy is configured to require the card and a PIN, during the card enrollment flow the user will be required to enroll an ESSO-UAM PIN in conjunction with the card together as one event.

About ESSO-UAM Policies

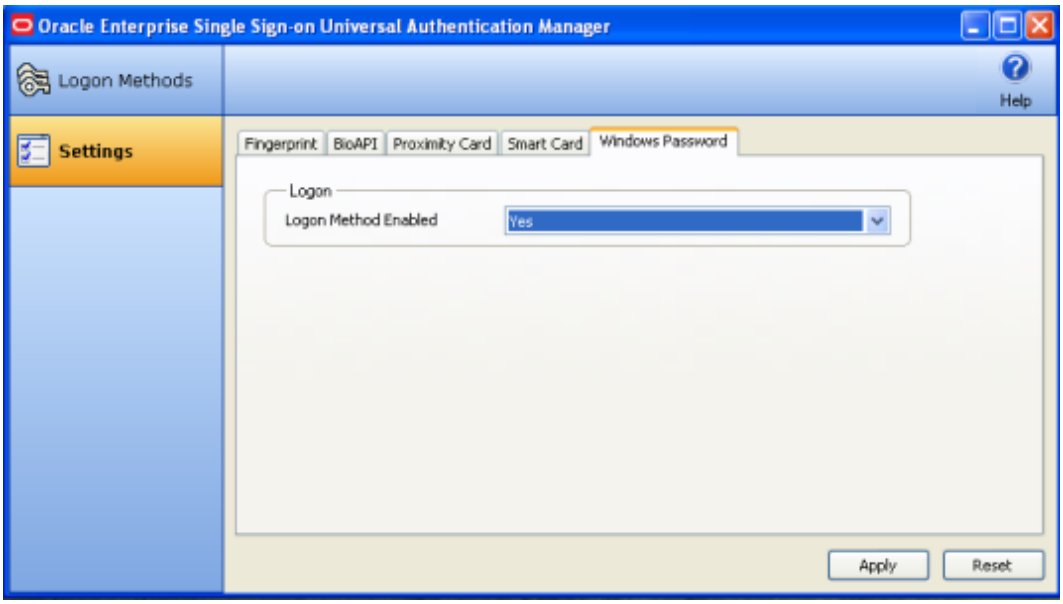
This section describes the policies that apply to *all* of the logon methods. For policies specific to a particular logon method, see the specific logon method settings section for a description.

Logon Method Enabled Policy

The Logon Method Enabled policy is a per-logon method policy that allows administrators or users to disable an installed ESSO-UAM logon method.

This policy applies to all logon methods individually and each logon method will have its own value.

- In Enterprise Client Mode, the Logon Method Enabled policy setting is an Administrative policy only. This means that the policy will never appear in the ESSO-UAM Client Application settings.
- In Local Client Mode, the Logon Method Enabled policy setting is an end-user policy setting. You can manage the policy setting right from the Settings tab in the ESSO-UAM Client Application:



Windows Password Exception

ESSO-UAM automatically enables Windows Password authentication if no other logon methods are enrolled.

This is a "built-in" behavior that requires no configuration. For example, if you've disabled Windows Password via the Logon Method Enabled policy, a password will be allowed for logon, re-authentication and unlock, *if* you are not enrolled in at least one other method.

> If you are enrolled in one or more other methods, but those methods (and password) are all disabled, you will be locked out. The Administrator will have to correct this by re-configuring the Logon Method Enabled policy in the ESSO-LM Administrative Console.

Configuring the Policy

Before you publish the Logon Method enabled policy:

- You must install the ESSO-LM Administrative Console on the system.
- You must install the ESSO-UAM Client in Enterprise Client Mode on the end-user's system.
- You must install the enabled logon method on the end-user's system.
- You must configure the end user's system for synchronization to the repository.

To configure the policy:

1. Launch the ESSO-LM Administrative Console.
2. Either create a new ESSO-UAM policy or select an existing one to modify.
3. Enable or disable each logon method by setting the Logon Method Enabled value to **Yes** or **No**.
4. Publish the new / changed ESSO-UAM policy to the UAM Storage Container for your user or user group in the repository so that the ESSO-UAM Client will apply the policy to the end-user.
5. The ESSO-UAM Client syncs the ESSO-UAM policy for the end-user.

Logon Method Enabled Rules

If the Logon Method Enabled is configured to **No** for a logon method:

- The logon method is displayed in the ESSO-UAM Client Application Logon Methods tab with a status of DISABLED. The only action users are allowed to perform is a Delete, as long as they are enrolled using the logon method. No other enrollment actions (Enroll or Modify) are available.
- In Enterprise Client Mode, the logon method appears in the ESSO-UAM Client Application Settings tab. All policy settings are disabled, and the Logon Method Enabled policy setting is not displayed.
- In Local Client Mode, the logon method appears in the ESSO-UAM Client Application Settings tab. The Logon Method Enabled policy setting is enabled, and all other policy settings are disabled.
- Users are not allowed to log onto or enroll on the workstation using that logon method. If they attempt to log on with a disabled logon method, they will receive an error message.
- Users are not allowed to re-authenticate using the logon method and will not see the logon method as an authentication option. A password authentication is enabled for Logon, Unlock, and Re-authentication, if they are not enrolled in any other method.

Enrollment Prompt Policy

The Enrollment Prompt is a per-logon method policy that controls whether end-users are prompted to enroll credentials for a specific logon method and if the enrollment is optional or required. This applies to all logon methods that support enrollment (not Windows Password), and each logon method will have its own value. The options are:

- **Never**. Users will not be prompted to enroll in that logon method.
- **Optional** (default). Users are prompted to enroll in the logon method each time they log on to their system as well as every time they launch the ESSO-UAM Client.
- **Required**. Users are prompted to enroll in this logon method. Unless a Grace Period exists or an alternative logon method, such as Windows Password, is enabled, they will not be able to log on to their systems unless they enroll in this logon method.

If multiple logon methods are set to optional or required, users will be consecutively prompted to enroll each logon method. When prompted to enroll in each logon method, they may choose from the following options:

- **Enroll**. Enroll in the logon method now.
- **Not Now**. Exit and ask me to enroll later. This option does not exist when an enrollment is required and a Grace Period has not been set.
- **Never**. Exit and do not ask me to enroll again. This option only exists when this policy is set to Optional.

This policy works in tandem with the Grace Period policy. When Enrollment Prompt is set to "Required" and a Grace Period is set, you can require enrollment with a specific logon method without immediately restricting end-users' access to systems. You can configure a suitable number of days in which an end-user will be allowed to defer enrollment.

The Enrollment Prompt policy setting is an Administrative Enterprise Client Policy only. You can edit the policy setting only by using the ESSO-LM Administrative Console.

> Enrollment Grace Period does not appear as a user setting in the ESSO-UAM Client in either Local or Enterprise Client Mode. The value defaults to zero, and may be overridden by a policy in Enterprise Mode.

Configuring the Policy

Before you publish the Enrollment Prompt policy:

- You must install the ESSO-LM Administrative Console on the system.
- You must install the ESSO-UAM Client in Enterprise Client Mode on the end-user's system.
- You must install the desired logon method on the end-user's system.
- You must configure the end user's system for synchronization to the repository.

To configure the policy:

1. Launch the ESSO-LM Administrative Console.
2. Either create a new ESSO-UAM policy or select an existing one to modify.
3. Set the Enrollment Prompt value for each logon method to Never, Optional or Required.
4. Publish the new / changed ESSO-UAM policy to the UAM Storage Container for your user or user group in the repository so that the ESSO-UAM Client will apply the policy to the end-user.
5. The ESSO-UAM Client syncs the ESSO-UAM policy for the end-user.

Enrollment Grace Period Policy

The Enrollment Grace Period is a per-logon method policy that allows end-users to defer a required enrollment for a configured number of days (the grace period). This applies to all logon methods that support enrollment (not Windows Password) individually, and each logon method will have its own value.

This feature allows you to require enrollment with a specific logon method without immediately restricting end-users' access to workstations. You can configure a suitable number of days in which an end-user will be allowed to defer enrollment.

The Enrollment Grace Period policy setting is an Administrative Enterprise Client Policy only. You can edit the policy setting only by using the ESSO-LM Administrative Console.

The Enrollment Grace Period policy setting is a numeric policy editor restricted to the range of zero to 365 days.

Enrollment Grace Period does not appear as a user setting in the ESSO-UAM client in either Local or Enterprise Client Mode. The value defaults to zero, and may be overridden by a policy in Enterprise Mode.

Configuring the Policy

Before you publish the Grace Period policy:

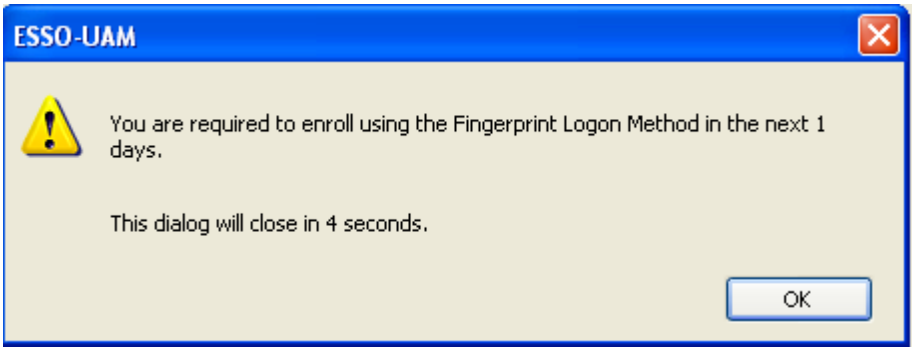
- You must install the ESSO-LM Administrative Console on the system.
- You must install the ESSO-UAM Client in Enterprise Client Mode on the end-user's system.
- The ESSO-UAM Client must operate in Enterprise Client Mode.
- You must install the desired logon method on the end-user's system.
- You must configure the end user's system for synchronization to the repository.

To configure the policy:

1. Launch the ESSO-LM Administrative Console.
2. Either create a new ESSO-UAM policy or select an existing one to modify.
3. At a minimum, enable and configure the following policies for the desired logon method:
   - Set Enrollment Grace Period to a value greater than zero.
   - Set Enrollment Prompt to "Required."
4. Publish the new/changed ESSO-UAM policy to the UAM Storage Container for your user or user group in the repository so that the ESSO-UAM Client will apply the policy to the end-user.
5. The ESSO-UAM Client syncs the ESSO-UAM policy for the end-user.

At the next system logon, users see that they have a set number of days to enroll using the desired logon method.

If the user clicks **Not Now**, a message box appears, stating how many days remain within the grace period.



Conditions that Disable the Policy

The Enrollment Grace Period will not be in effect (that is, it will be disabled) if any of the following conditions are met:

- The Logon Method Enrollment Prompt policy setting is NOT configured to "Required."
- The Logon Method Enrollment Grace Period policy setting is configured to zero.

Managing Policies in the ESSO-LM Administrative Console

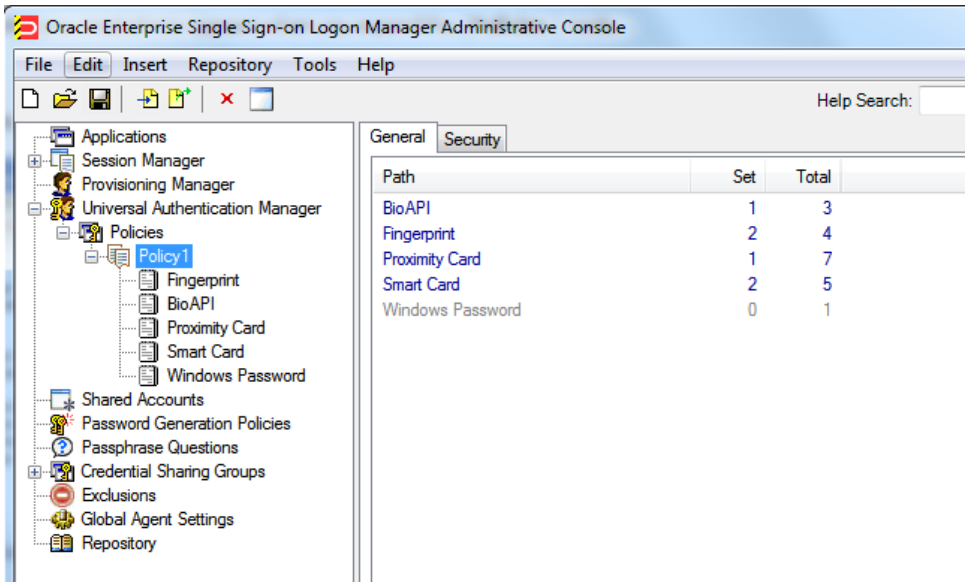
ESSO-UAM administrators can configure and apply ESSO-UAM policy settings from a central location using the ESSO-LM Administrative Console. The ESSO-LM Administrative Console contains ESSO-UAM functions that allow administrators to configure policies. Policies control the privileges, restrictions, and enforcement of enrollment and logon rules for Active Directory users who log on to workstations connected to an Active Directory domain. Each policy you create contains a unique set of conditions for using ESSO-UAM that you can apply to users and user groups.

Under **Universal Authentication Manager** in the left pane, select **Policies**. The right pane will display the following items:

- **Policy Name**: The name you give to a policy.
- **Items Set**: The number of settings, or details, that have been configured for that policy.
- **Total Items**: The total number of settings available for configuration.
- **Add**: Click this button to create a new policy.
- **Delete**: Click this button to remove a policy from the list.

To modify the settings for a policy,

1. Double-click the policy name in the right pane or expand **Policies** in the left pane.
2. Under **Policies**, double-click the policy name.



3. Under the policy name, click the logon method you wish to modify.

After creating policies, you must publish them in order to apply them to users and user groups. See Publishing a UAM Policy for this procedure.

Creating a New ESSO-UAM Policy

To create a new ESSO-UAM policy, do one of the following:

- Click **Universal Authentication Manager** in the left pane. In the right pane, click **Add Policy** at the bottom of the screen.

  or

- Expand **Universal Authentication Manager** in the left pane and select **Policies**. Click the **Add** button at the bottom of the screen.

  or

- Right-click **Universal Authentication Manager** or **Policies** in the left pane and select **New Policy**.

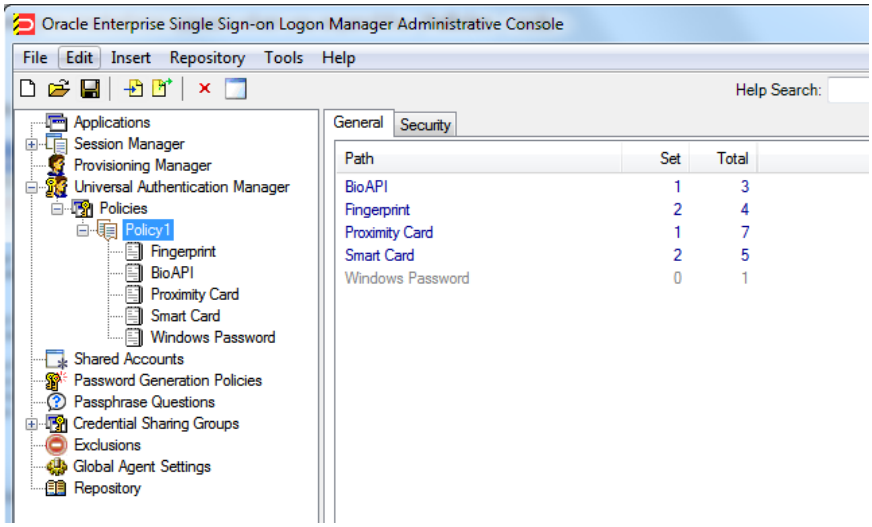
  or

- Select **UAM Policy** from the Insert menu.

A dialog box opens, prompting you to name the policy. Enter a name for the policy and click **OK**. The policy you created now appears when you expand the **Policies** node.

The General Tab and Security Tab

When you click the name of the policy, you will see two tabs in the right pane: **General** and **Security**.



The General tab shows general information about the policy. The Security tab shows Security information about the policy. For details, see General Tab (for a Selected Policy) and Security Tab (for a Selected Policy).

Logon Method Settings

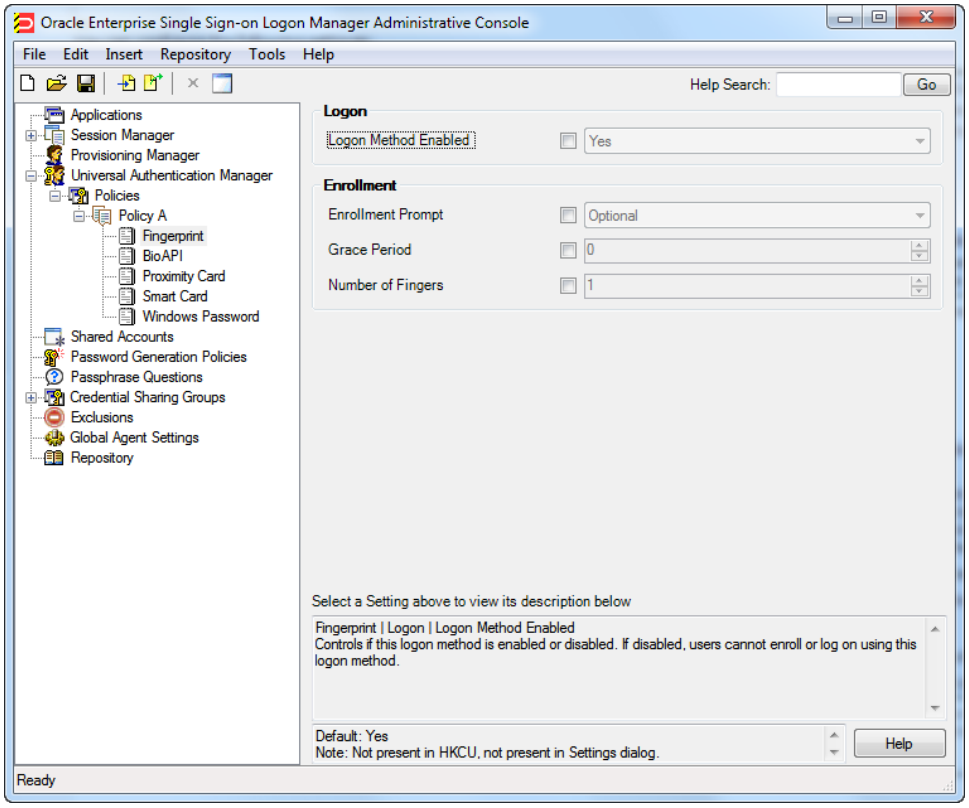
Expand the node for your policy set. Options for all of the logon methods appear below the policy name. Using these options, you can configure settings for each logon method within that particular policy set. For details on each logon method settings, see:

- Fingerprint Settings
- BioAPI Settings
- Proximity Card Settings
- Smart Card Settings
- Windows Password Settings

As a best security practice, Oracle recommends that you configure and apply policies for users to prevent them from configuring their own settings. If you do not define policies for users, they can define and change their own settings.

Fingerprint Settings

When you select **Fingerprint** for a chosen policy, you are presented with all of the available fingerprint settings. All settings will be disabled by default and set to default values; to change a setting, select the check box next to the setting and configure a value.



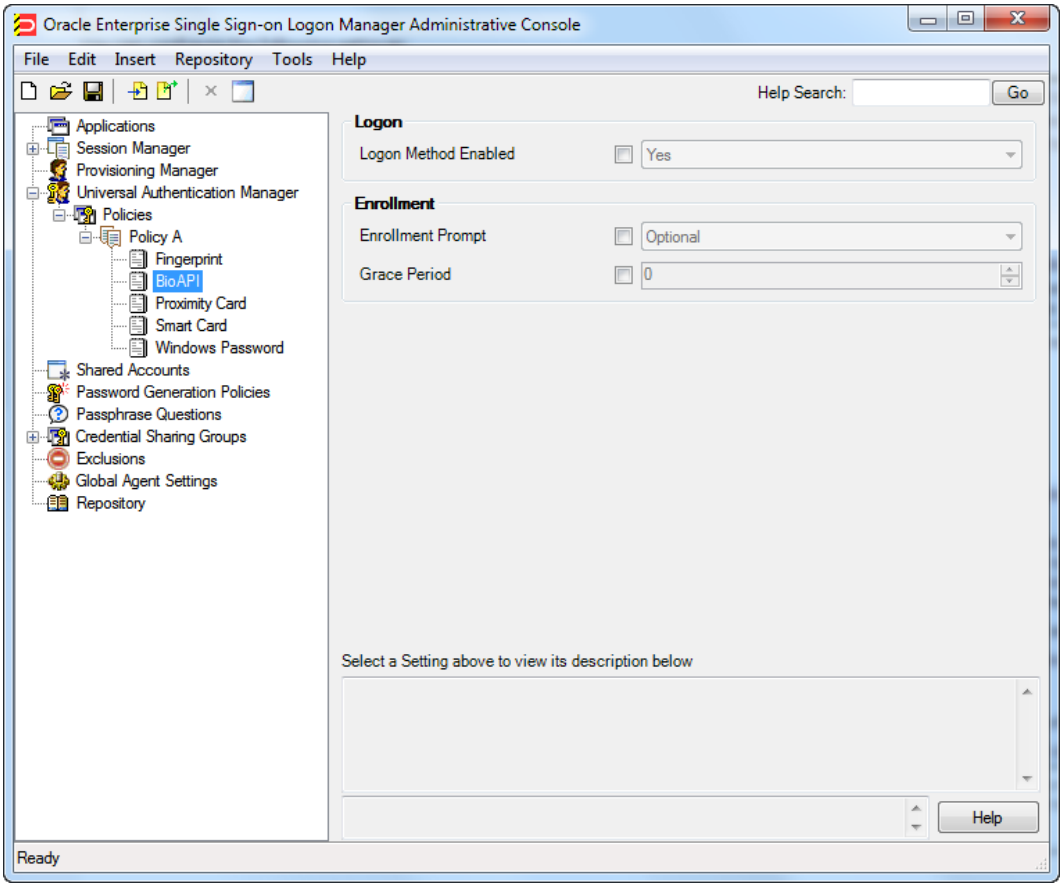
You can configure the following settings:

Logon Method Enabled	Allows you to enable or disable an installed authenticator on an ESSO-UAM Client. This policy setting enhances security by controlling the specific logon methods that end-users are allowed to use. **Options:** • Yes (default) • No If you select **No**, the end-user is not allowed to log on to or enroll on the workstation using this logon method. If users attempt to log on with a disabled logon method, they will receive an error message.
Enrollment Prompt	Controls whether a user is prompted to enroll and whether enrollment is optional or required. **Options:** • Never • Optional (default) • Required
Grace Period	Allows end-users to defer a required enrollment for a configured number of days (the grace period).

	Allows administrators to require enrollment with a desired logon method without immediately restricting end-users' access to workstations. Administrators can configure a suitable number of days in which an end-user will be allowed to defer enrollment. The Enrollment Grace Period is disabled if any of the following conditions are met: • The **Enrollment Prompt** policy setting is NOT configured to "Required." • This setting is configured to zero. Default is 0. Maximum grace period is 365 days.
Number of Fingers	Specifies the number of fingers the user is required to enroll. This policy requires the user to enroll exactly the specified number of finger samples during enrollment. Default is 1.

BioAPI Settings

When you select **BioAPI** for a chosen policy, you are presented with all of the available BioAPI settings. All settings will be disabled by default and set to default values; to change a setting, select the check box next to the setting and configure a value.



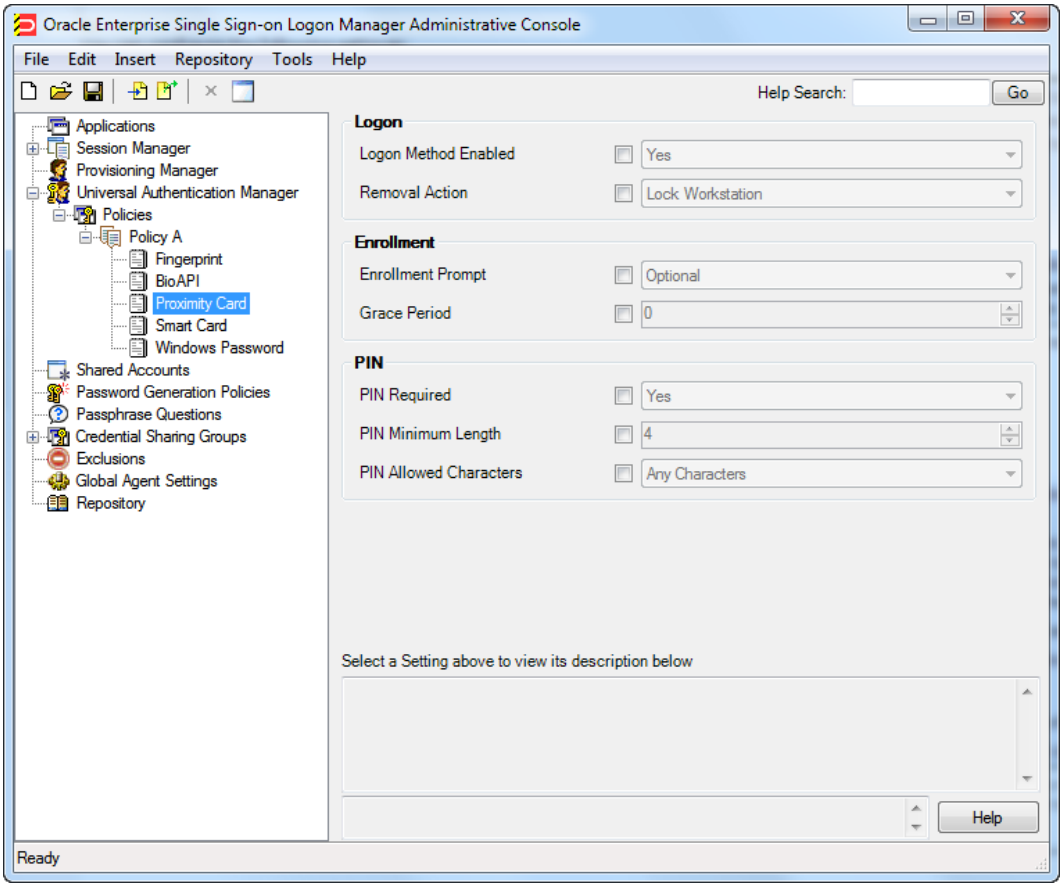
You can configure the following settings:

Logon Method Enabled	Allows administrators to enable or disable an installed authenticator on an ESSO-UAM Client. This policy setting enhances security by controlling the specific logon methods that end-users are allowed to use. **Options:** • Yes (default) • No If you select **No**, the end-user is not allowed to log on to or enroll on the workstation using this logon method. If users attempt to log on with a disabled logon method, they will receive an error message.
Enrollment Prompt	Controls whether a user is prompted to enroll and whether enrollment is optional or required. **Options:** • Never • Optional (default) • Required

Grace Period	Allows end-users to defer a required enrollment for a configured number of days (the grace period). Allows administrators to require enrollment with a desired logon method without immediately restricting end-users' access to workstations. Administrators can configure a suitable number of days in which an end-user will be allowed to defer enrollment. The Enrollment Grace Period is disabled if any of the following conditions are met: • The **Enrollment Prompt** policy setting is NOT configured to "Required." • This setting is configured to zero. Default is 0. Maximum grace period is 365 days.

Proximity Card Settings

When you select **Proximity Card** for a chosen policy, you are presented with all of the available proximity card settings. All settings will be disabled by default and set to default values; to change a setting, select the check box next to the setting and configure a value.



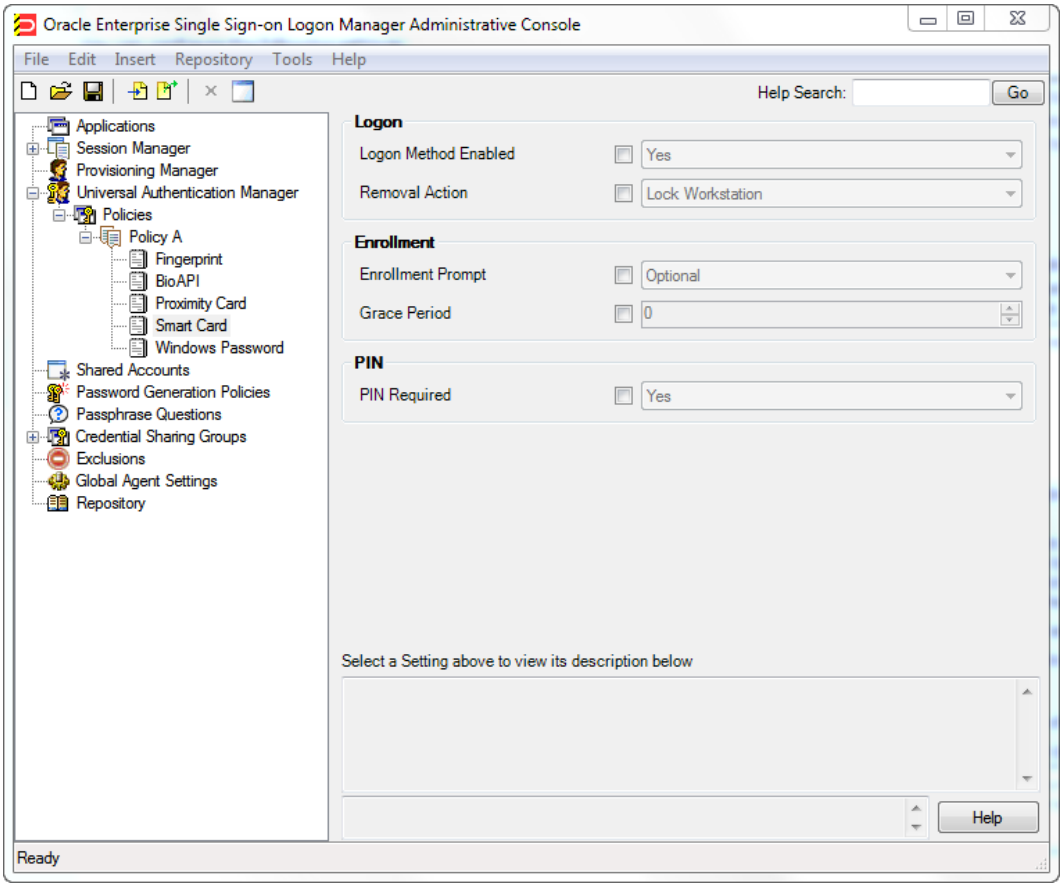
You can configure the following settings:

Logon Method Enabled	Allows administrators to enable or disable an installed authenticator on an ESSO-UAM Client. This policy setting enhances security by controlling the specific logon methods that end-users are allowed to use. **Options:** • Yes (default) • No If you select **No**, the end-user is not allowed to log on to or enroll on the workstation using this logon method. If users attempt to log on with a disabled logon method, they will receive an error message.
Removal Action	Controls how the computer responds to a proximity card event when a user is logged on. Removal Action is only enforced when the corresponding logon method was the last method used to log on to or unlock the computer. **Options:** • No Action

	• Lock Workstation (default) • Force Logoff
Enrollment Prompt	Controls whether a user is prompted to enroll and whether enrollment is optional or required. **Options:** • Never • Optional (default) • Required
Grace Period	Allows end-users to defer a required enrollment for a configured number of days (the grace period). Allows administrators to require enrollment with a desired logon method without immediately restricting end-users' access to workstations. Administrators can configure a suitable number of days in which an end-user will be allowed to defer enrollment. The Enrollment Grace Period is disabled if any of the following conditions are met: • The **Enrollment Prompt** policy setting is NOT configured to "Required." • This setting is configured to zero. Default is 0. Maximum grace period is 365 days.
PIN Required	Controls if a user is required to enroll a PIN that is associated with the card. If a PIN is required, after the proximity card is presented to reader, the user will be challenged to submit the PIN to authenticate. **Options:** • Yes (default) • No
PIN Minimum Length	The minimum allowed length of the proximity card PIN. **Options:** • Possible values 4-16 (default is 4)
PIN Allowed Characters	The character sets allowed for users to enroll a PIN that is associated with a proximity card. **Options:** • Any characters (default) • Alphanumeric only • Numeric only

Smart Card Settings

When you select **Smart Card** for a chosen policy, you are presented with all of the available smart card settings. All settings will be disabled by default and set to default values; to change a setting, select the check box next to the setting and configure a value.



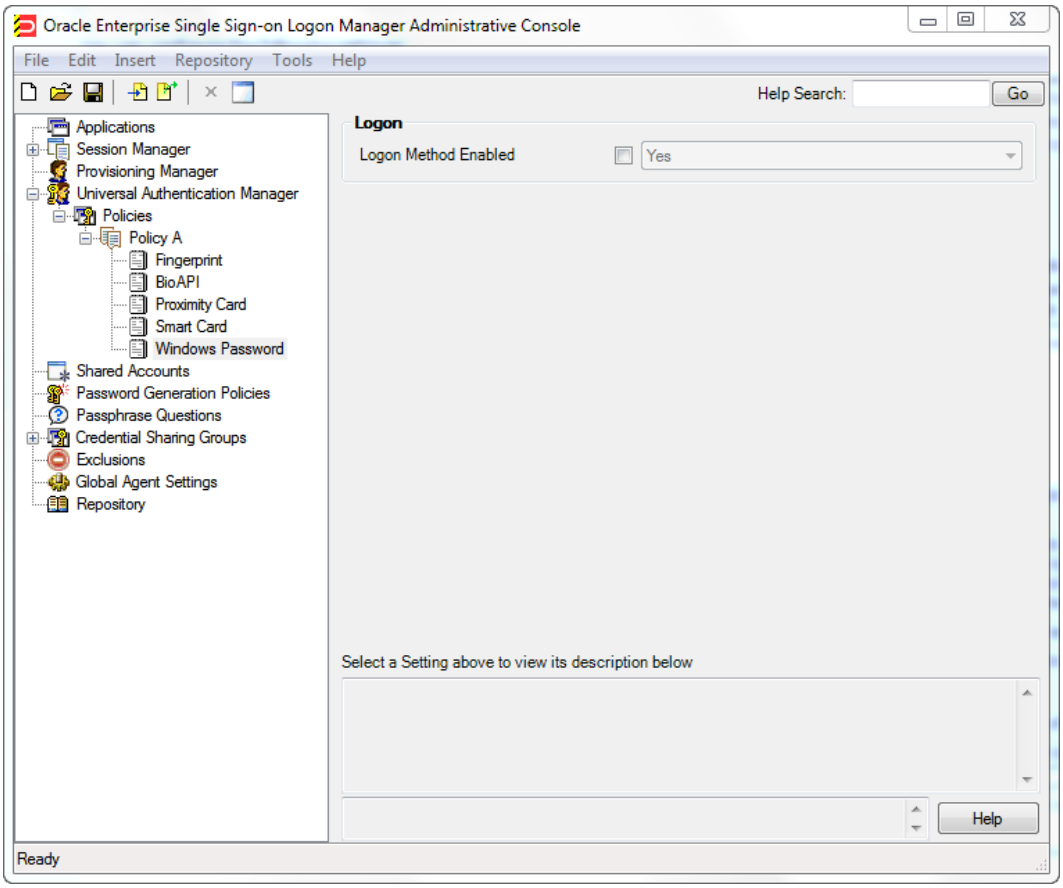
You can configure the following settings:

Logon Method Enabled	Allows administrators to enable or disable an installed authenticator on an ESSO-UAM Client. This policy setting enhances security by controlling the specific logon methods that end-users are allowed to use. **Options:** • Yes (default) • No If you select **No**, the end-user is not allowed to log on to or enroll on the workstation using this logon method. If users attempt to log on with a disabled logon method, they will receive an error message.
Removal Action	Controls how the computer responds when the smart card is removed from a card reader. Removal Action is only enforced when the corresponding logon method was the last method used to log on to or unlock the computer. **Options:** • No Action

	• Lock Workstation (default) • Force Logoff
Enrollment Prompt	Controls whether a user is prompted to enroll and whether enrollment is optional or required. **Options:** • Never • Optional (default) • Required
Grace Period	Allows end-users to defer a required enrollment for a configured number of days (the grace period). Allows administrators to require enrollment with a desired logon method without immediately restricting end-users' access to workstations. Administrators can configure a suitable number of days in which an end-user will be allowed to defer enrollment. The Enrollment Grace Period is disabled if any of the following conditions are met: • The **Enrollment Prompt** policy setting is NOT configured to "Required." • This setting is configured to zero. Default is 0. Maximum grace period is 365 days.
PIN Required	Controls if a user is challenged to submit the smart card's PIN when the card is used to authenticate. **Options:** • Yes (default) • No

Windows Password Settings

When you select **Windows Password** for a chosen policy, the page that opens displays a Windows Password setting for you to edit. The setting will be disabled by default and set to a default; to change the setting, select the check box next to it and configure a value.



Logon Method Enabled	Allows administrators to enable or disable an installed authenticator on an ESSO-UAM Client. This policy setting enhances security by controlling the specific logon methods that end-users are allowed to use. **Options:** • Yes (default) • No If you select **No**, the end-user is not allowed to log on to or enroll on the workstation using this logon method. If users attempt to log on with a disabled logon method, they will receive an error message.

If you disable Windows Password and a user is not enrolled in any other methods, the password is still allowed until a user enrolls in at least one ESSO-UAM method.

General Tab (for a Selected Policy)

From the General tab for a selected policy, you can review how many settings have been configured for the Logon Methods for that policy. Specifically, this tab displays the following information:

- **Path:** The name of each Logon Method that makes up a group of related settings.
- **Set:** The number of settings that have been configured.
- **Total:** The total number of settings per Logon Method
- **Add Notes:** Launches the "Notes" dialog box should you want to make any notes about this policy.

After settings are configured, re-selecting the policy in the left pane will display a summary of settings on the General tab that were changed. The text in the columns changes its color to highlight where changes were made to the policy.

Security Tab (for a Selected Policy)

From the Security tab for a selected policy, you can configure the users or user groups who can view and modify policies using the ESSO-LM Administrative Console. You should not need to modify any of the security settings.

If the ESSO-UAM Service Account can read the policy object, it will be an active policy. If not, it will be ignored. See the *ESSO-UAM Installation Guide* for more information on the ESSO-UAM Service Account.

For more information on this tab, refer to the *ESSO-LM Administrative Console* help.

Publishing an ESSO-UAM Policy

The procedure for publishing an ESSO-UAM policy is similar to that for publishing ESSO-LM objects.

ESSO-UAM policies can be applied to Active Directory users or user groups. Before you can publish a policy to apply to a user or group, ensure the user or user group exists, or create a new user or user group. Then you must create a new ESSO-UAM storage container for that user or user group under the ESSO-UAM Policies container in the repository. After you have created a new ESSO-UAM policy and configured its settings, you can publish it by connecting to the repository.

If you are going to create a new Active Directory user group, keep the following in mind:

- User groups should be in the same domain.
- User groups should be Security groups, not Distribution groups.

Policies must contain at least one setting; that is, you cannot publish an empty policy.

See the *ESSO-UAM Installation Guide* for instructions on how to prepare the repository for policy synchronization.

Publishing a Policy

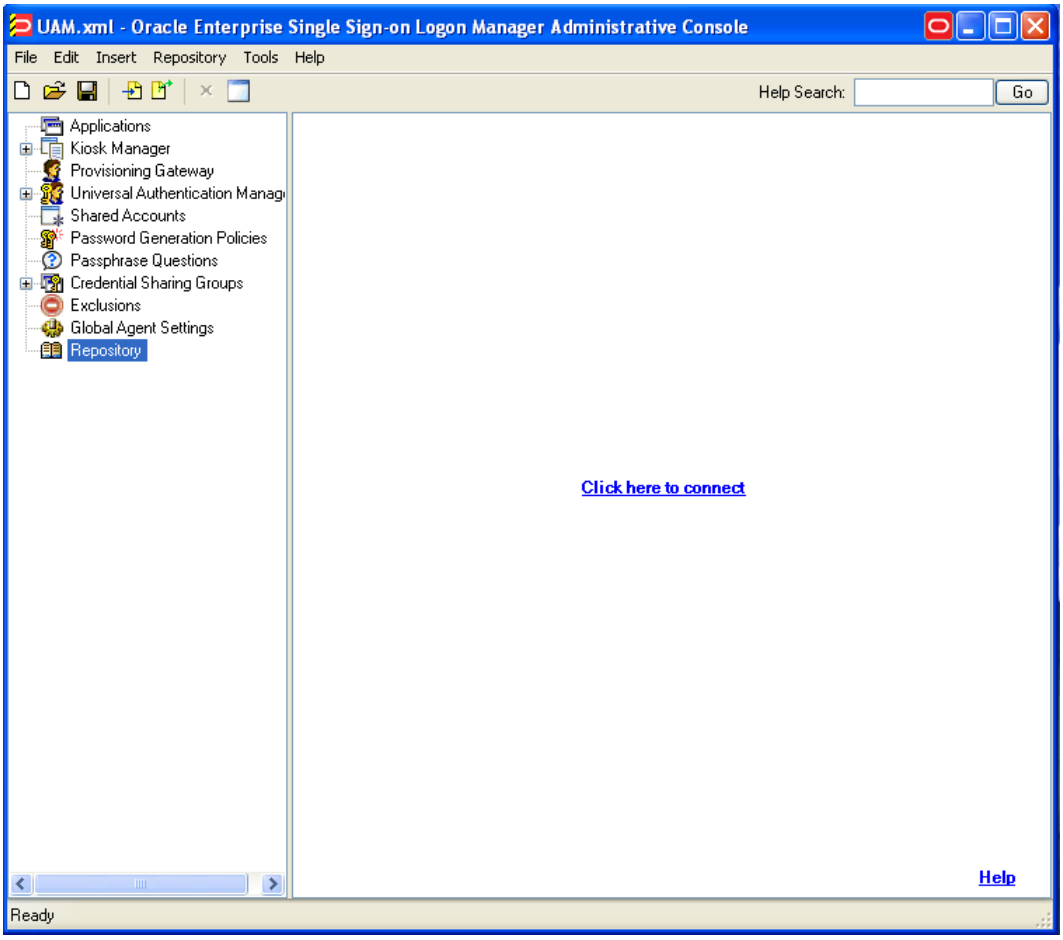
After you have created a new ESSO-UAM policy and configured its settings, you can publish it by connecting to the repository.

If you will be publishing a policy to the Domain Users group, use the Domain Users ESSO-UAM Storage container created by the ESSO-UAM initialize storage. The Console allows each policy to be published to multiple repository user groups and/or users; however, only one policy may be applied to each user or user group. Oracle recommends the following:

- Only publish a policy set to the Domain Users Security Group if you want to apply a global policy to all users.
- Create repository groups for use with ESSO-UAM.
- Add users to exactly one group. You must ensure that each user is only configured to receive at most one policy set from a group, otherwise the results are non-deterministic.

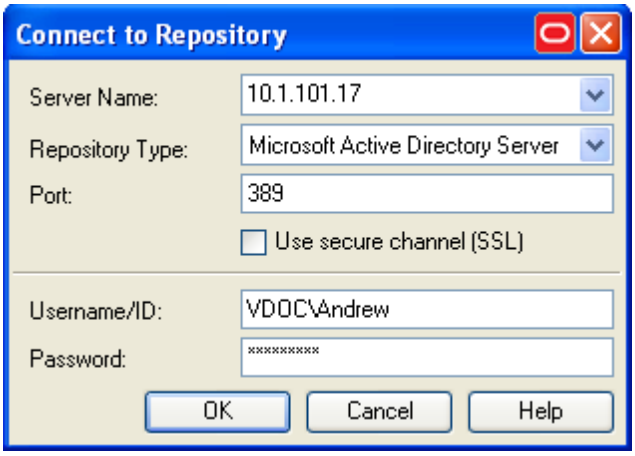
Connecting to the Repository

1. With **Repository** selected in the left-hand navigation pane, select **Click here to connect**.



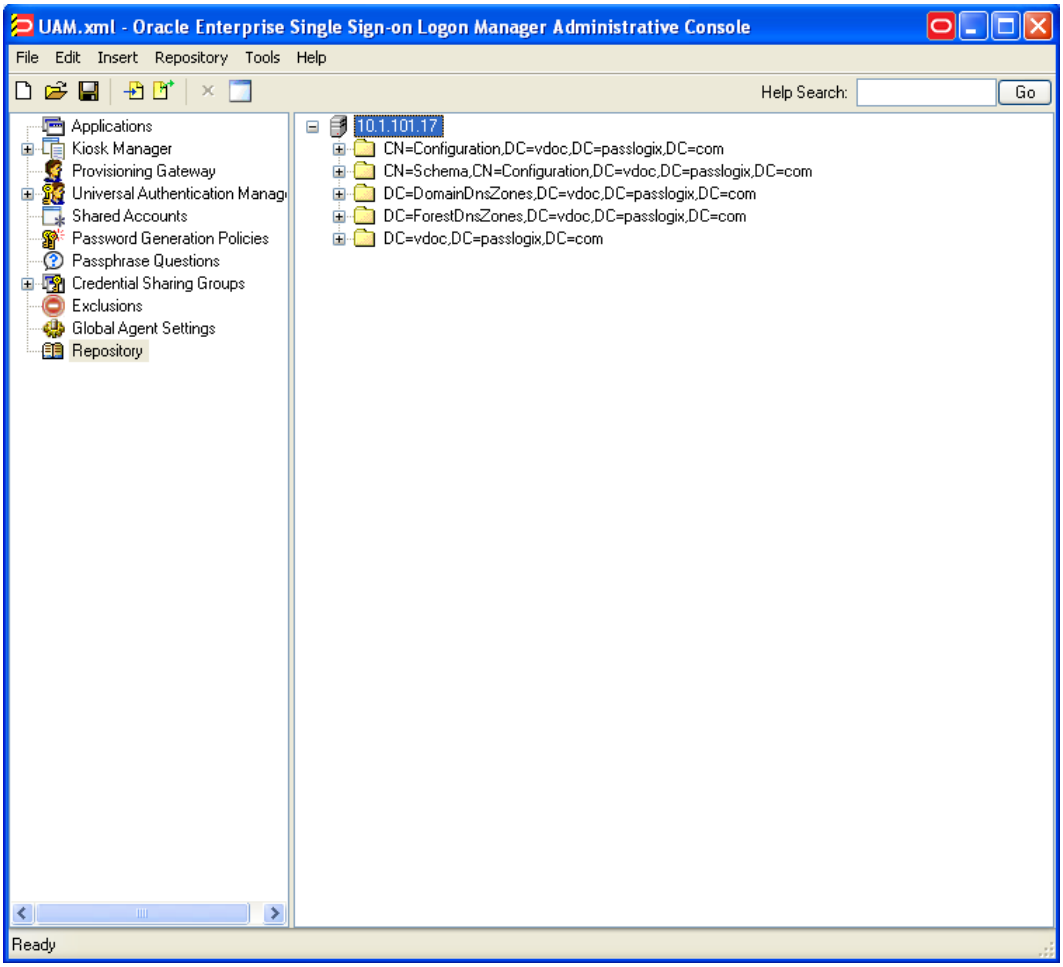
2. In the Connect to Repository dialog box, enter a **Server Name** (for this example, the name is DC01), select **Microsoft Active Directory Server** or **Microsoft ADAM** from the drop-down menu, **Port** , and the **Username/ID** and **Password** of an administrative account with the appropriate administrative permissions. Refer to the *ESSO-UAM Installation Guide* for

information on the necessary permissions. Click **OK** when finished.

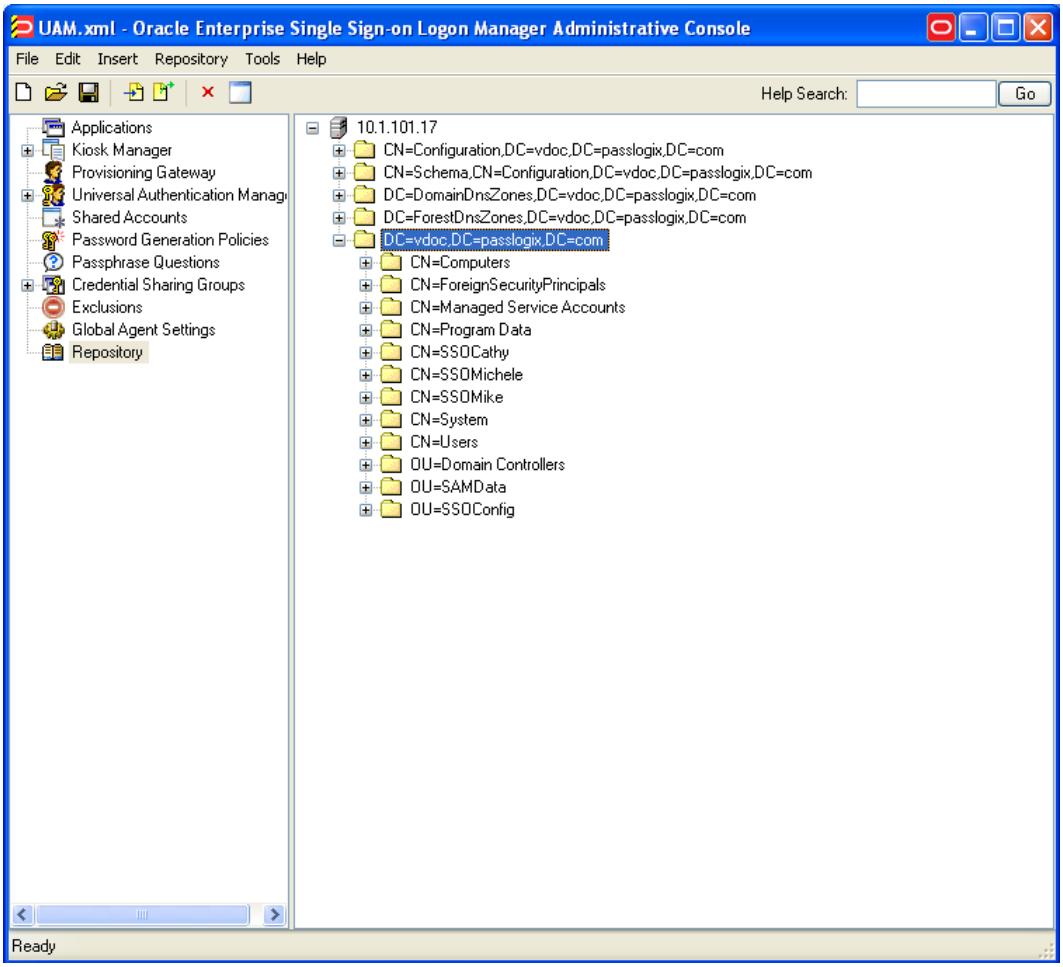


Create a New ESSO-UAM Policies Container

1. From the right-hand pane, select the name of the server you created to expand its tree.



2. Expand the root domain container.



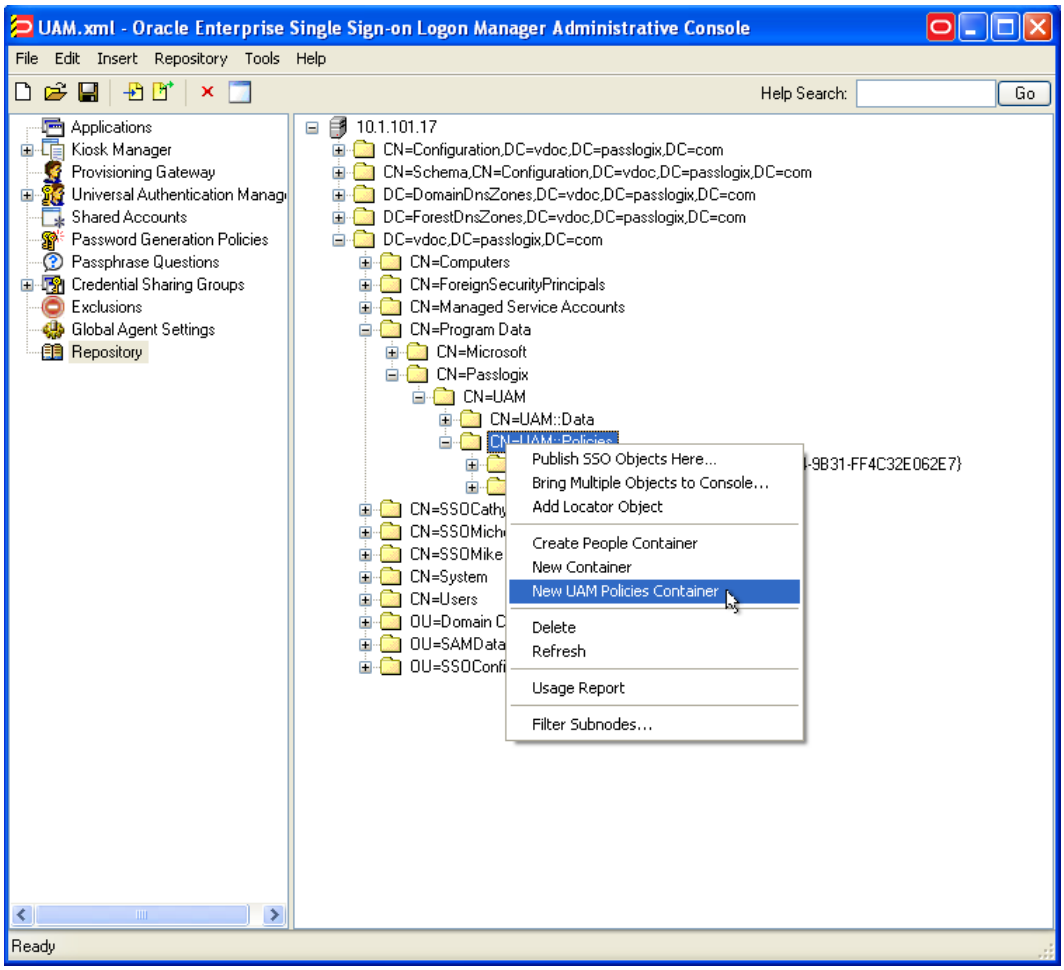
3. In this directory, create a container that represents the User or User Group to which you want to publish a policy.

   a. Open **CN=Program Data**>**CN=Passlogix**>**CN=UAM**>**CN=UAM::Policies**.

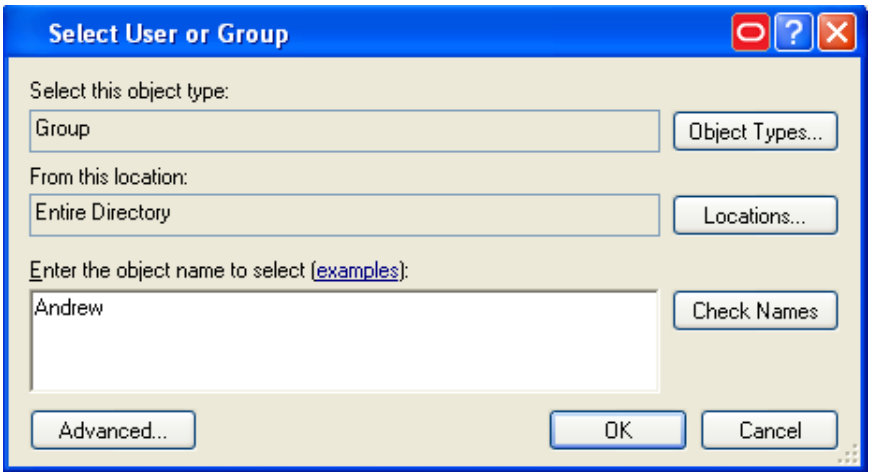
> These containers are created under CN=Program Data when you execute "Initialize UAM Storage" during deployment. Refer to the *ESSO-UAM Installation Guide* for more information on initializing storage for ESSO-UAM.

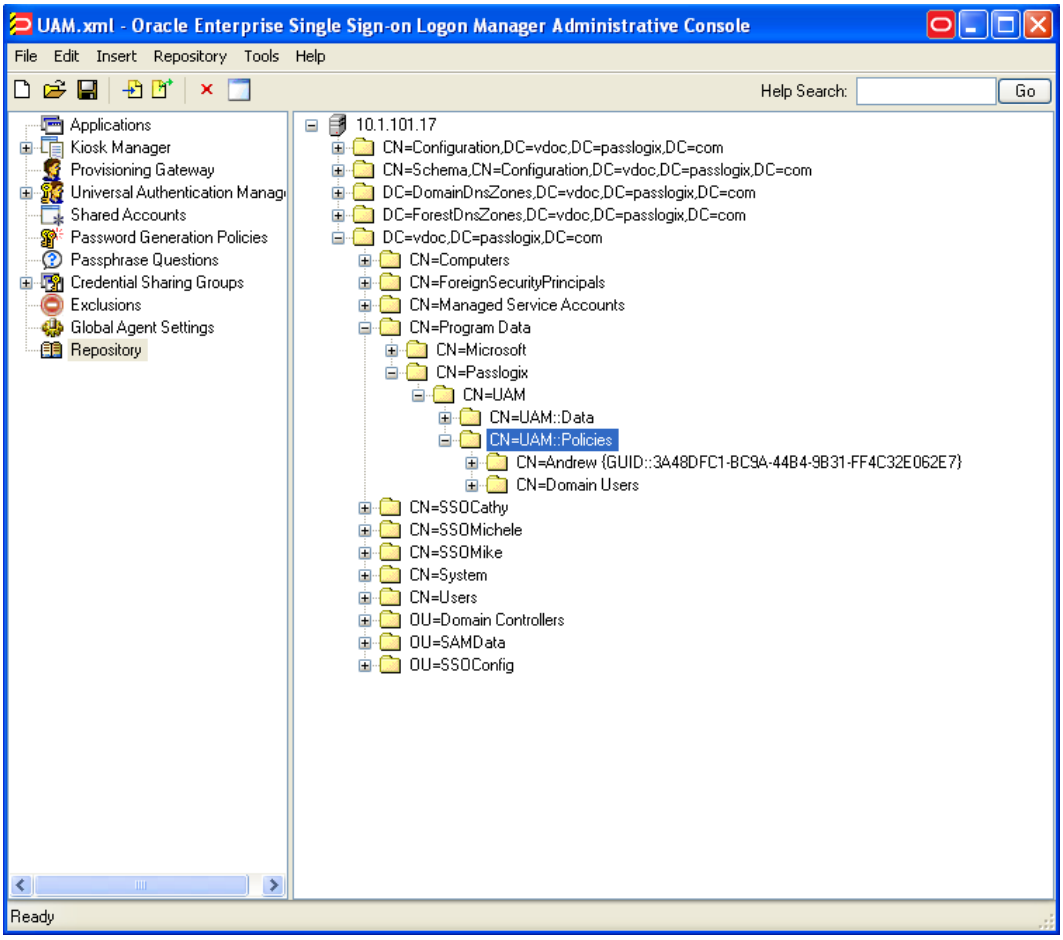
b. Right-click **CN=UAM::Policies** and select **New UAM Policies Container**.

> If you are publishing a policy for a User Group, specify the name of the Active Directory User Group to which you want to apply the policy. Click **OK** to create the container.
>
> If you are publishing a policy for a User, click **Object Types...** in the "Select User or Group" dialog box. In the "Object Types" dialog box, select the **Users** checkbox, and click **OK**. Specify the name of the Active Directory User to which you want to apply the policy. Click **OK** to create the container.



4. In the Select User or Group dialog box, type the first few characters of the group or user name and click **Check Names**. The system retrieves the name of the group. Select the group and click **OK**.



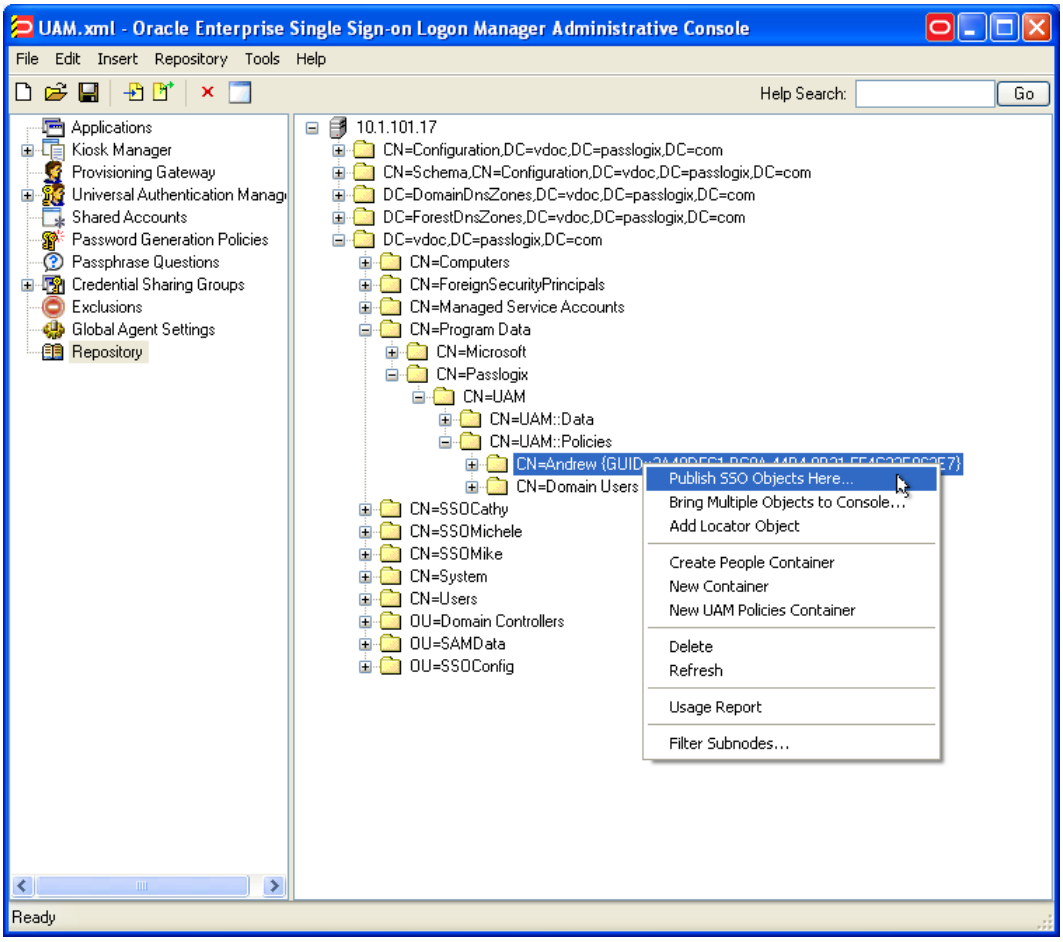


5. The container is added under the Policies container.

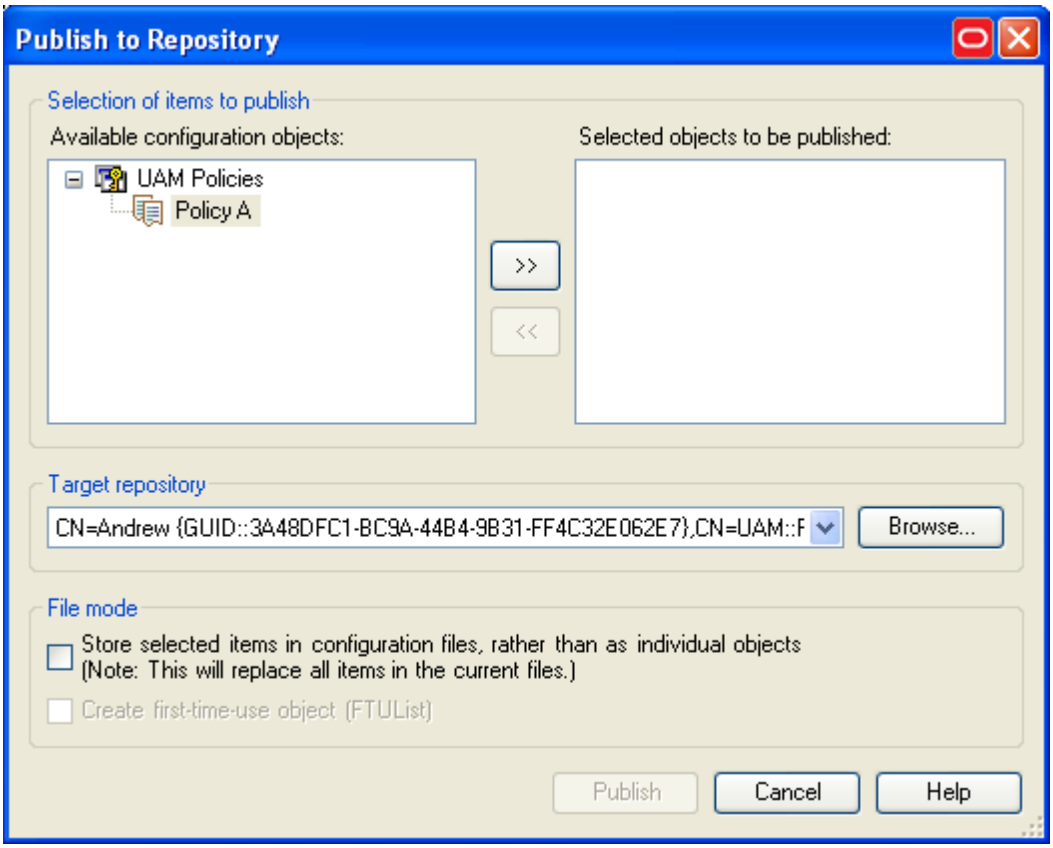
Publishing a Policy to the New User or Group

You can publish an ESSO-UAM policy to the container that represents the User or User Group by selecting a **Publish** option in the Administrative Console.

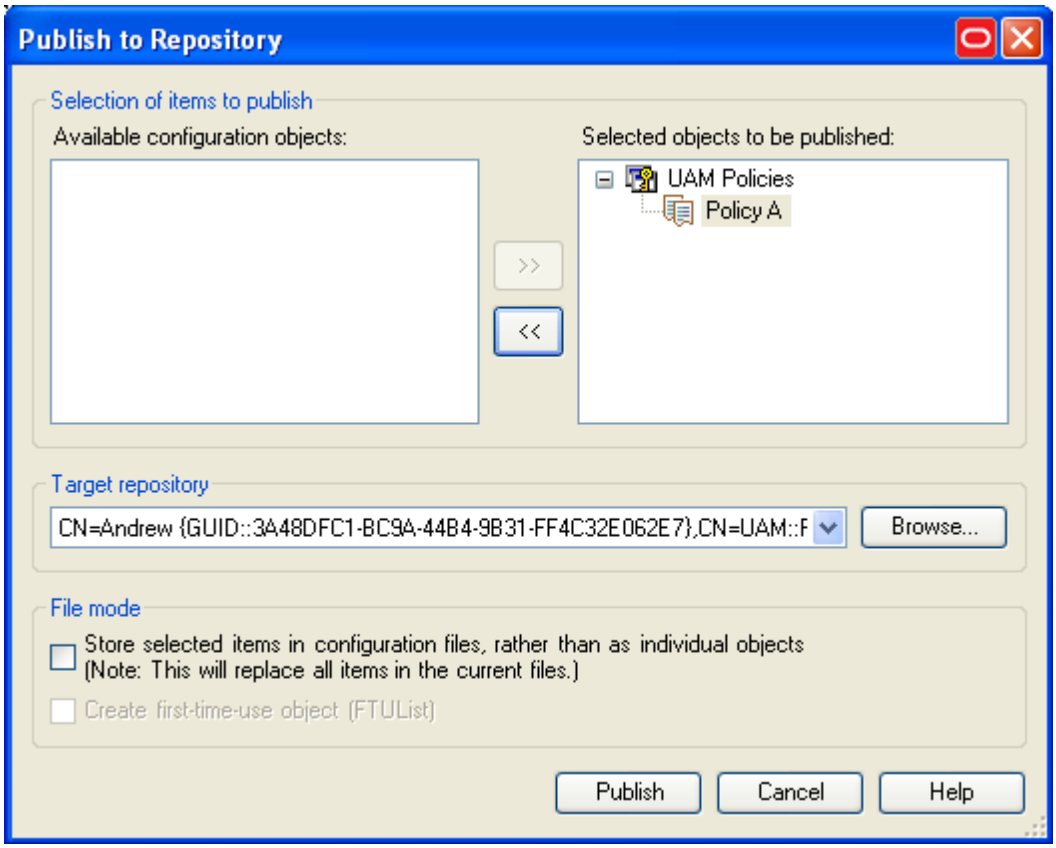
1. Right-click the new container and select **Publish SSO Objects Here...**



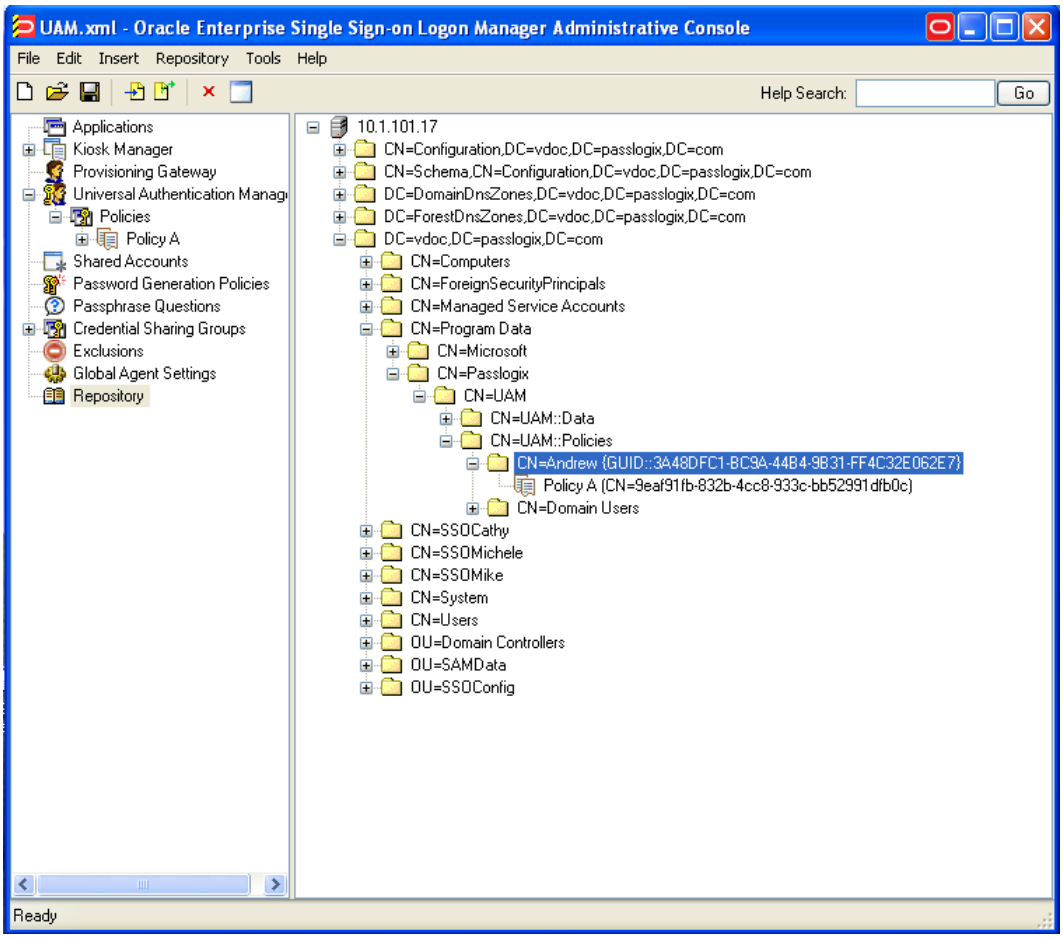
2. In the Publish to Repository dialog, in the Available configuration objects list box, expand the **Universal Authentication Manager** menu, and select the policy to publish. Click the **>>** button.



3. The policy moves to the Selected objects to be published list box. Click the **Publish** button.

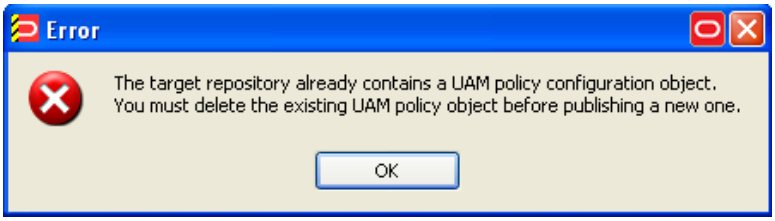


4. The policy appears in the ESSO-UAM Policies container.


UAM.xml - Oracle Enterprise Single Sign-on Logon Manager Administrative Console
File Edit Insert Repository Tools Help
Help Search: Go
Applications
Kiosk Manager
Provisioning Gateway
Universal Authentication Manag
Policies
Policy A
Shared Accounts
Password Generation Policies
Passphrase Questions
Credential Sharing Groups
Exclusions
Global Agent Settings
Repository
10.1.101.17
CN=Configuration,DC=vdoc,DC=passlogix,DC=com
CN=Schema,CN=Configuration,DC=vdoc,DC=passlogix,DC=com
DC=DomainDnsZones,DC=vdoc,DC=passlogix,DC=com
DC=ForestDnsZones,DC=vdoc,DC=passlogix,DC=com
DC=vdoc,DC=passlogix,DC=com
CN=Computers
CN=ForeignSecurityPrincipals
CN=Managed Service Accounts
CN=Program Data
CN=Microsoft
CN=Passlogix
CN=UAM
CN=UAM::Data
CN=UAM::Policies
CN=Andrew {GUID::3A48DFC1-BC9A-44B4-9B31-FF4C32E062E7}
Policy A (CN=9eaf91fb-832b-4cc8-933c-bb52991dfb0c)
CN=Domain Users
CN=SSOCathy
CN=SSOMichele
CN=SSOMike
CN=System
CN=Users
OU=Domain Controllers
OU=SAMData
OU=SSOConfig
Ready

Modifying an ESSO-UAM Policy

ESSO-UAM will not allow you to publish more than one policy per user and user group. If you try to overwrite an existing policy with a new (modified) version of the same policy, you will receive an error message.

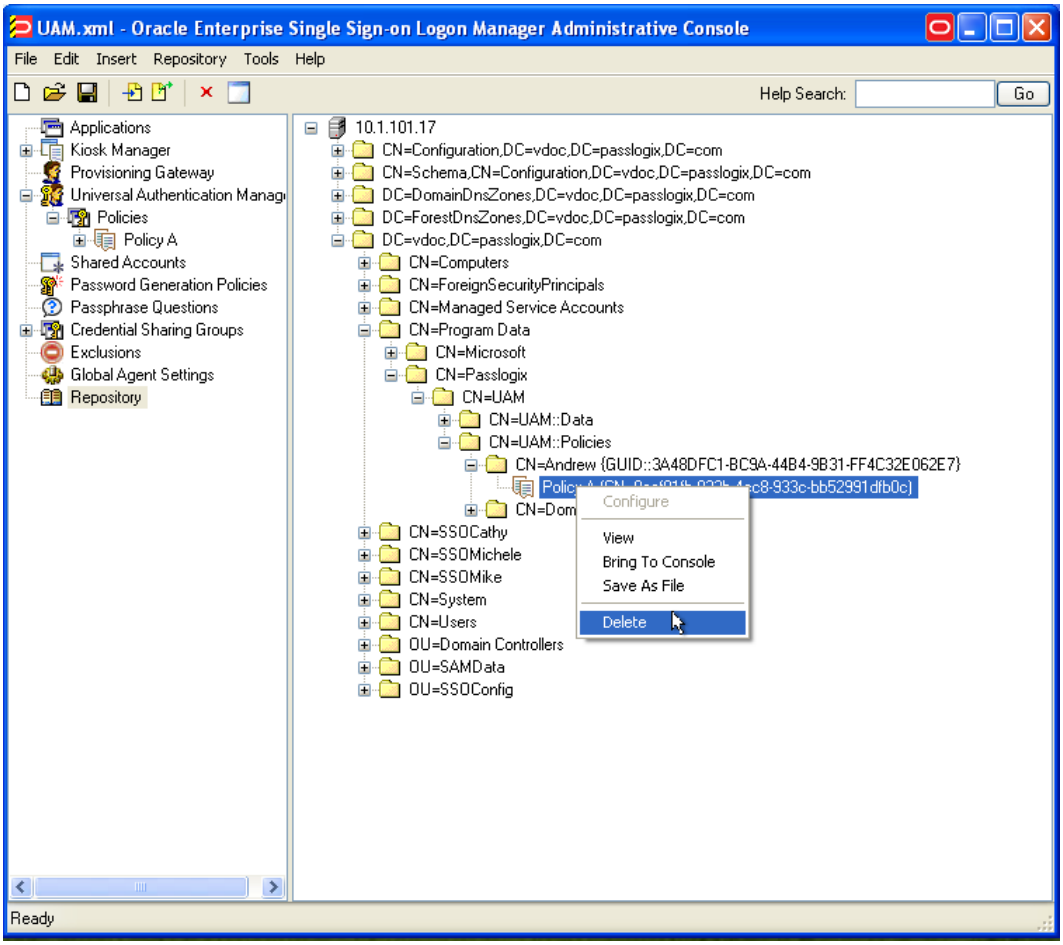


Therefore, if at any time you wish to modify a policy that has already been published, you must delete the existing policy from the repository and re-publish the version that you modified.

1. Select the policy in the left pane of the Console and make changes to the policy settings as necessary.

> If the policy does not appear in the left pane of the Console, you can locate it in the repository and bring it to your local workspace in the Console. See the instructions in the following section, Copying and Modifying a Policy from the Repository.

2. Locate the policy in the repository. Right-click the policy and select **Delete** from the pop-up menu.

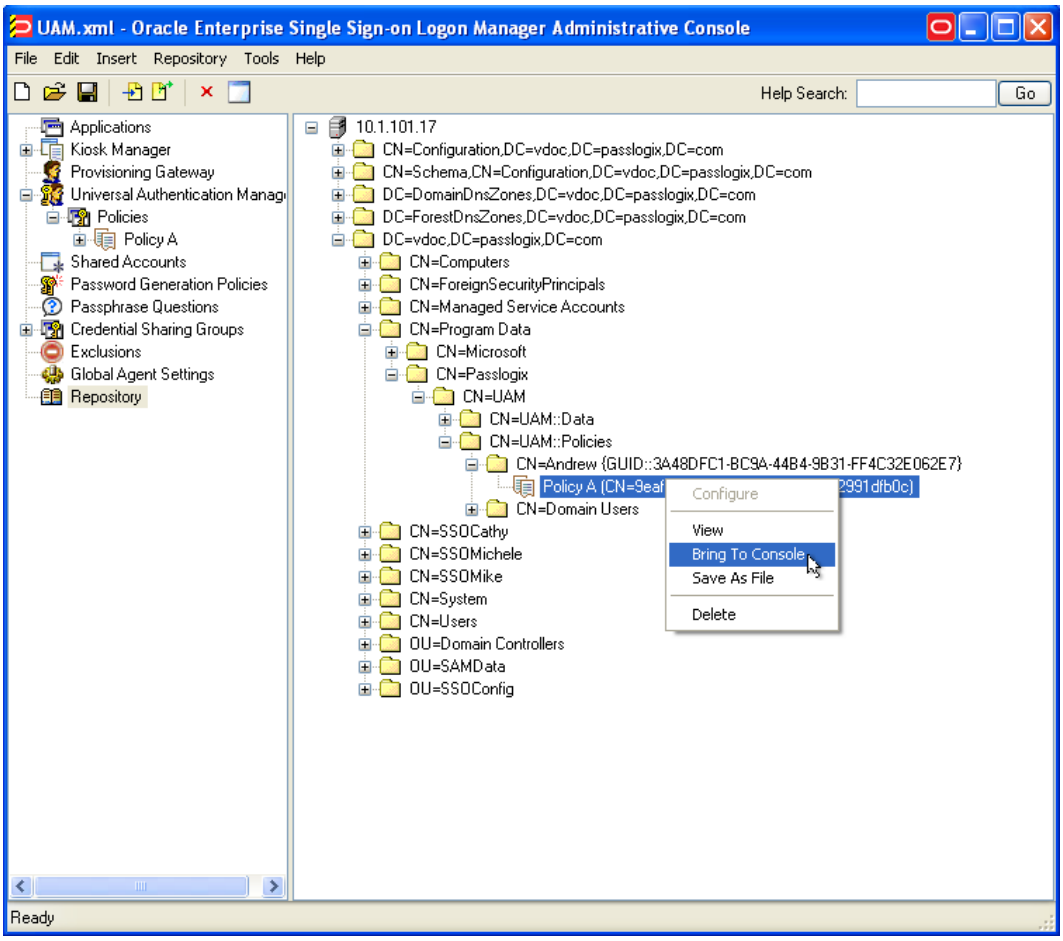


3. Re-publish the policy from your local workspace to the Console as described in Publishing an ESSO-UAM Policy.

Copying and Modifying a Policy from the Repository

If the policy you wish to modify exists in the repository, but does not exist in the left pane of the Console in your local workspace, you can copy it from the repository to your local workspace and edit it locally. Then you can delete the existing policy from the repository and re-publish the version of it that you edited.

1. Locate the policy in the repository.
2. Right click the policy and select **Bring to Console** from the pop-up menu. A copy of the policy appears in your local workspace.



3. Make the necessary changes to the copy of the policy in your local workspace.
4. Locate the policy in the repository. Right-click the policy and select **Delete** from the pop-up menu.
5. Re-publish the policy from your local workspace to the Console as described in Publishing an ESSO-UAM Policy.

Compatibility with Windows Default Domain Policies

Windows default domain policies are enforced by ESSO-UAM. ESSO-UAM extends your system's native Windows logon behavior. Microsoft Windows and Active Directory include numerous security policies and settings that affect the Windows log on and unlock flows; ESSO-UAM conforms to these policies. For example, if a user's password reaches the maximum password age, ESSO-UAM still requires the user to change the password before logon is allowed.

AutoLogon Behavior

ESSO-UAM supports AutoLogon. For information on how to configure AutoLogon on a Windows XP workstation, visit Microsoft Support:

http://support.microsoft.com/?kbid=315231

Windows Password Logon and Unlock

The ESSO-UAM Windows XP logon replicates all native Windows XP password logon and unlock flows.

Windows Password Logon and Unlock Errors

The ESSO-UAM logon component conforms with Windows password authentication error scenarios and duplicates the flows of the Windows XP GINA. For example, if the user types an invalid password, the error flow is identical and the user receives the same error messages as with Windows XP.

Microsoft Active Directory Security Policies

The ESSO-UAM Client encompasses the Windows XP logon GINA and extends its capabilities. Microsoft Windows and Active Directory include numerous security policies and settings that affect the Windows log on and unlock flows. Once installed, the ESSO-UAM Client conforms with all Microsoft Active Directory security policies.

Ensure that security policies are not set to require smart cards for logon.

Active Directory Password Policies

This group of policies is used to manage Active Directory password constraints and password aging, and drives the logic behind password change prompts and expiration. For example, if a user's password reaches the maximum password age as configured in Active Directory, the ESSO-UAM GINA requires the user to change the password before permitting a logon.

ESSO-UAM Authentication Methods and Lockout

ESSO-UAM supports managing the number of invalid logon attempts that will cause a user's account to be temporarily or permanently disabled. If these policies are enabled to enforce account lockout, the ESSO-UAM GINA tracks and increments failed logon and unlock attempts for all supported methods and locks out accounts that exceed the account lockout threshold.

Changing User Passwords as the Administrator

If, as an administrator, you change a user's password, and the user then tries to log in with an ESSO-UAM credential, an Incorrect Cached Password error dialog will be presented to the user. The user will be required to type in the new password; ensure that you have informed the user of the new password.

The incorrect cached password will count as one failed logon attempt, and may trigger the Windows account lockout threshold, depending on how your Windows password policies are configured.

Authenticator Preferred Display Order

This feature provides the ability to set the order in which logon methods are displayed in the user interface screens throughout ESSO-UAM. This must be manually set up in the registry.

If you make changes to these keys, and later uninstall and reinstall or run an installation repair, you will have to manually reconfigure the authenticator preferred display order settings.

Open the Windows registry and navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix\UAM\Authenticators\{authID}:"Order" = DWORD`

(where `authID` refers to the logon method identifier).

Any numeric decimal value can be used. Methods appear in the user interface from left to right and from smaller to larger order.

The following is the default order installed by ESSO-UAM:

Fingerprint

```
HKEY_LOCAL_MACHINE\Software\Passlogix\UAM\Authenticators\{16627EE1-FAE3-43B5-B884-D3661649B97D}

Order REG_DWORD 100
```

BioAPI

```
HKEY_LOCAL_MACHINE\Software\Passlogix\UAM\Authenticators\{17875AD3-D203-4F07-BF48-78876545AF4C}

Order REG_DWORD 110
```

Proximity Card

```
HKEY_LOCAL_MACHINE\Software\Passlogix\UAM\Authenticators\{4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}

Order REG_DWORD 500
```

Smart Card

```
HKEY_LOCAL_MACHINE\Software\Passlogix\UAM\Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}

Order REG_DWORD 600
```

Windows Password

```
HKEY_LOCAL_MACHINE\Software\Passlogix\UAM\Authenticators\{0C29417D-8A20-48B7-8CC4-D948D384E9B2}

Order REG_DWORD 999
```

If the `Order` key does not exist, the default is 800.

Troubleshooting

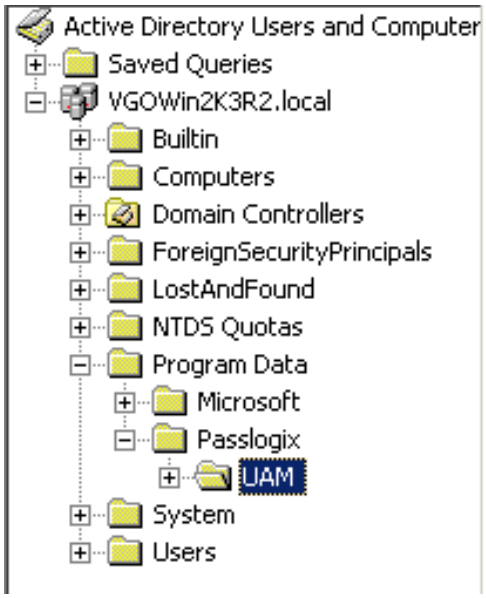
This section describes solutions to issues you may encounter when working with ESSO-UAM.

Recovery from Deletion of the Service Account

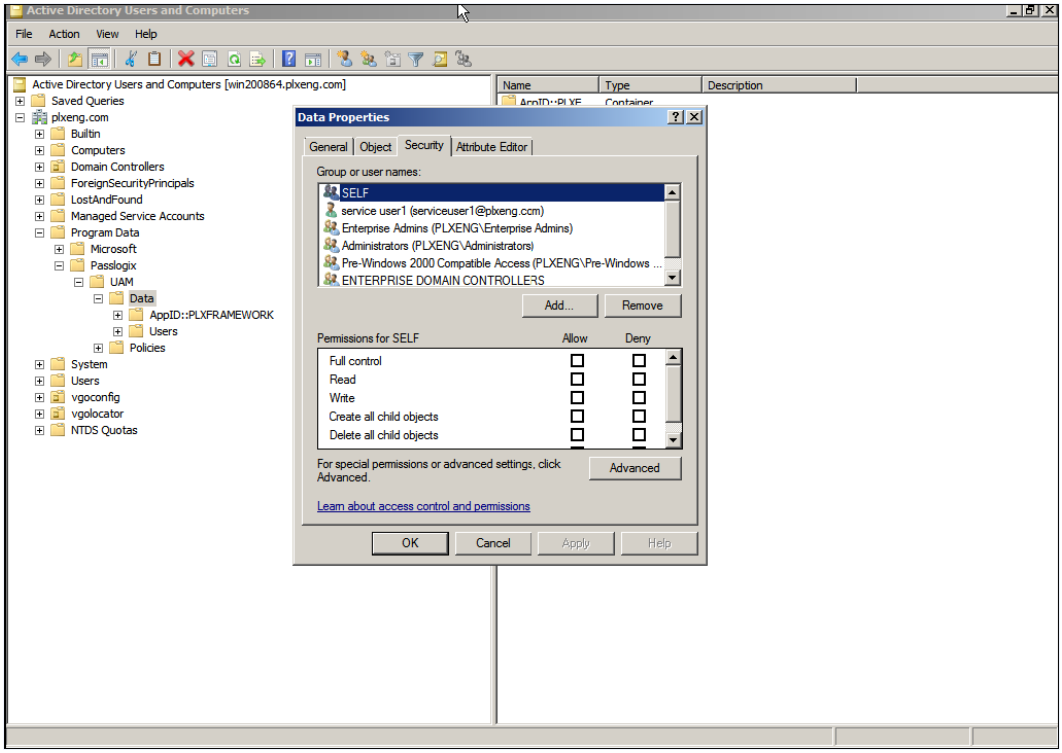
The ESSO-UAM Service Account is used by all ESSO-UAM Clients to securely access the repository to read and write data. If the Service Account is deleted or disabled, all clients will fail to synchronize to the repository and users may not be able to log on because the ESSO-UAM Service won't be able to start when the computer is restarted. If you cannot log on to perform the manual configuration steps, you will have to log on in Windows safe mode. It is important to ensure that this account is protected.

To prevent the ESSO-UAM Service Account from being compromised, set the password to never expire, use a strong password, and be sure no one deletes or changes it. If for some reason the Service Account is deleted or changed, use one of the following procedures to recover your system.

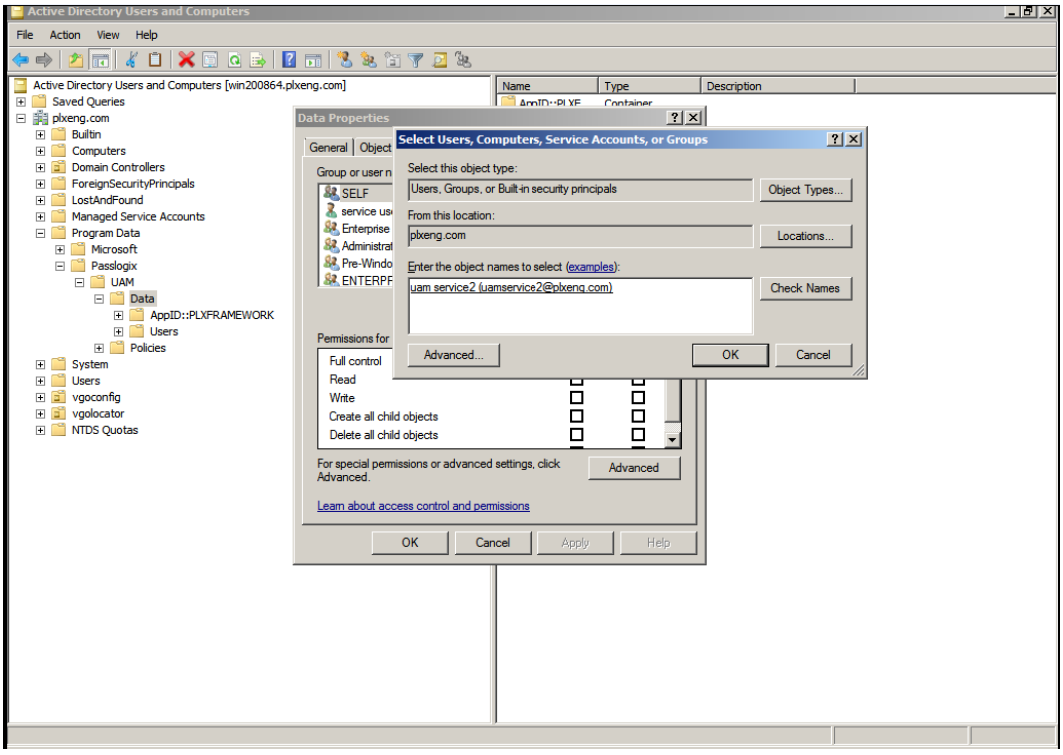
1. On your Windows server, Navigate to **Active Directory Users and Computers**.
2. On the View menu, ensure that **Advanced Features** is checked.
3. Create a new ESSO-UAM Service Account with a different name from that of the deleted one. For example, instead of "uamservice," use "uamservice2."
4. Expand **Program Data\Passlogix**.



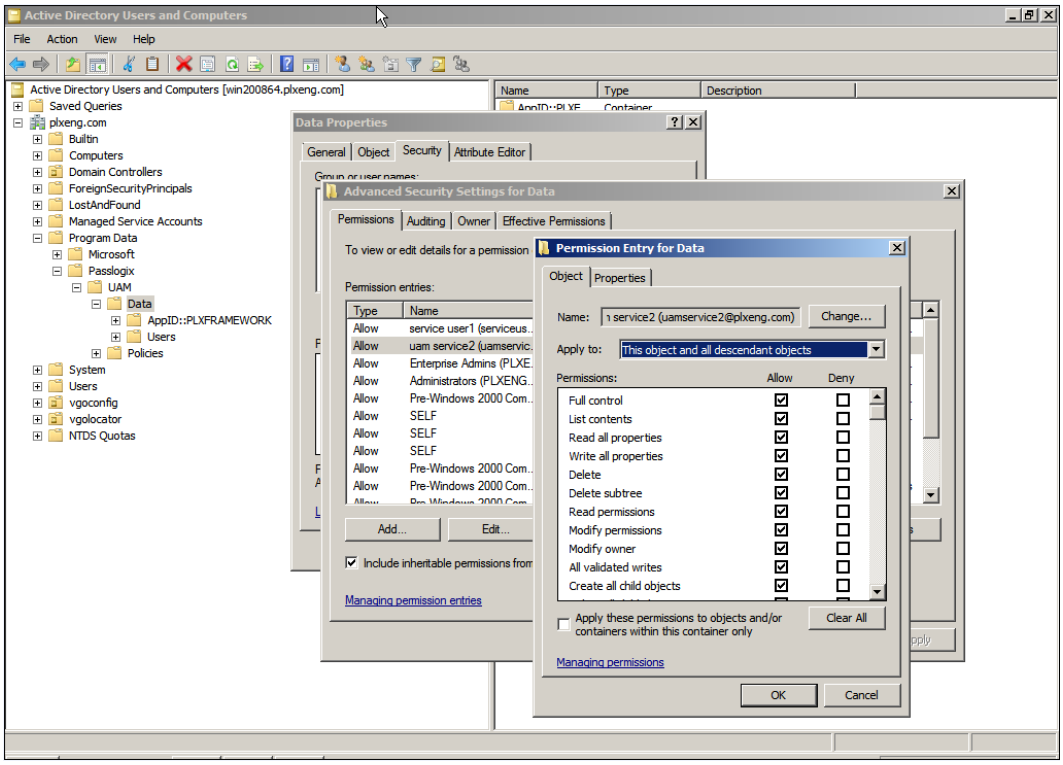
5. Right-click **UAM**.
6. Click the **Security** tab.



7. Click **Add**.
8. Choose the newly-created ESSO-UAM Service Account, and click **OK**.



9. Select the new account and check **Allow/Full Control**.
10. Click **Advanced**.
11. Choose your new Service Account and click **Edit**.
12. On both the Object and Properties tabs, verify that the Service Account has Full Control (full permissions).
13. On both the Object and Properties tabs, set the **Apply To** field to **This object and all descendant objects**.



14. Click **OK** three times to complete the process.
15. Reconfigure the Service Account, pointing to the new Service Account. See the *ESSO-UAM Installation Guide* for information on performing this procedure.

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. 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 - Add/Remove Programs.

4. Change the **Log On As** value back to the ESSO-UAM Service Account user. From the Control Panel, launch Administrative Tools. Under Services, right-click the UAM Authentication Service and click **Properties**. On the Log On tab, change the **Log On As** value from the local system account to the ESSO-UAM Service Account user.
5. Restart the UAM Authentication Service. From the Control Panel, launch Administrative Tools. Under Services, right-click the UAM Authentication Service and click **Start**.

AutoLogon Condition is Incorrectly Configured

If the AutoLogon condition is enabled but incorrectly configured, users logging on will see the Microsoft Logon dialog box instead of the ESSO-UAM GINA. If the user then logs on to the workstation with a Windows password, he will not be prompted to enroll any logon methods. The user sees no PIN prompt or error message. However, users will see the ESSO-UAM logon dialog when unlocking the workstation, since AutoLogon pertains only to logon behavior, but not to unlocking a workstation. Users may see the Microsoft Logon dialog box when they log off if ForceAutoLogon is not enforced.

For information on how to configure AutoLogon on a Windows XP workstation, visit Microsoft Support:

http://support.microsoft.com/?kbid=315231

Avoid Using Dual Purpose Cards with Dual Purpose Readers

A dual-purpose card is a card that can act as both a smart card and a proximity card. A dual-purpose reader is a reader than can recognize both smart cards and proximity cards. Oracle does not recommend using dual-purpose cards together with dual-purpose readers, as the card will be simultaneously recognized by ESSO-UAM as both a smart card and a proximity card. In this case, ESSO-UAM will not be able to determine which technology the user intends to use for enrollment. For example, if you use a dual-purpose device--such as a smart card that contains a proximity chip--with a dual purpose reader, the proximity function of the reader will read the proximity element of the card before you can fully insert the card into the reader for the smart card functionality. A better practice is to use a dual-purpose card with a single-purpose reader, or a single-purpose card with a dual-purpose reader.

Configuring Your System with Settings and Registry Keys

You can configure ESSO-UAM using a variety of tools to edit registry values.

Managing Settings Configured in Multiple Locations

It is important to be aware of how policies and settings interact with each other (if you set values for the same settings in more than one location). Some settings will always overwrite others. The following is a high-level description for the different types of settings:

- Administrative settings indicate that the setting was configured in the registry of a an end-user workstation.
- Administrative per-user settings indicate that the setting was configured in the registry and applies to a particular user.
- Administrative per-computer indicates that a setting was configured in the registry that applies to all users on a computer.

In Local Mode:

Administrative per-user settings take precedence over any administrative per-computer settings. However, administrative settings, either per-user or per-computer, always take precedence over user settings (those that are configured through the Client Application).

There are no roaming policies in local mode.

In Enterprise Mode:

Roaming policies (those that are configured from the Administrative Console) take precedence over any administrative per-computer settings. Administrative per-computer settings take precedence over any enterprise user settings (those that are configured through the Client Application).

Administrative per-user settings are ignored in enterprise mode.

Global Client Settings

These are general ESSO-UAM application configuration settings that control the behavior of various ESSO-UAM features. Most settings of this type apply to all users on a particular computer. These settings should not need to be modified in most cases.

Target	Category	Type	Name	Values	Description	Path
Framework	General	DWORD	ClientMode	Enterprise Client Mode (1) (default) or Local Client Mode (0)	Client Mode may be set to Local or Enterprise during install.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM
Framework	Logging	DWORD	SimpleLoggerOn	Yes (1) or No (0) (default)	Turn debug logging on or off.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix
Framework	Logging	DWORD	SimpleLoggerLevel	Fatal Errors Only (1), Business Logic Errors (2), Warnings - Recoverable Error Conditions (3), Informational - Business Logic Flow (4) (default), Debug - Extra Debugging Information (5), Verbose - Maximum Debugging Information (6)	Maximum logging verbosity. Each level includes all preceding levels of a lesser numeric value.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix
Framework	Logging	SZ	SimpleLoggerPath	default is c:\uamlog.txt	Specify debug log path and filename.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix
Framework	Logging	SZ	SimpleLogger ProcShow	N/A	Regular expression to only show matching log entries by process name. Default is to show all entries.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix
Framework	Logging	SZ	SimpleLogger ProcHide	N/A	Regular expression to hide matching log entries by process name. Default is to show all entries.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix
Framework	Logging	SZ	SimpleLogger FileShow	N/A	Regular expression to only show matching log entries by source filename. Default is to show all entries.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix
Framework	Logging	SZ	SimpleLogger FileHide	N/A		HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix
Framework	Communication	DWORD	IpcTimeout	Default is 5000 ms Allowed range is 1-60000 ms	Controls the communication timeouts between ESSO-UAM Client Applications and the ESSO-UAM auth service. It is unlikely this will ever need to be modified, but it is possible that on extremely slow computers, it may need to be increased in order for Client Applications to function.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM
Framework	Communication	DWORD	IpcRetries	Default is 3 retries Allowed range is 0-10 retries	Service connect retries. It is unlikely this will ever need to be modified, but it is possible that on extremely slow computers, it may need to be increased in order for Client Applications to function.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM

Target	Category	Type	Name	Values	Description	Path
Framework	User Resolution	DWORD	UserIDCacheSize	Default is 5 users Allowed range is 1-2147483646 users	Number of user identities to cache in the disconnected MRU. Also used during synchronization.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM
Framework	User Resolution	DWORD	UserResolve Timeout1	Default is 1000 ms Allowed range is 1-2147483646 ms	How long to wait for live resolution before falling back to cache.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM
Framework	User Resolution	DWORD	UserResolve Timeout2	Default is 5000 ms Allowed range is 1-2147483646 ms	Additional time to wait for live results when cache is empty.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM
Framework	Enrollment	DWORD	PromptToken Description	Prompt User for Description (1) or Do Not Prompt User for Description (0) (default)	Ask user to enter a token description during enrollment. If not prompted, the default description is automatically used.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM
Framework	Enrollment	SZ	DefaultToken Description	N/A	Default description to associate with each token. Used only if specific authenticator has no default description.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM
Framework	Enrollment	SZ	DefaultToken Description-{4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}	N/A	Default description for each proximity card.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM
Framework	Enrollment	SZ	DefaultToken Description-{A1B34553-8D40-42A9-8ED5-F70E3497E138}	N/A	Default description for each smart card.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM
Framework	Reauthentication	DWORD	MaxAuthAttempts	Default is 3 attempts Allowed range is 1-2147483646 attempts	Number of consecutive credential capture attempts allowed during reauthentication. Note: Windows Password always has unlimited attempts.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM
Framework	Reauthentication	SZ	Default Authenticator	None (default), Fingerprint, BioAPI, Proximity Card, Smart Card, Windows Password	Default authenticator to use in preference to remembering the last used method.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM
Framework	Reauthentication	DWORD	HideAlways UseMethod	Hide Checkbox (1) or Show Checkbox (0) (default)	Hide or show the Always Use Method checkbox.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM
Synchronization	ASDI Sync	SZ	UAMProgram DataLocation	N/A	Optional LDAP path to global data in format "LDAP:\\[host[:port]\]CN=path,DC=domain". Blank will contact any available domain controller on default port and will use the default path of "CN=UAM,CN=Passlogix,CN=Program Data,DC=domain".	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\ UAM\SyncManager\ Synchronizers \ADSI

Target	Category	Type	Name	Values	Description	Path
Synchronization	ASDI Sync	DWORD	StoreUser DataUnder ProgramData	Store with Global Data (1) or Store Under User Objects (0) (default)	Choose where to store per-user credentials. Note: User Objects are only supported in AD.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ SyncManager\ Synchronizers \ ADSI
Synchronization	Sync Timeouts	DWORD	SyncData Timeout	Default is 10000 ms Allowed range is 1-2147483646 ms	Time to wait for any foreground data sychronization to complete.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ SyncManager
Synchronization	Sync Timeouts	DWORD	SyncPolicy Timeout	Default is 10000 ms Allowed range is 1-2147483646 ms	Time to wait for any foreground policy sychronization to complete.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ SyncManager
Synchronization	Per-Logon Sync	DWORD	SyncData AuthInterval	Default is 5 minutes Allowed range is 1-2147483646 minutes	Sync user data at logon only if data sync not performed with past X minutes.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ SyncManager
Synchronization	Per-Logon Sync	DWORD	SyncData AuthAsync	Asynchronous Update (1) (default), or Synchronous Update (0)	Sync user data at logon synchronously or asynchronously.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ SyncManager
Synchronization	Per-Logon Sync	DWORD	SyncPolicy AuthInterval	Default is 5 minutes Allowed range is 1-2147483646 minutes	Sync user policy at logon only if policy sync not performed with past X minutes.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ SyncManager
Synchronization	Per-Logon Sync	DWORD	SyncPolicy AuthAsync	Asynchronous Update (1) (default), or Synchronous Update (0)	Sync user policy at logon synchronously or asynchronously.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ SyncManager
Synchronization	Background Sync	DWORD	SyncBackground	Disabled - No background sync (0) (default), Enabled - Sync Policy and Data (1), Sync User Data Only (2), Symc User Policy Only (3)	Enable or disable periodic background service update of cached user policy and data.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ SyncManager
Synchronization	Background Sync	DWORD	SyncBackground Interval	Default is 90 minutes Allowed range is 1-2147483646 minutes	Set time interval between periodic background service update of cached user policy and data	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\ UAM\ SyncManager
Client	Enrollment	DWORD	DisplayEnroll Success	Default is 5 seconds Allowed range is 1-2147483646 seconds	Hide or display enroll success dialog and configure auto-submit timer.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\ UAM\Client
Logon	General	SZ	DefaultAuthenticator	None, Fingerprint, BioAPI, Proximity Card, Smart Card, Windows Password	Default authenticator to use in preference to remembering the last used method.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\ UAM\Gina
Fingerprint	BIO-key BSP	DWORD	NumFingers ToEnroll	Default is 3 fingers Allowed range is 1-10 fingers	WARNING: MUST BE DEFINED AND SET TO 1 OR ESSO-UAM WILL NOT WORK. Internal BIO-key fingers per enrollment setting with default of 3.	HKEY_LOCAL_MACHINE\ SOFTWARE\ BIO-key\Biometric Service Provider\Setting

Target	Category	Type	Name	Values	Description	Path
					This setting is NOT related to the policy to control the number of fingers required for enrollment.	
Proximity Card	General	DWORD	InsertionDelay	Default is 0 ms Allowed range is 1-2147483646 ms	Rest period between accepting consecutive proximity token insertions.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}\ Settings
Proximity Card	Omnikey Provider	DWORD	EnableOmnikey	Enabled (1) (default), or Disabled (0)	Enable or disable the Omnikey proximity card provider.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}\ Settings
Proximity Card	Omnikey Provider	DWORD	MinPresence	Default is 0 ms Allowed range is 1-2147483646 ms	Minimum token presence before accepting a proximity token. Note: Use 1500 or greater to resolve Omnikey 5125 driver defect.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}\ Settings
Proximity Card	RFIdeas Provider	DWORD	EnableRFIdeas	Enabled (1) (default), or Disabled (0)	Enable or disable the RFIdeas proximity card provider.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}\ Settings
Proximity Card	RFIdeas Provider	DWORD	RFIdeasMinBits	Default is 8 bits Allowed range is 0-64 bits	Minimum number of bits to accept as a serial number.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}\ Settings
Proximity Card	RFIdeas Provider	DWORD	RFIdeasSerial	Enabled (1), or Disabled (0) (default)	Enable or disable RFIdeas serial COM port devices.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}\Settings

Target	Category	Type	Name	Values	Description	Path
Smart Card	General	DWORD	EnableUamPin	Disabled - User Smart Card PIN (0) (default), Enabled - Use UAM PIN (1)	Configure smart card authenticator to use CARD PIN or a virtual UAM PIN.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Settings
Smart Card	Microsoft Base CSP Provider	DWORD	Enabled	Enabled (1) (default), or Disabled (0)	Enable or disable smart card authenticator support for Microsoft Base CSP.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5F70E3497E138}\ Providers\BaseCSP
Smart Card	PKCS#11 Provider	DWORD	Enabled	Enabled (1) (default), or Disabled (0)	Enable or disable smart card authenticator support for PKCS#11.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\ PKCS#11
Smart Card	PKCS#11 Provider	SZ	PathFileName	N/A	Relative or full path to PKCS#11 DLL. Appended to Registry Key/Value contents, if any.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\PKCS#11
Smart Card	PKCS#11 Provider	SZ	PathRegKey	N/A	Registry key to read PKCS#11 DLL path and/or filename from. Used with Registry Value.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\ PKCS#11
Smart Card	PKCS#11 Provider	SZ	PathRegValue	N/A	Registry value to read PKCS#11 DLL path and/or filename from. Used with Registry Key.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\ PKCS#11
Smart Card	PKCS#11 Provider	DWORD	CardTimeout	Default is 2000 ms Allowed range is 0-5000 ms	Registry value to read PKCS#11 DLL path and/or filename from. Used with Registry Key.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Settings
Smart Card	PKCS#11 Provider	DWORD	SerialTimeout	Default is 500 ms Allowed range is 0-5000 ms	Max time to wait for a PKCS#11 module to report serial information for an inserted card.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\ Settings

Target	Category	Type	Name	Values	Description	Path
Smart Card	PKCS#11 Provider	DWORD	NeverUnload Module	Unload DLLs After Use (0) (default), Never Unload DLLs (1)	Option to keep each PKCS#11 DLL permanently loaded in each process.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\ Settings
Smart Card	PKCS#11 Provider	DWORD	ExternalAuthMode	Smart Card PIN Authentication (0) (default), PKCS#11 Protected Auth Flag (1), Force External Authentication (2), Create Session Object (Morpho) (3)	Smart card authentication behavior.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\ PKCS#11
Smart Card	PKCS#11 Provider	DWORD	ExternalAuthDialog	Hide Status Dialog (0) (default), Show Status Dialog (1)	Show or hide status dialog when performing external authentication.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\ PKCS#11
Smart Card	PKCS#11 Provider	DWORD	ExternalEnrollMode	Auth Mode Reauthentication (0) (default), PIN + Morpho Fingerprint Enroll (1), Force Smart Card PIN Auth (2), No Auth (Register Card ID Only) (3)	Smart card enrollment behavior.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\ PKCS#11

Global Branding Settings

These are general settings related to branding. They allow customers to modify certain brandable text or graphical elements of ESSO-UAM on a per-deployment or per-computer basis.

Target	Category	Type	Name	Values	Description	Path
Framework	Common	SZ	STR:Framework:136	ESSO-UAM	Product Short Name	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\Branding
Framework	Common	SZ	STR:Framework:137	Oracle Enterprise Single Sign-on Universal Authentication Manager	Product Long Name	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\Branding
Framework	Reauthentication	SZ	BMP:Framework:112	N/A	Reauthentication Banner (500x75)	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\Branding
Framework	Reauthentication	SZ	BMP:Framework:111	N/A	Reauthentication Band (500x2)	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\Branding
Logon	General	SZ	BMP:uamgina:1	N/A	Logon/Unlock Banner (500x75)	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\Gina\Branding
Logon	General	SZ	BMP:uamgina:2	N/A	Logon/Unlock Band (500x2)	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\Gina\Branding
Fingerprint	General	SZ	STR:BiometricAuth:107	Fingerprint	Authenticator Name	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {16627EE1-FAE3-43B5-B884-D3661649B97D}\Branding
Fingerprint	General	SZ	ICO:BiometricAuth:103	N/A	Authenticator Icon (24x24)	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {16627EE1-FAE3-43B5-B884-D3661649B97D}\Branding
Fingerprint	General	SZ	ICO:BiometricAuth:109	N/A	Authenticator Icon (48x48)	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Authenticators\ {16627EE1-FAE3-43B5-B884-D3661649B97D}\ Branding
BioAPI	General	SZ	STR:BiometricAuth:108	BioAPI	Authenticator Name	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Authenticators\ {17875AD3-D203-4F07-BF48-78876545AF4C}\ Branding
BioAPI	General	SZ	ICO:BiometricAuth:103	N/A	Authenticator Icon (24x24)	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Authenticators\ {17875AD3-

Target	Category	Type	Name	Values	Description	Path
						D203-4F07-BF48-78876545AF4C}\ Branding
BioAPI	General	SZ	ICO:BiometricAuth:109	N/A	Authenticator Icon (48x48)	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Authenticators\ {17875AD3-D203-4F07-BF48-78876545AF4C}\ Branding
Proximity Card	Sound Effects	SZ	WAV:ProxCardAuth:113	N/A	Omnikey: Undefined = default sound; Blank = disabled. RFIdeas: Disabled by default; use "DEFAULT" to enable.	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Authenticators\ {4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}\Branding
Proximity Card	Sound Effects	SZ	WAV:ProxCardAuth:110	N/A	Disabled by default; use "DEFAULT" to enable.	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Authenticators\ {4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}\Branding
Proximity Card	Sound Effects	SZ	WAV:ProxCardAuth:112	N/A	Applies only to Omnikey, if MinPresence is enabled. Undefined = default sound; Blank = disabled.	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Authenticators\ {4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}\Branding
Proximity Card	General	SZ	STR:ProxCardAuth:101	Proximity Card	Authenticator Name	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Authenticators\ {4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}\ Branding
Proximity Card	General	SZ	ICO:ProxCardAuth:106	N/A	Authenticator Absent Icon (24x24)	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Authenticators\ {4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}\Branding
Proximity Card	General	SZ	ICO:ProxCardAuth:109	N/A	Authenticator Absent Icon (48x48)	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Authenticators\ {4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}\Branding
Proximity Card	General	SZ	ICO:ProxCardAuth:107	N/A	Authenticator Present Icon (24x24)	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Authenticators\ {4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}\Branding
Proximity Card	General	SZ	ICO:ProxCardAuth:108	N/A	Authenticator Present Icon (48x48)	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Authenticators\ {4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}\Branding

Target	Category	Type	Name	Values	Description	Path
Smart Card	General	SZ	STR:SmartCardAuth:101	Smart Card	Authenticator Name	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Branding
Smart Card	General	SZ	ICO:SmartCardAuth:103	N/A	Authenticator Absent Icon (24x24)	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Branding
Smart Card	General	SZ	ICO:SmartCardAuth:110	N/A	Authenticator Absent Icon (48x48)	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Branding
Smart Card	General	SZ	ICO:SmartCardAuth:108	N/A	Authenticator Present Icon (24x24)	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Branding
Smart Card	General	SZ	ICO:SmartCardAuth:109	N/A	Authenticator Present Icon (48x48)	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Branding
Windows Password	General	SZ	STR:WinPwdAuth:101	Windows Password	Authenticator Name	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Authenticators\ {0C29417D-8A20-48B7-8CC4-D948D384E9B2}\Branding
Windows Password	General	SZ	ICO:WinPwdAuth:104	N/A	Authenticator Icon (24x24)	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Authenticators\ {0C29417D-8A20-48B7-8CC4-D948D384E9B2}\Branding
Windows Password	General	SZ	ICO:WinPwdAuth:103	N/A	Authenticator Icon (48x48)	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Authenticators\ {0C29417D-8A20-48B7-8CC4-D948D384E9B2}\Branding

Per-Computer Administrative Settings

These are the system-wide Administrative Settings, which override any local user settings. In Local Mode, these can be overridden by Per-User Administrative Settings. In Enterprise Mode, they can instead be overridden by Roaming Policy.

For complete descriptions of the settings, see the explanations earlier in this guide about each one:

- Logon Method Enabled
- Enrollment Prompt
- Grace Period
- Removal Action
- PIN Settings

Target	Category	Type	Name	Values	Description	Path
Fingerprint	Logon	SZ	{C8D690F8-BB7F-4955-9101-DEF05B589327}_{16627EE1-FAE3-43B5-B884-D3661649B97D}	Yes (1) (default), or No (0)	Logon Method Enabled	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\ UAM\Policy\AdminSettings
Fingerprint	Enrollment	SZ	{D4C8B939-3CD5-479E-9EB9-A4EDAB1A50DE}_{16627EE1-FAE3-43B5-B884-D3661649B97D}	Never (1), Required (2) (default), or Optional (3)	Enrollment Prompt	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\ UAM\Policy\AdminSettings
Fingerprint	Enrollment	SZ	{27579BAF-BADA-4B24-BA59-E10DD7F6D981}_{16627EE1-FAE3-43B5-B884-D3661649B97D}	Default is 0 days Allowed range is 0-365 days	Grace Period	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\ UAM\Policy\AdminSettings
Fingerprint	Enrollment	SZ	{08AB29CE-763D-4A2F-B330-B9E9DD3F70DF}_{16627EE1-FAE3-43B5-B884-D3661649B97D}	Default is 1 finger Allowed range is 0-10 fingers	Number of Fingers.	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\ UAM\Policy\AdminSettings
BioAPI	Logon	SZ	{C8D690F8-BB7F-4955-9101-DEF05B589327}_{17875AD3-D203-4F07-BF48-78876545AF4C}	Yes (1) (default), or No (0)	Logon Method Enabled	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\ UAM\Policy\AdminSettings
BioAPI	Enrollment	SZ	{D4C8B939-3CD5-479E-9EB9-A4EDAB1A50DE}_{17875AD3-D203-4F07-BF48-78876545AF4C}	Never (1), Required (2) or Optional (3) (default)	Enrollment Prompt	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\ UAM\Policy\AdminSettings
BioAPI	Enrollment	SZ	{27579BAF-BADA-4B24-BA59-E10DD7F6D981}_{17875AD3-D203-4F07-BF48-78876545AF4C}	Default is 0 days Allowed range is 0-365 days	Grace Period	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\ UAM\Policy\AdminSettings
Proximity Card	Logon	SZ	{C8D690F8-BB7F-4955-9101-DEF05B589327}_{4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}	Yes (1) (default), or No (0)	Logon Method Enabled	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\ UAM\Policy\AdminSettings

Target	Category	Type	Name	Values	Description	Path
Proximity Card	Enrollment	SZ	{D4C8B939-3CD5-479E-9EB9-A4EDAB1A50DE}_{4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}	Never (1), Required (2) or Optional (3) (default)	Enrollment Prompt	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\ UAM\Policy\AdminSettings
Proximity Card	Enrollment	SZ	{27579BAF-BADA-4B24-BA59-E10DD7F6D981}_{4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}	Default is 0 days Allowed range is 0-365 days	Grace Period	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\ UAM\Policy\AdminSettings
Proximity Card	Logon	SZ	{2B7E42A3-35D8-4573-BEBE-0C82F1A2998F}_{4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}	No Action (1), Lock Workstation (2) (default), or Force Logoff (3)	Removal Action	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\ UAM\Policy\AdminSettings
Proximity Card	PIN	SZ	{0E210D72-3F54-46C4-A95D-4960393F3AA1}_{4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}	Yes (1) (default), or No (0)	PIN Required	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\ UAM\Policy\AdminSettings
Proximity Card	PIN	SZ	{582A6014-0816-4B44-B3DD-91DFD11C0684}_{4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}	Default is 4 characters Allowed range is 4-16 characters	PIN Minimum Length	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\ UAM\Policy\AdminSettings
Proximity Card	PIN	SZ	{8CC1ED12-EF2B-4275-9125-56401F9AC189}_{4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}	Any Characters (1) (default) Alphanumeric Only (2) Numeric Only (3)	PIN Allowed Characters	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\ UAM\Policy\AdminSettings
Smart Card	Logon	SZ	{C8D690F8-BB7F-4955-9101-DEF05B589327}_{A1B34553-8D40-42A9-8ED5-F70E3497E138}	Yes (1) (default) or No (0)	Logon Method Enabled	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\ UAM\Policy\AdminSettings
Smart Card	Enrollment	SZ	{D4C8B939-3CD5-479E-9EB9-A4EDAB1A50DE}_{A1B34553-8D40-42A9-8ED5-F70E3497E138}	Never (1), Required (2) or Optional (3) (default)	Enrollment Prompt	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\ UAM\Policy\AdminSettings
Smart Card	Enrollment	SZ	{27579BAF-BADA-4B24-BA59-E10DD7F6D981}_{A1B34553-8D40-42A9-8ED5-F70E3497E138}	Default is 0 days Allowed range is 0-365 days	Grace Period	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\ UAM\Policy\AdminSettings
Smart Card	Logon	SZ	{2B7E42A3-35D8-4573-BEBE-0C82F1A2998F}_{A1B34553-8D40-42A9-8ED5-F70E3497E138}	No Action (1), Lock Workstation (2) (default), or Force Logoff (3)	Removal Action	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\ UAM\Policy\AdminSettings
Smart Card	PIN	SZ	{33CCA390-B497-4BF7-A472-E17403D319B0}_{A1B34553-8D40-42A9-8ED5-F70E3497E138}	Yes (1) (default) or No (0)	PIN Required	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\ UAM\Policy\AdminSettings
Windows Password	Logon	SZ	{C8D690F8-BB7F-4955-9101-DEF05B589327}_{0C29417D-8A20-48B7-8CC4-D948D384E9B2}	Yes (1) (default) or No (0)	Logon Method Enabled	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\ UAM\Policy\AdminSettings

Per-User Administrative Settings

These are the system-wide Per-User Administrative Settings to override the Roaming Policy or user settings for the selected user on this computer. These are only used in Local Mode, and can override both User Settings and Per-Computer Administrative Settings.

The registry path for the Per-User Administrative Settings will depend on whether the user is a Domain user or Local user. Values must be all uppercase, and prefixed by `SID::` (Local) or `GUID::` (Domain). The examples in the table below are for a Local User.

- If the user is a Local user, the registry path will end with "`SID::<USER'S SECURITY IDENTIFIER>`." For example, `SID::S-1-5-21-776561741-838170752-682003330-1003`.
- If the user is a Domain user, the registry path will end with "`GUID::<USER'S GLOBAL UNIQUE IDENTIFIER>`." For example, `GUID::{86C79ABC-913C-471B-9DCB-8DC38AAC7DE1}`.

For complete descriptions of the settings, see the explanations earlier in this guide about each one:

- Logon Method Enabled
- Enrollment Prompt
- Grace Period
- Removal Action
- PIN Settings

Target	Category	Type	Name	Values	Description	Path
Fingerprint	Logon	SZ	{C8D690F8-BB7F-4955-9101-DEF05B589327}_{16627EE1-FAE3-43B5-B884-D3661649B97D}	Yes (1) (default), or No (0)	Logon Method Enabled	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Policy\ AdminSettings\ SID::<Identifier>
Fingerprint	Enrollment	SZ	{D4C8B939-3CD5-479E-9EB9-A4EDAB1A50DE}_{16627EE1-FAE3-43B5-B884-D3661649B97D}	Never (1), Required (2) (default), or Optional (3)	Enrollment Prompt	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Policy\ AdminSettings\ SID::<Identifier>
Fingerprint	Enrollment	SZ	{27579BAF-BADA-4B24-BA59-E10DD7F6D981}_{16627EE1-FAE3-43B5-B884-D3661649B97D}	Default is 0 days Allowed range is 0-365 days	Grace Period	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Policy\ AdminSettings\ SID::<Identifier>
Fingerprint	Enrollment	SZ	{08AB29CE-763D-4A2F-B330-B9E9DD3F70DF}_{16627EE1-FAE3-43B5-B884-D3661649B97D}	Default is 1 finger Allowed range is 0-10 fingers	Number of Fingers.	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Policy\ AdminSettings\ SID::<Identifier>
BioAPI	Logon	SZ	{C8D690F8-BB7F-4955-9101-DEF05B589327}_{17875AD3-D203-4F07-BF48-78876545AF4C}	Yes (1) (default), or No (0)	Logon Method Enabled	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Policy\ AdminSettings\

Target	Category	Type	Name	Values	Description	Path
						SID::<Identifier>
BioAPI	Enrollment	SZ	{D4C8B939-3CD5-479E-9EB9-A4EDAB1A50DE}_{17875AD3-D203-4F07-BF48-78876545AF4C}	Never (1), Required (2) (default), or Optional (3)	Enrollment Prompt	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Policy\ AdminSettings\ SID::<Identifier>
BioAPI	Enrollment	SZ	{27579BAF-BADA-4B24-BA59-E10DD7F6D981}_{17875AD3-D203-4F07-BF48-78876545AF4C}	Default is 0 days Allowed range is 0-365 days	Grace Period	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Policy\ AdminSettings\ SID::<Identifier>
Proximity Card	Logon	SZ	{C8D690F8-BB7F-4955-9101-DEF05B589327}_{4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}	Yes (1) (default), or No (0)	Logon Method Enabled	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Policy\ AdminSettings\ SID::<Identifier>
Proximity Card	Enrollment	SZ	{D4C8B939-3CD5-479E-9EB9-A4EDAB1A50DE}_{4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}	Never (1), Required (2) or Optional (3) (default)	Enrollment Prompt	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Policy\ AdminSettings\ SID::<Identifier>
Proximity Card	Enrollment	SZ	{27579BAF-BADA-4B24-BA59-E10DD7F6D981}_{4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}	Default is 0 days Allowed range is 0-365 days	Grace Period	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Policy\ AdminSettings\ SID::<Identifier>
Proximity Card	Logon	SZ	{2B7E42A3-35D8-4573-BEBE-0C82F1A2998F}_{4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}	No Action (1), Lock Workstation (2) (default), or Force Logoff (3)	Removal Action	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Policy\ AdminSettings\ SID::<Identifier>
Proximity Card	PIN	SZ	{0E210D72-3F54-46C4-A95D-4960393F3AA1}_{4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}	Yes (1) (default), or No (0)	PIN Required	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Policy\ AdminSettings\ SID::<Identifier>
Proximity Card	PIN	SZ	{582A6014-0816-4B44-B3DD-91DFD11C0684}_{4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}	Default is 4 characters Allowed range is 4-16 characters	PIN Minimum Length	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Policy\ AdminSettings\ SID::<Identifier>
Proximity Card	PIN	SZ	{8CC1ED12-EF2B-4275-9125-56401F9AC189}_{4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}	Any Characters (1) (default) Alphanumeric Only (2) Numeric Only (3)	PIN Allowed Characters	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Policy\ AdminSettings\ SID::<Identifier>

Target	Category	Type	Name	Values	Description	Path
Smart Card	Logon	SZ	{C8D690F8-BB7F-4955-9101-DEF05B589327}_{A1B34553-8D40-42A9-8ED5-F70E3497E138}	Yes (1) (default) or No (0)	Logon Method Enabled	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Policy\ AdminSettings\ SID::<Identifier>
Smart Card	Enrollment	SZ	{D4C8B939-3CD5-479E-9EB9-A4EDAB1A50DE}_{A1B34553-8D40-42A9-8ED5-F70E3497E138}	Never (1), Required (2) or Optional (3) (default)	Enrollment Prompt	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\ Policy\ AdminSettings\ SID::<Identifier>
Smart Card	Enrollment	SZ	{27579BAF-BADA-4B24-BA59-E10DD7F6D981}_{A1B34553-8D40-42A9-8ED5-F70E3497E138}	Default is 0 days Allowed range is 0-365 days	Grace Period	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\Policy\AdminSettings\ SID::<Identifier>
Smart Card	Logon	SZ	{2B7E42A3-35D8-4573-BEBE-0C82F1A2998F}_{A1B34553-8D40-42A9-8ED5-F70E3497E138}	No Action (1), Lock Workstation (2) (default), or Force Logoff (3)	Removal Action	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\Policy\ AdminSettings\ SID::<Identifier>
Smart Card	PIN	SZ	{33CCA390-B497-4BF7-A472-E17403D319B0}_{A1B34553-8D40-42A9-8ED5-F70E3497E138}	Yes (1) (default) or No (0)	PIN Required	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\Policy\AdminSettings\ SID::<Identifier>
Windows Password	Logon	SZ	{C8D690F8-BB7F-4955-9101-DEF05B589327}_{0C29417D-8A20-48B7-8CC4-D948D384E9B2}	Yes (1) (default) or No (0)	Logon Method Enabled	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\Policy\ AdminSettings\ SID::<Identifier>