Oracle® Enterprise Single Sign-On Universal Authentication Manager

Administrator's Guide

Release 11.1.2

E27160-02

August 2012

ORACLE®

Oracle Enterprise Single Sign-On Universal Authentication Manager, Administrator's Guide, Release 11.1.2

E27160-02

Table of Contents

Preface

The Oracle Fusion Middleware Administrator's Guide for Oracle Enterprise Single Sign-On Universal Authentication Manager describes how to deploy and configure Universal Authentication Manager across your enterprise.

Audience

This guide is intended for experienced administrators responsible for the planning, implementation, and deployment of Universal Authentication Manager. Administrators are expected to understand single sign-on concepts and be familiar with the Windows registry, the Oracle Enterprise Single Sign-On 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 as well as strong authentication technologies such as smart cards, proximity cards, and biometrics and the configuration and deployment procedures for Logon Manager, Password Reset, and Kiosk Manager.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support.

For information, visit http://www.oracle.com/support/contact.html or visit http://www.oracle.com/accessibility/support.html if you are hearing impaired.

Related Documents

For more information, see the other documents in the Oracle Enterprise Single Sign-On Suite Plus documentation set for this release.

Oracle Enterprise Single Sign-On Suite Plus

Release Notes

Installation Guide

Administrator's Guide

Secure Deployment Guide

User's Guide

Oracle Enterprise Single Sign-On Logon Manager

Deploying Logon Manager with Microsoft Active Directory

Deploying Logon Manager with Microsoft Active Directory Application Mode and Active Directory Lightweight Directory Services

Deploying Logon Manager with a Lightweight Directory Access Protocol Directory

Template Configuration and Diagnostics for Windows Applications

Template Configuration and Diagnostics for Web Applications

Template Configuration and Diagnostics for Mainframe Applications

Oracle Enterprise Single Sign-On Provisioning Gateway

Administrator's Guide

Command Line Interface Guide

Oracle Identity Manager Connector Guide

Sun Java System Identity Manager Connector Guide

IBM Tivoli Identity Manager Connector Guide

Oracle Enterprise Single Sign-On Universal Authentication Manager

Administrator's Guide

User's Guide

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Overview of Universal Authentication Manager

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 Universal Authentication Manager system also enhances enterprise security beyond traditional password authentication by providing two-factor authentication methods. Universal Authentication Manager enables users to rapidly and securely enroll credentials that will be used to identify and authenticate them.

At its core, Universal Authentication Manager 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, Universal Authentication Manager offers four built-in and configurable authentication methods: smart cards, passive proximity cards, biometric fingerprint, and a challenge questions quiz. Native Windows Passwords are also supported.

Universal Authentication Manager 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.

Universal Authentication Manager Repository Synchronization

Universal Authentication Manager can synchronize with Microsoft Active Directory for centralized storage of Universal Authentication Manager policies. When Universal Authentication Manager is configured to utilize a repository, it periodically synchronizes logon method policies and user credential enrollment data to and from the repository.

Synchronization only takes place when a client workstation is deployed in enterprise mode to utilize a centralized repository. The repository itself must be properly configured to support Universal Authentication Manager synchronization (for information on preparing the repository, see Configuring Oracle Enterprise Single Sign-On Universal Authentication Manager for Synchronization with a Repository).

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. User credential enrollment data is reconciled by timestamp - that is, newer local data is uploaded to the repository, while newer remote data is downloaded and cached on the client computer.

Universal Authentication Manager 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 every authentication and enrollment event. You can customize synchronization settings as described in Configuring Advanced Universal Authentication Manager Options.

Repository Functions

- Stores Universal Authentication Manager policies and enrollment data.
- Leverages existing repository schemas used by other Oracle Enterprise Single Sign-On Suite Plus products.
- Enrollment data is secure and access to is restricted.

Synchronization Functions

- Retrieves Universal Authentication Manager policies from the repository to local data cache.
- Reconciles data updated during offline operations from repository.
- Enforces security for proper access rights to repository data.

Administration of Universal Authentication Manager

Universal Authentication Manager administrators can configure and apply Universal Authentication Manager policy settings from a central location using the Oracle Enterprise Single Sign-On Administrative Console. The Oracle Enterprise Single Sign-On Administrative Console contains Universal Authentication Manager 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 control how a user or user group authenticates to the system and is stored as an object within the repository and Universal Authentication Manager's local cache. 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 a Policy for details.

Using the Oracle Enterprise Single Sign-On Administrative Console, an administrator can perform the following tasks:

Manage Universal Authentication Manager Policies

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

Manage the Deployment

- Configure the centralized data repository. See Configuring Universal Authentication Manager for Synchronization with a Repository for information on performing this procedure.

Fingerprints

Universal Authentication Manager enables you to enroll and use third party USB biometric fingerprint readers and readers embedded in laptops as an authentication mechanism to Universal Authentication Manager.

Administrators can configure up to ten fingerprint samples to be enrolled. By default, one fingerprint sample is required by Universal Authentication Manager, but Oracle recommends administrators increase this number to at least two to prevent lockout in case of injury in which the primary sample becomes unusable.

This logon method requires a supported biometric reader device and the BIO-key BSP v1.10 (older versions are not supported) 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.

Proximity Cards

A passive proximity card or token is an identity object (such as a workplace ID badge) containing a circuit that a card-reading device can detect and decipher. When the proximity card is placed in close proximity to a reader, the reader detects the token's presence and recognizes identifying information that is associated with a specific user. This Universal Authentication Manager logon method includes the option to require a user to enroll a PIN that is associated with a proximity token. When so configured, Universal Authentication Manager 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 or complete a logon or an 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. For more information, see the Registry Settings Reference.

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

Universal Authentication Manager supports two proximity card authentication methods:

- Proximity card only (no PIN)
- Proximity card plus Universal Authentication Manager PIN (default value)

About Proximity Card PINs

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 securely managed and stored (hash only) by Universal Authentication Manager. A Universal Authentication Manager 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 Universal Authentication Manager PIN is required for user authentication. When a Universal Authentication Manager 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 a Universal Authentication Manager PIN in conjunction with the card together as one event.

Smart Cards

A smart card is a credit card-sized token containing a chip or embedded circuits that can store and process data securely. Information stored on a smart card can also be used for identification and authentication. Universal Authentication Manager enables enrolling and using smart cards for user logon and authentication without writing any data to the smart card. A PIN is required to enroll and use a smart card at all times.

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.

About Smart Card PINs

Smart cards issued to users have an associated PIN that is stored and managed on each card. Universal Authentication Manager requires users to utilize a PIN with their smart card at all times and you may choose to require either the smart card's built in PIN or allow the user to generate and assign a custom Universal Authentication Manager PIN to the smart card. This PIN is securely stored (hash only, never the actual PIN) and managed by Universal Authentication Manager and is not written to the card. To select the desired PIN mode, see Configuring a Smart Card Policy.

Your environment must satisfy the following prerequisites in order to use a smart card with its built-in PIN:

- Each card must have an embedded serial number.
- Each card must have a valid digital certificate and a key pair, which can be generated either by third-party tools or Universal Authentication Manager. Oracle recommends using the method that conforms more closely to your organization's security policies. Cards without a valid certificate and key pair can only be used with a Universal Authentication Manager-generated PIN.

> To have Universal Authentication Manager generate a key pair, you must configure it to do so via Universal Authentication Manager Registry Settings. Universal Authentication Manager does not generate digital certificates and one is not required in such scenario.

- Your card's middleware must conform to the Microsoft Base CSP standard **or** be both fully PKCS#11-compliant and provide a CSP module.
- If using Windows XP and Microsoft Base CSP-compliant middleware, the Microsoft Base CSP framework must be installed.

A policy setting controls whether the card's built in PIN or a user-assigned Universal Authentication Manager PIN will be used. Settings for controlling the minimum PIN length and allowed characters are also available.

During card enrollment, a user must either correctly submit a smart card’s PIN value or provide a new custom PIN 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.

Challenge Questions

Challenge Questions is a question-and-answer quiz that can be used as a fallback logon method when authentication via other enrolled methods fails. Challenge Questions requires the user to correctly answer enough questions to satisfy a predetermined weight requirement for successful logon.

In local mode, the questions and answers, as well as their weight requirements are preconfigured and cannot be altered. In enterprise mode, Universal Authentication Manager supports

synchronization with Password Reset, which enables the use of Password Reset to store questions and answers enrolled by the user through Universal Authentication Manager (existing Password Reset enrollments cannot be used by Universal Authentication Manager) providing portability for the enrollment data. Synchronization with Password Reset also enables control over the questions that are available to different users and groups, as well as individual customization of the weight of each question, as allowed by Password Reset.

> If you're deploying Universal Authentication Manager in enterprise mode and install the Challenge Questions logon method,you **must** configure synchronization with a Password Reset server, as described in Integrating with Password Reset. Otherwise, users will be unable to enroll with or authenticate via the Challenge Questions method across your network.

In order to synchronize with Password Reset, you must:

- Deploy Password Reset on your network.
- Deploy Universal Authentication Manager in enterprise mode.
- Provide the Password Reset synchronization URL of a fully functional Password Reset server instance.
- Instruct users to select their questions and provide answers by enrolling the Challenge Questions logon method via Universal Authentication Manager; existing Password Reset enrollments cannot be used by Universal Authentication Manager.

> If you are using the Challenge Questions logon method on a machine that is not connected to the Internet and are experiencing long delays when enrolling in or answering a Challenge Questions quiz, disable the option **Check for publisher's certificate revocation** in Internet Explorer. The delay is caused by the Microsoft .NET Framework attempting to look up the server's certificate and timing out when a certificate authority cannot be reached.

Deploying Universal Authentication Manager

This section covers the following Universal Authentication Manager deployment tasks:

- Selecting the Client Mode
- Configuring Universal Authentication Manager for Synchronization with a Repository
- Integrating with Logon Manager
- Integrating with Password Reset
- Integrating with Kiosk Manager

Selecting the Client Mode

During installation, you can select whether to install Universal Authentication Manager in either local mode or enterprise mode.

Local Mode

In local mode, Universal Authentication Manager securely stores policies and enrollment data on the local machine. Note that:

- A Windows-default security policy limits the local account's use of blank passwords to workstation logon only. In consequence, local accounts with blank passwords can not be used to authenticate to Universal Authentication Manager, even though they can still be used to authenticate to Windows. Oracle recommends that you enforce cryptographically strong passwords across your enterprise at all times.
- If Universal Authentication Manager is switched to enterprise mode and synchronizes with a repository, any policy settings configured by the administrator will be enforced and override all local policy settings; locally stored enrollment data will be stored in the repository instead from that point forward.
- If you have deployed Universal Authentication Manager in local mode and are planning to switch to enterprise mode, users must not enroll on multiple machines; doing so will cause an encryption key mismatch once the multiple enrollments are synchronized to the repository and result in possible loss of the enrollment data.

Enterprise Mode

In enterprise mode, Universal Authentication Manager synchronizes with a central repository in which it stores enrollment data and from which it retrieves policy settings deposited by the administrator. Note that:

- When Universal Authentication Manager is able to connect to the repository, it synchronizes any policy and user enrollment changes as required during each authentication and enrollment operation. Various aspects of synchronization can be configured by the administrator, including recurring background synchronization.
- When Universal Authentication Manager is unable to connect to the repository, it will continue to function and use a locally stored copy of policies and enrollments retrieved during the last successful synchronization. Any policy updates deployed to the repository will not take effect until a connection to the repository is reestablished and synchronization is completed.
- When deploying Universal Authentication Manager in enterprise mode, users must not enroll in any logon methods until synchronization with the repository has been properly configured and tested. Otherwise, the pre-synchronization enrollment data will be lost.

If you're deploying Universal Authentication Manager in enterprise mode and install the Challenge Questions logon method, you **must** configure synchronization with a Password Reset server, as described in Integrating with Password Reset. Otherwise, users will be unable to enroll with or authenticate via the Challenge Questions method across your network.

Switching from Local to Enterprise Mode on an Existing Installation

If you plan to have Universal Authentication Manager synchronize with a repository, as a best practice, Oracle recommends installing Universal Authentication Manager in local mode and switching over to enterprise mode manually after the repository has been prepared and synchronization settings configured as described in Preparing the Universal Authentication Manager Repository.

To switch an existing Universal Authentication Manager installation from local mode to enterprise mode, set the registry key `HKLM\Software\Passlogix\UAM\ClientMode` to a dword value of 1 (0x00000001) and restart the machine.

When making the switch, enforce the following:

- Users must not enroll or authenticate to Universal Authentication Manager at all (even with Windows password) prior to switching from local to enterprise mode. Otherwise, all enrollment data will be lost.
- The switch should occur after installing Universal Authentication Manager and configuring the Universal Authentication Manager service account but before rebooting the workstation.

Configuring Universal Authentication Manager for Synchronization with a Repository

Before completing the procedures in this section, note that:

- Oracle recommends that you install Universal Authentication Manager in local mode and switch it to enterprise (synchronization) mode as described in Selecting the Client Mode only after you have prepared the repository and configured synchronization settings. Otherwise, Universal Authentication Manager data structures may not be correctly created or permissions correctly set within the repository.
- When deploying Universal Authentication Manager in enterprise mode, users must not enroll in any logon methods until synchronization with the repository has been properly configured and tested. Otherwise, enrollment data will be lost.
- Only Microsoft Active Directory is supported as a repository.

In order to allow Universal Authentication Manager to centrally store and manage policies and enrollment data, you must prepare an Active Directory-based repository and configure Universal Authentication Manager for synchronization with that repository by performing the following tasks:

- Create a Universal Authentication Manager Service Account
- Extend the Schema
- Enable Data Storage Under User Objects
- Initialize Universal Authentication Manager Storage
- Configure the Universal Authentication Manager Synchronizer

When assigning user groups, keep the following in mind:

- User groups used should be in the same domain,
- Use security groups, not distribution groups,
- Universal Authentication Manager will only support a single Active Directory domain.

Preparing the Repository when Logon Manager is Already Deployed

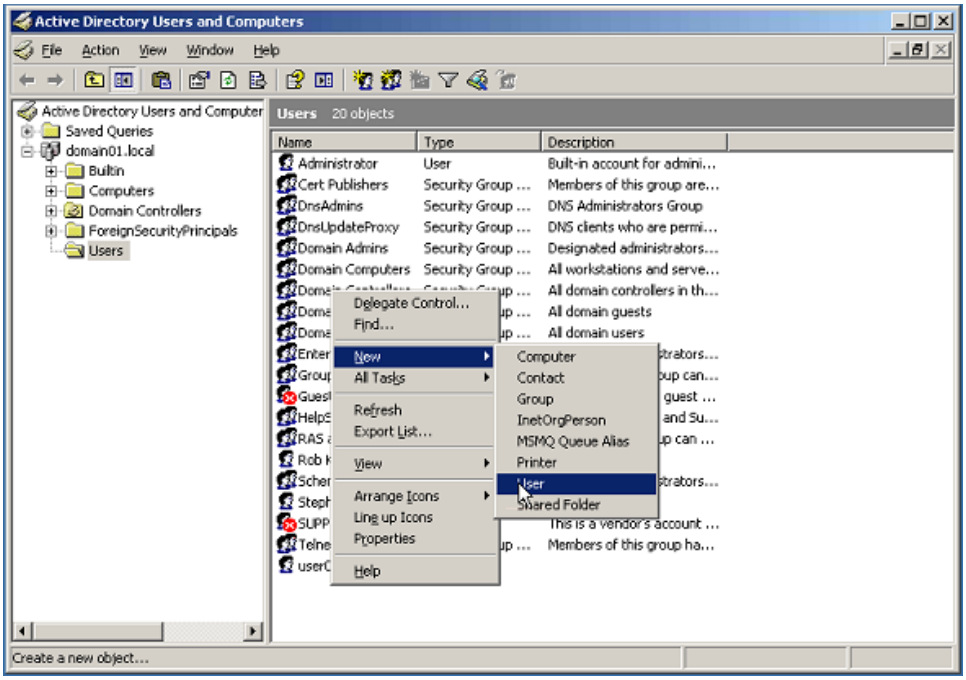
If Logon Manager is already installed and synchronizing with your Active Directory-based repository, Universal Authentication Manager will be sharing Logon Manager's repository container to store its own policies and settings. In such cases, you do not need to extend the schema or enable data storage under user objects. Instead, complete the following steps:

- Complete the steps in Initializing Universal Authentication Manager Storage.
- Complete the steps in Configuring the Universal Authentication Manager Synchronizer.

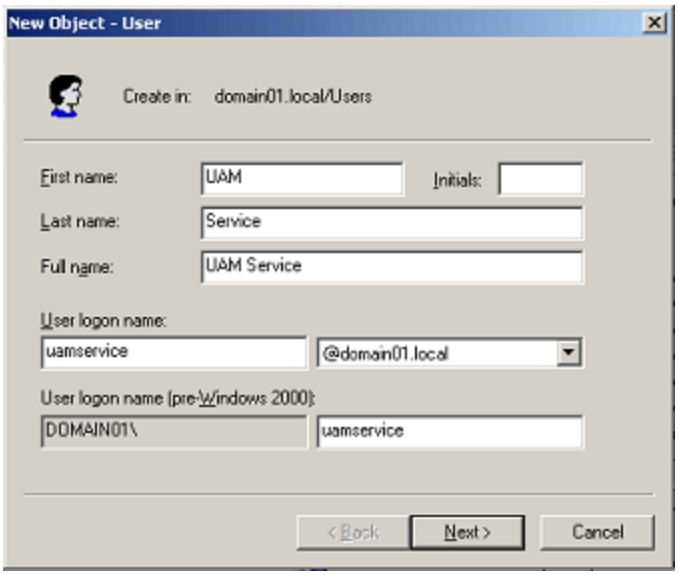
Creating a Universal Authentication Manager Service Account

In order for Universal Authentication Manager to read and write data in the repository, you must give it the privileges to do so. This is accomplished by creating a service account that Universal Authentication Manager uses to interact with its repository. This account should be a standard domain account (member of Domain Users); no other permissions are necessary.

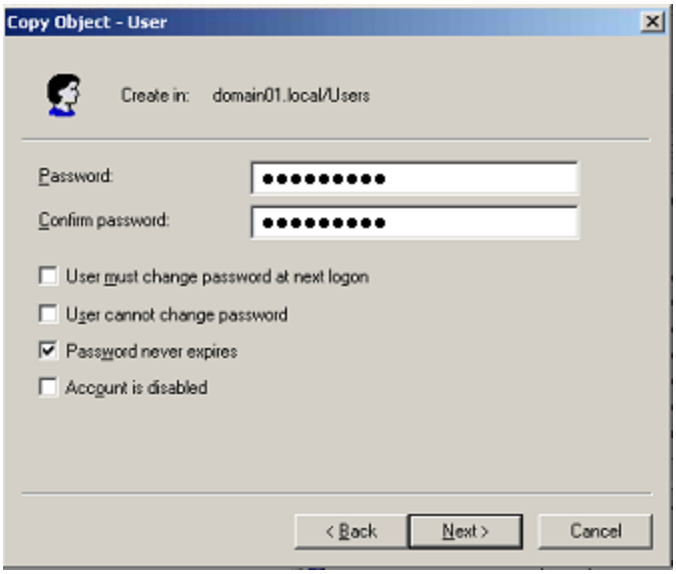
1. On the workstation that will serve as your domain controller, launch **Active Directory Users and Computers**.
2. Right-click in the Users container and select **New > User**. The User account is a regular member of the Domain Users group.



3. Enter a name for the user or group account (for this example, the name is `uamservice`) and click **Next>**.



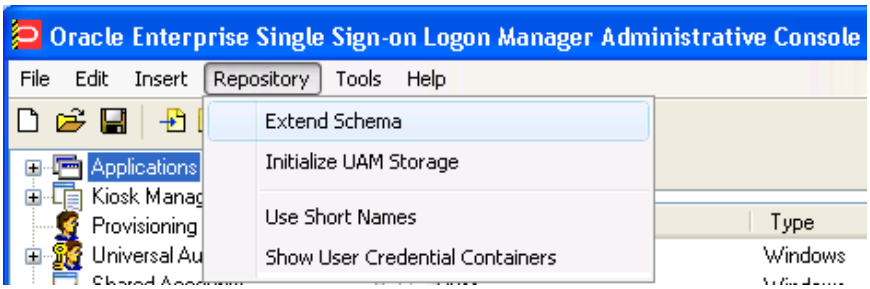
4. Enter a password and check the **Password never expires** box.



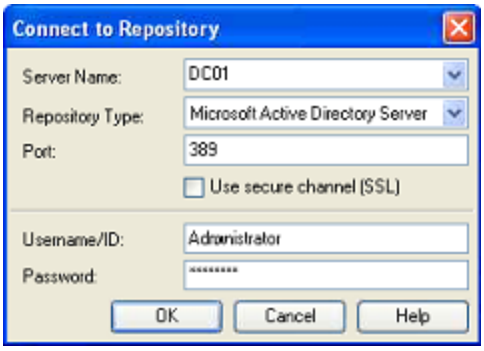
Extending the Schema

> If you are not sure whether you have already extended the schema, simply complete the steps below; performing the schema extension multiple times will not harm your repository or the data it contains.

1. Launch the Oracle Enterprise Single Sign-On Administrative Console.
2. From the Repository menu, select **Extend Schema**.



3. In the Connect to Repository dialog box that appears, enter a **Server Name** (for this example, the name is DC01), select **Microsoft Active Directory Server** from the drop-down menu, select the **Use secure channel (SSL)** check box if your environment is configured for SSL connectivity, enter the**Port** number (this example uses port 389), and the **Username/ID** and **Password** of an administrative account with Domain and Schema Administrator permissions. Click **OK** when finished.

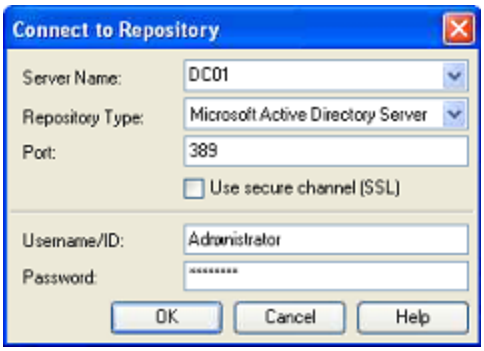


Enabling Data Storage Under User Objects

After extending the schema, you must allow Universal Authentication Manager to store enrollment data under each respective user's user object within the repository. To do so, complete the following steps:

> If Logon Manager is already installed and synchronizing with your repository, you do not need to enable this option, as it is already enabled; proceed to the next section.

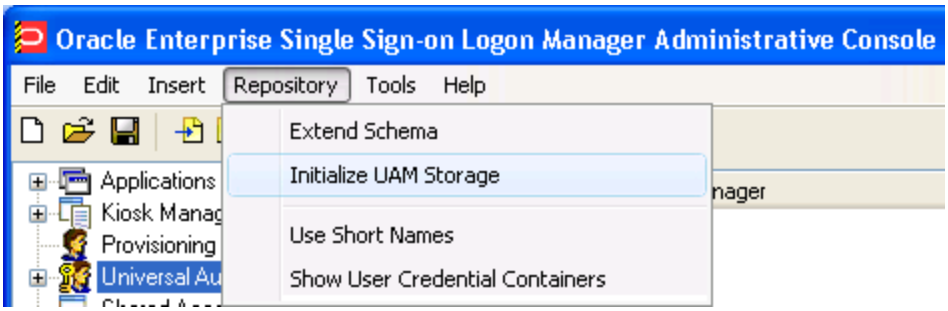
1. In the left-hand tree, right-click the **Repository** node and select **Connect To...** from the context menu.
2. In the Connect to Repository dialog box that appears, enter a **Server Name** (for this example, the name is DC01), select **Microsoft Active Directory Server** from the drop-down menu, select the **Use secure channel (SSL)** check box if your environment is configured for SSL connectivity, enter the**Port** number (this example uses port 389), and the **Username/ID** and **Password** of an administrative account with Domain and Schema Administrator permissions. Click **OK** when finished.



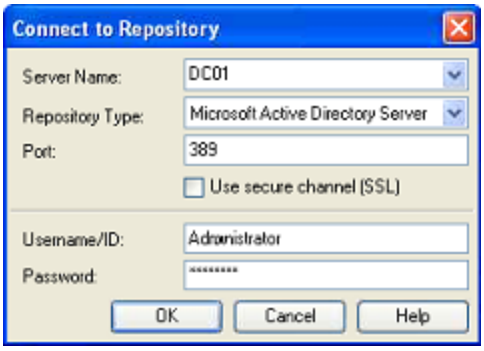
3. From the **Repository** menu, select **Enable Storing Credentials Under User Object**.
4. In the prompt that appears, click **OK**.
5. In the confirmation dialog that appears, click **OK** to dismiss it.

Initializing Universal Authentication Manager Storage

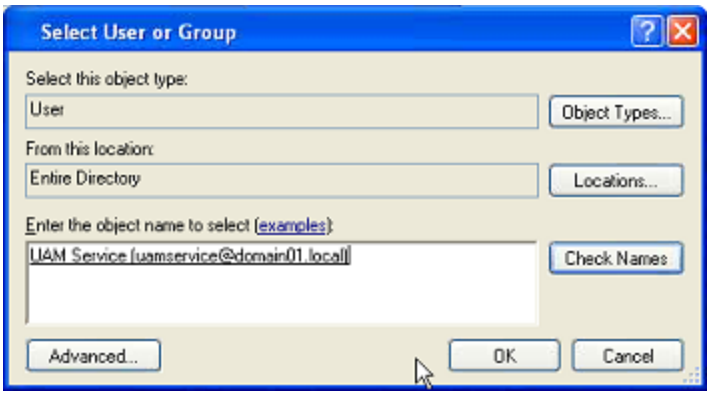
1. After successfully extending the schema, return to the Repository menu and select **Initialize UAM Storage**.



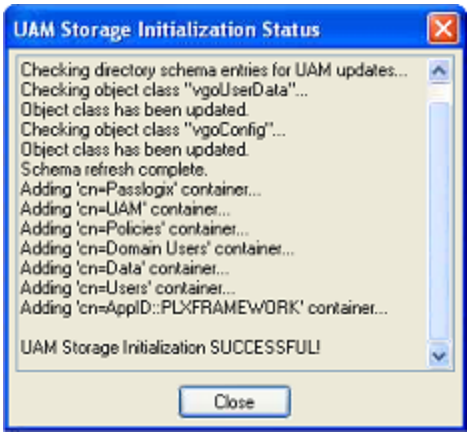
2. From the drop-down menu, select the server that you just created. The other fields are filled in automatically.



3. Click **OK**.
4. In the Select User or Group window, start typing the name of your service account, then click **Check Names**. The service account name is filled in automatically.



5. Click **OK** and wait for the success message.

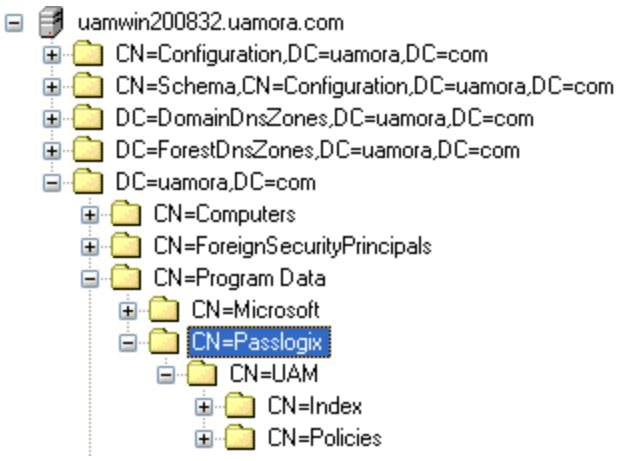


The data structures have now been created and the required permissions set. For more information on what's done in the repository during this step, see the next section.

About The Universal Authentication Manager Repository Data Structures and Permissions

When you invoke the **Initialize UAM Storage** command described earlier, Universal Authentication Manager does the following within your repository:

1. Modifies the schema to ensure that vgoUser and vgoConfig classes may be placed inside Container objects.
2. Builds the default container structure "Program Data/Passlogix/UAM" with subcontainers "Policies" and "Index" as shown below:



Never manually modify the contents of the index and policies containers.

The containers can be named differently if your environment requires so; however, you will need to manually configure all Universal Authentication Manager client instances to point to the custom-named containers. Oracle highly recommends you leave the container names at their defaults.

3. Grants the Universal Authentication Manager service account generic read, write, modify, and delete permissions to the index container (as well as all other permissions inherited from its parent) so that the Universal Authentication Manager service can read, create, modify, and delete objects in the index container.
4. Grants the Universal Authentication Manager service account generic read permissions (as well as any permissions inherited from its parent) so that the Universal Authentication Manager service can read objects within the policies container.
5. Updates the domain root DSE object to grant the Universal Authentication Manager service account permissions to create and delete vgoConfig and vGoUser objects under User objects across the entire domain. (If the user objects have been relocated to a custom location, the permissions can be set directly at the target container instead of at the root.)
6. Updates the domain root DSE object to grant the Universal Authentication Manager service account generic read permissions to all vgoConfig objects across the domain so that the Universal Authentication Manager service can read all vgoConfig objects regardless of their location in the repository.

Configuring the Universal Authentication Manager Synchronizer

You are now ready to configure the Universal Authentication Manager to allow Universal Authentication Manager to synchronize with the repository. Complete the following steps:

1. Launch the Oracle Enterprise Single Sign-On Administrative Console.
2. In the left-hand tree navigate to **Global Agent Settings > [TargetSettingsSet>] > Synchronization.**
3. If Logon Manager is not installed and synchronizing with the repository, add a configuration node for the Active Directory synchronizer to your settings set as follows (otherwise skip to the next step):

a. Right-click the **Synchronization** node and select **Manage** synchronizers from the context menu.

b. In the window that appears, click **Add**.

c. In the list of available synchronizers, select **Active Directory**, enter ADEXT as the name, and click **OK**.

d. Click **OK** to dismiss the dialog. The **ADEXT** node appears under the **Synchronization** node.

4. Do one of the following:

   - If Logon Manager is installed and synchronizing with the repository, do not modify the value of the **Base location(s) for configuration objects** field; instead, skip to the next step.
   - If Logon Manager is *not* installed and synchronizing with the repository, do the following in the **Base location(s) for configuration objects** field:

     i. Select the check box.

     ii. Click the **...** button.

     iii. In the window that appears, enter the fully qualified DN of the Universal Authentication Manager **Policies** container.

     iv. Click **OK**.

5. In the **Base location(s) for UAM storage index** field, select the check box, click the ... button, and enter the fully qualified DN of the Index container, then click **OK**.
6. If it is not already set, select the check box next to the **Location to store user credentials** option and select **Under respective directory user objects** from the drop-down list.
7. Configure other synchronization settings as desired; for more information on each setting, see the Console help.
8. Export your settings to a .REG file for distribution to end-user workstations:

   a. From the **File** menu, select **Export**.

   b. In the dialog that appears, click **HKLM Registry Format**.

   c. In the "Save" dialog that appears, navigate to the desired location and provide a name for the .REG file, then click **Save**.

9. Distribute the .REG file to your Universal Authentication Manager workstations and merge it into their Windows registries.

Configuring Universal Authentication Manager Synchronization for Administrative Users

The rights necessary to store credentials under user objects are granted at the tree root and inherited down to user objects. If you are deploying Universal Authentication Manager in enterprise mode in an environment where members of protected user groups, such as Administrators, will be using it, you must grant the Universal Authentication Manager service account through the AdminSDHolder object the permissions necesary to create and delete vGOUserData and vGOSecret objects.

If Logon Manager is already installed and synchronizing with the same repository that Universal Authentication Manager is utilizing, you will also need to grant these permissions to the AdminSDHolder object itself, which was most likely done during Logon Manager deployment. This granting will appear as "SELF" in the affected adminstrative user's permissions list, as well as in the AdminSDHolder object's permissions list.

Without this explicit permission application, administrative users will be blocked from storing their Universal Authentication Manager data in the repository due to automatic inheritance of restrictive rights from the AdminSDHolder object. This is because the object's ACL, which governs the ACLs of all protected groups, prohibits rights inheritance by default. More information about this issue is available in the following MS Knowledge Base article: http://support.microsoft.com/kb/817433.

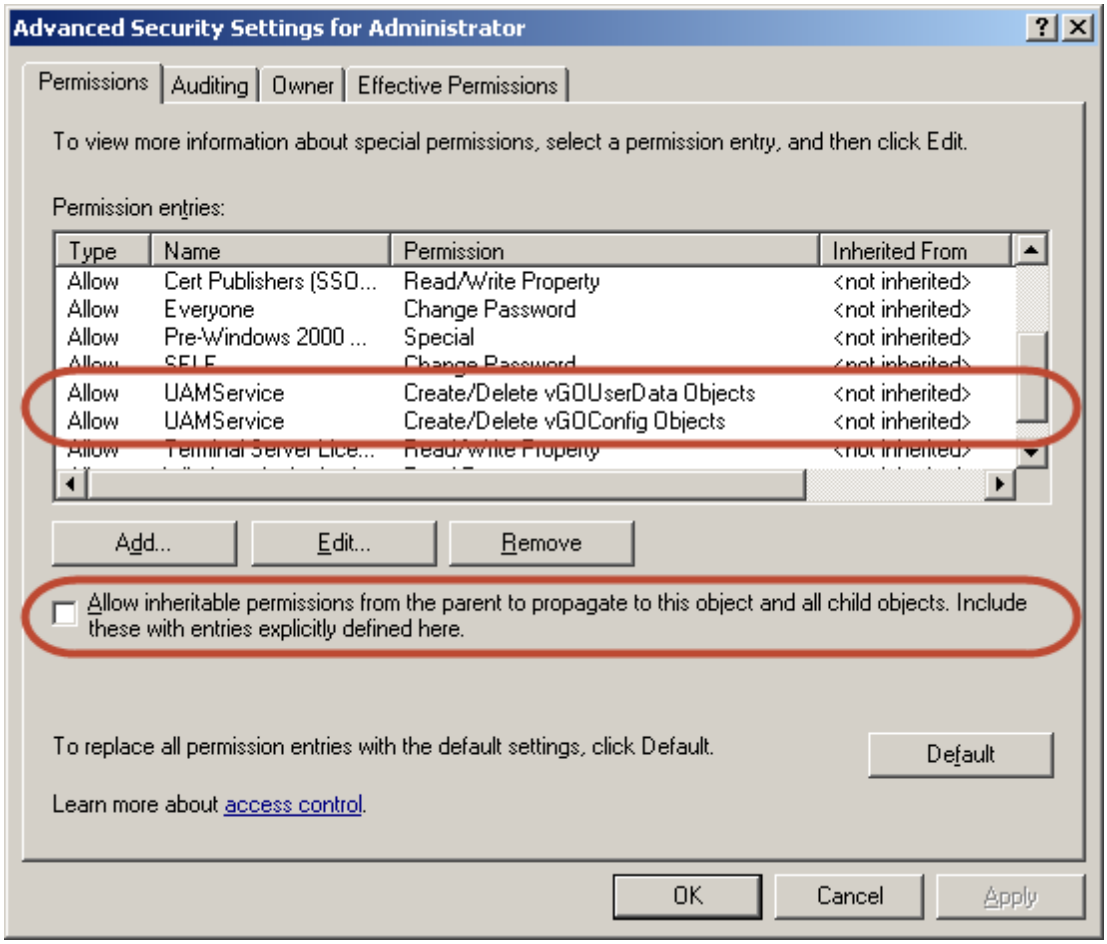
The following protected user groups are known to be affected by this problem:

- Enterprise Admins
- Schema Admins
- Domain Admins
- Administrators
- Account Operators
- Server Operators
- Print Operators
- Backup Operators
- Cert Publishers

To verify that you are experiencing this particular issue, do the following:

1. Log in to the primary domain controller as a domain administrator.
2. Open the "Active Directory Users and Computers" MMC snap-in.
3. From the **View** menu, select **Advanced Features**.
4. Navigate to the affected user object, right-click it, and select **Properties**.
5. In the dialog that appears, select the **Security** tab.

6. Click **Advanced**. The "Advanced Security Settings" dialog appears:

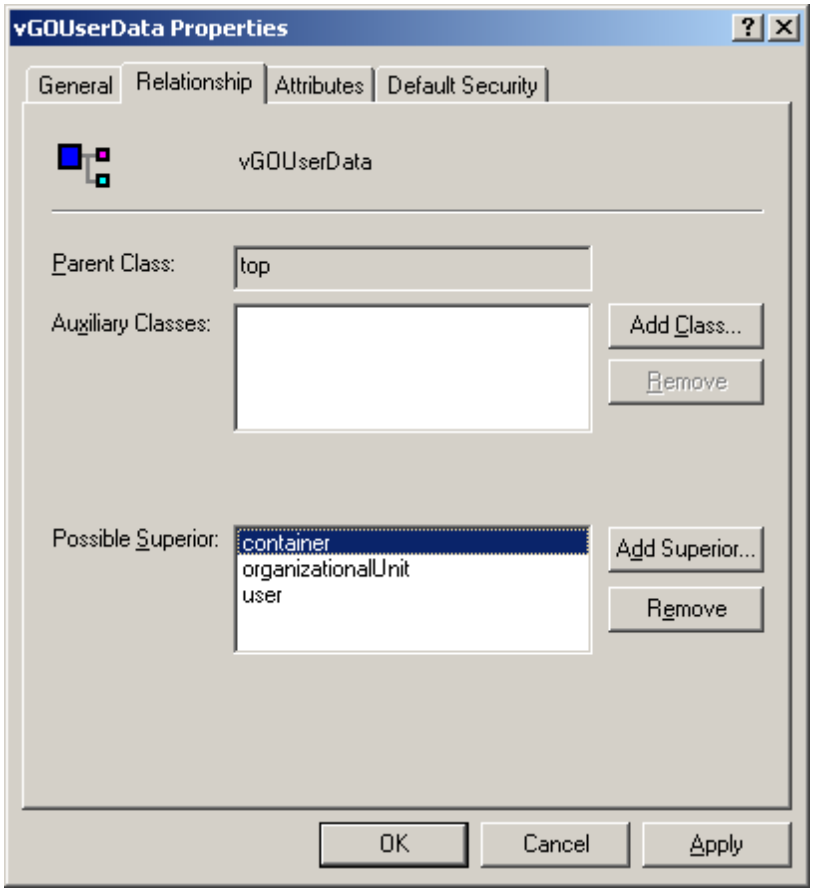


7. In the dialog, check whether:
   - **The Allow inheritable permissions...** check box is not selected.
   - The permissions highlighted in the figure in step 6 are not present in the list.

   If the above conditions are true, the user object is not inheriting the necessary permissions from the directory root.

To rectify this issue, you must manually modify the ACL of the AdminSDHolder object to grant the right to create objects of type vGOConfig and vGOUserData. The steps are as follows:

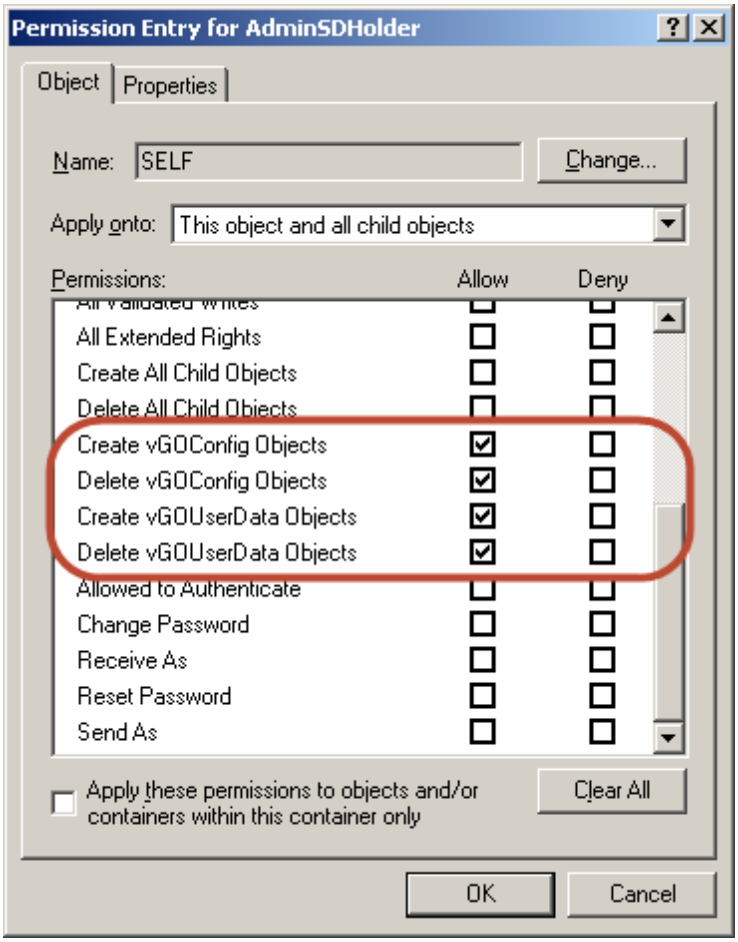
1. Log in to the primary domain controller as a domain administrator.
2. In the Microsoft Management Console, open the "Active Directory Schema" snap-in.
3. In the left-hand tree, drill down the **Classes** node and locate the **vGOUserData** node.
4. Right-click the **vGOUserData** node and select **Properties** from the context menu.
5. In the properties dialog that appears, select the **Relationship** tab.
6. Click the **Add Superior** button.
7. In the dialog that appears, select container from the drop-down list and click **OK**.
   The container class appears in the "Possible Superior" field.



8. In the Microsoft Management Console, open the "Active Directory Users and Computers" snap-in.
9. From the **View** menu, select **Advanced Features**.
10. Navigate to the **AdminSDHolder** container located in cn=AdminSDHolder,cn=System,dc=<domainName>,dc=<domainSuffix>
11. Right-click the **AdminSDHolder** container and select **Properties**.
12. In the "Properties" dialog, select the **Security** tab and click **Advanced**.
13. In the "Advanced Security Settings" dialog, click **Add...** .
14. In the "Select User, Computer, or Group" dialog, enter the name of the Universal Authentication Managerservice account and click **OK**.
15. In the "Permission Entry" dialog, do the following:
    a. From the **Apply onto:** drop-down list, select **This object and all child objects**.

> If the create and delete permissions for vGOUserData objects do not appear in the permissions list, select **User objects** from the **Apply onto:** drop-down list instead. This variation occurs between different versions and patches of Active Directory and the underlying operating system.

    b. In the list of permissions, select the **Allow** check box for the permissions shown below:



c. Click **OK**.

16. Trigger the SD propagator (SDPROP) process to immediately propagate the changes throughout the network. Instructions for launching the SD propagator process are provided in the following Microsoft Knowledge Base article: http://support.microsoft.com/kb/251343.

> If you encounter a version of this procedure that calls to apply the above permissions onto "**This object only,**" disregard it. It is deprecated and has been superseded by the steps above.
>
> If you are running Windows Server 2008 R2, you can trigger the SD propagator process by kicking off the RunProtectAdminGroupsTask task.

Integrating with Logon Manager

You can configure Logon Manager to use Universal Authentication Manager as its primary logon method. Universal Authentication Manager supports integration with Logon Manager version 11.1.2.

When the Universal Authentication Manager installer detects that Logon Manager is installed, the Universal Authentication Manager Authenticator custom setup option is displayed, allowing you to choose to install the authenticator to enable integration with Logon Manager. If you choose to install the authenticator, the installer will ask whether you'd like to configure Universal Authentication Manager as the only available Logon Manager logon method. For details on installation, see the *Oracle Enterprise Single Sign-On Suite Plus Installation Guide*.

Integrating with Password Reset

The Universal Authentication Manager Challenge Questions logon method enables the use of Password Reset to store questions and answers enrolled by the user through Universal Authentication Manager (existing Password Reset enrollments cannot be used by Universal Authentication Manager) providing portability for the enrollment data. Synchronization with Password Reset also enables control over the questions that are available to different users and groups, as well as individual customization of the weight of each question, as allowed by Password Reset.

In order to configure Universal Authentication Manager to integrate with Password Reset, you must do the following:

1. Install the Challenge Questions logon method if it has not already been installed. For instructions, see the *Oracle Enterprise Single Sign-On Suite Plus Installation Guide*.
2. Install and configure Password Reset as described in the *Oracle Enterprise Single Sign-On Suite Plus Installation Guide.*
3. Obtain the Password Reset synchronization URL.
   The URL will have the following format:
   `https://<hostname>:<port>/vGOSelfServiceReset/WebServices/Synchronization.asmx`
4. Configure Universal Authentication Manager to synchronize with Password Reset as described in the next section.
5. Configure the challenge questions as desired within Password Reset. For more information, see Password Reset documentation.
6. Instruct users to select their questions and provide answers by enrolling the Challenge Questions logon method via Universal Authentication Manager; existing Password Reset enrollments cannot be used by Universal Authentication Manager.

To configure Universal Authentication Manager to leverage Password Reset questions and answers for authentication, do the following:

1. Launch the Oracle Enterprise Single Sign-On Suite Plus Administrative Console.
2. Under the **Global Agent Settings** node navigate to the settings set you want to modify, or load it if necessary.
3. Navigate to the **Password Reset** node and select it.
4. In the right-hand pane, select the check-box next to the **Password Reset Synchronization URL** option and enter the appropriate URL in the following format:

   `https://<hostname>:<port>/vGOSelfServiceReset/WebServices/Synchronization.asmx`

   
   If you have not configured your Password Reset deployment for SSL connectivity, replace https:// with http://.

5. Export your settings to a .REG file for distribution to end-user machines:
   a. From the **File** menu, select **Export**.
   b. In the dialog that appears, click **HKLM Registry Format (.REG)**.
   c. In the "Save" dialog that appears, navigate to a desired target location, enter a descriptive file name and click **Save**.

6. Distribute the .REG file to end-user machines and merge it into each machine's Windows registry.

Integrating with Kiosk Manager

On Windows XP deployments, Universal Authentication Manager can be used as an authentication mechanism for locking and unlocking Kiosk Manager sessions in kiosk environments. (Kiosk Manager is not compatible with Windows 7.)

In order to configure Universal Authentication Manager to integrate with Kiosk Manager, you must do the following:

1. Install and configure Logon Manager and Kiosk Manager as described in the *Oracle Enterprise Single Sign-On Suite Plus Installation Guide*.
2. Install Universal Authentication Manager as described in the *Oracle Enterprise Single Sign-On Suite Plus Installation Guide.* When prompted to keep replace the current GINA, you must select the **Keep Current GINA** option.
3. Set Universal Authentication Manager as the default logon method for Logon Manager as described in Integrating with Logon Manager.
4. Configure Universal Authentication Manager for synchronization with the repository, as described in Configuring Universal Authentication Manager for Synchronization with a Repository.
5. Configure Kiosk Manager as described in the next section.

To configure Kiosk Manager to allow the locking and unlocking of a session via Universal Authentication Manager, complete the following steps:

1. Configure Kiosk Manager strong authentication behavior as follows:
   a. Launch the Oracle Enterprise Single Sign-On Administrative Console.
   b. Navigate to **Global Agent Settings > [TargetSettingsSet] > Kiosk Manager**.
   c. In the **Strong Authentication** section, select the check box next to the **Monitor for device events** option and select **Always** from the drop-down menu.
   d. Select the check box next to the **Prepopulate on Startup** option and select **Always** from the drop-down menu.
   e. (Optional) If you don't want to lock the Kiosk Manager session when a Universal Authentication Manager token is removed, select the check box next to the **Lock session on ESSO-UAM token removal** option and select **No** from the drop-down menu. (The default is to lock the session on token removal.)
2. Configure Logon Managerto clear the user's local cache on shutdown:
   a. Navigate to **Global Agent Settings > [TargetSettingsSet] > Synchronization**.
   b. Select the check box next to the **Delete Local Cache** option and select **Yes** from the drop-down menu.
3. Configure Kiosk Manager user interface behavior as follows:
   a. Navigate to **Global Agent Settings > [TargetSettingsSet] > User Experience> Application Response**.

b. Select the check box next to the **Respond to hidden and minimized windows** option and select **No** from the drop-down menu.

4. Configure the Kiosk Manager session states required by Universal Authentication Manager:
   a. In the left hand tree, expand the **Kiosk Manager** (top level, not under **Global Agent Settings**) node.
   b. Configure the action and session state for the "KM Session Locked" event:
      i. Select the **Session States** sub-node.
      ii. Click **Add** and enter KMS_Locked as the name.
      iii. Select the **Events** tab.
      iv. Uncheck the **Session End** event.
      v. Check the **Session Locked** event.
      vi. Select the **Authenticators** tab.
      vii. Check the **Universal Authentication Manager** authenticator and uncheck all others.
      viii. Select the **Actions** tab.
      ix. Click **Add**.
      x. Enter KMA_Locked as the name, select the **Run List** option, and click **OK**.
      xi. Select the .NET API radio button and enter the following values into the fields:
         - **Assembly:** <ESSO-LM_Install_Directory> \AUI\UAMAuth\KioskSessionChange.dll
         - **Class:** CSessionStateChangeHandler
         - **Method:** SessionLocked
   c. Configure the action and session state for the "KM Before Session Unlocked" event:
      i. Select the **Session States** sub-node.
      ii. Click **Add** and enter KMS_IsUnlocking as the name.
      iii. Select the **Events** tab.
      iv. Uncheck the **Session End** event.
      v. Check the **Before Session Unlocked** event.
      vi. Select the **Authenticators** tab.
      vii. Check the **Universal Authentication Manager** authenticator and uncheck all others.
      viii. Select the **Actions** tab.
      ix. Click **Add**.
      x. Enter KMA_IsUnlocking as the name, select the **Run List** option, and click **OK**.
      xi. Select the .NET API radio button and enter the following values into the fields:
         - **Assembly:** <ESSO-LM_Install_Directory> \AUI\UAMAuth\KioskSessionChange.dll
         - **Class:** CSessionStateChangeHandler
         - **Method:** BeforeSessionUnlocked
5. Write your settings to the Windows Registry by selecting **Write Global Agent Settings to HKLM** from the **Tools** menu.

6. Publish your changes to the repository.

Working with Universal Authentication Manager Policies

This section describes the following tasks you can perform when working on policies:

Creating a Policy

To create a new Universal Authentication Manager 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**.

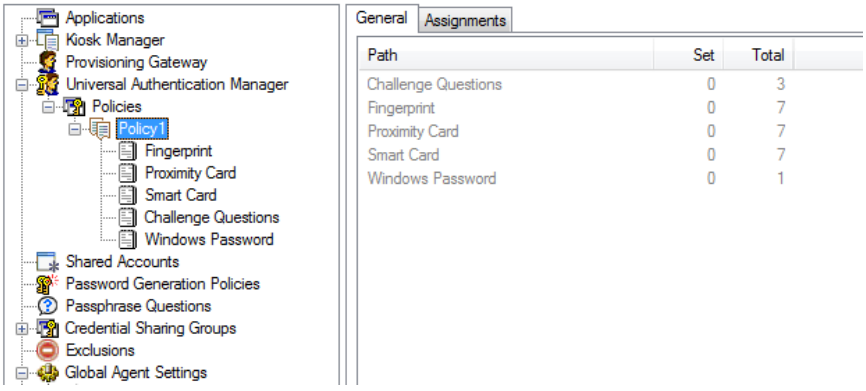
  or

- 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 and Assignments Tabs

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



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.

Assignments Tab (for a Selected Policy)

From the Assignments tab for a selected policy, you can assign the policy to specific user and/or user groups to which you want the policy applied.

For more information and restrictions on policy assignments, see Assigning Users and Groups to a Policy.

Configuring a Policy

Universal Authentication Manager 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.

Universal Authentication Manager administrators can configure and apply Universal Authentication Manager policy settings from a central location using the Oracle Enterprise Single Sign-On Administrative Console. The Oracle Enterprise Single Sign-On Administrative Console contains Universal Authentication Manager 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 Universal Authentication Manager that you can apply to users and user groups.

Before you begin creating policies, please read Ensuring Compatibility with Windows Domain Policies to ensure a conflict-free deployment.

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.

For details on configuring logon method settings, see:

- Configuring a Fingerprint Policy
- Configuring Proximity Card Policy
- Configuring a Smart Card Policy
- Configuring a Challenge Questions Policy
- Configuring a Windows Password Policy

> As a security best 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.

Enabling Logon Methods

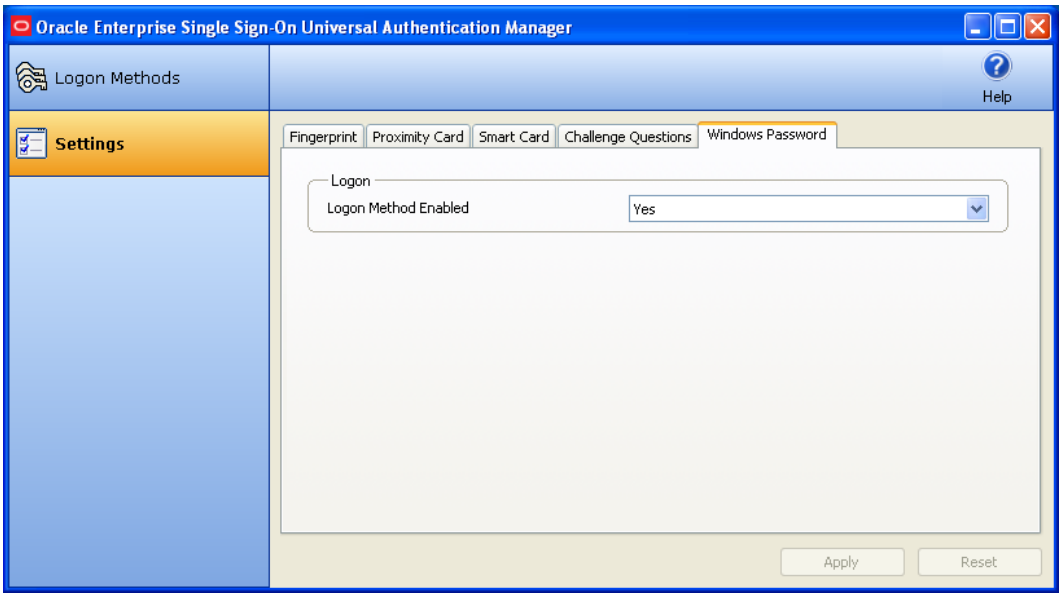
This section describes the policies that apply to *all* of the logon methods. For policies specific to a particular logon method, see the specific logon method settings section for a description.

Logon Method Enabled Policy

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

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

- In enterprise mode, the Logon Method Enabled policy setting is an Administrative policy only. This means that the policy will never appear in the Universal Authentication Manager settings.
- In local mode, the Logon Method Enabled policy setting is an end-user policy setting. You can manage the policy setting right from the Settings tab.



Windows Password Exception

Universal Authentication Manager 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* the user is not enrolled in at least one other method.

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

Logon Method Enabled Policy Prerequisites

Before you publish the Logon Method Enabled policy:

- You must install the Oracle Enterprise Single Sign-On Administrative Console on the system.
- You must install Universal Authentication Manager in enterprise 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 Oracle Enterprise Single Sign-On Administrative Console.
2. Either create a new Universal Authentication Manager 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 Universal Authentication Manager policy to the UAM Storage Container for your user or user group in the repository so that Universal Authentication Manager will apply the policy to the end-user.
5. Universal Authentication Manager syncs the Universal Authentication Manager policy for the end-user.

Logon Method Enabled Policy Rules

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

- The logon method is displayed in the 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 mode, the logon method appears in the Settings tab. All policy settings are disabled, and the Logon Method Enabled policy setting is not displayed.
- In local mode, the logon method appears in the 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.

Configuring Enrollment Prompts

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 Universal Authentication Manager.
- **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.

> Be careful when using the **Required** option. Since the Fingerprint, Proximity Card, and Smart Card logon methods require additional hardware, users may be unable to log on if one of those methods is configured as required and the required hardware is not available or functioning at logon time. Oracle highly recommends configuring a grace period or an optional enrollment for users who can potentially be affected by such a scenario.

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 policy only. You can edit the policy setting only by using the Oracle Enterprise Single Sign-On Administrative Console.

> Enrollment Grace Period does not appear as a user setting in Universal Authentication Manager in either local or enterprise mode. The value defaults to zero, and may be overridden by a policy in enterprise mode.

Configuring the Enrollment Prompt Policy

Before you publish the Enrollment Prompt policy:

- You must install the Oracle Enterprise Single Sign-On Administrative Console on the system.
- You must install Universal Authentication Manager in enterprise 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 Oracle Enterprise Single Sign-On Administrative Console.
2. Either create a new Universal Authentication Manager policy or select an existing one to modify.
3. Set the Enrollment Prompt value for each logon method to Never, Optional or Required.
4. Assign the policy to a user or group and publish it to the repository as described in Publishing a Policy.
5. Universal Authentication Manager applies the policy during the next synchronization with the repository.

Setting the Enrollment Grace Period

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) whenever the enrollment prompt for the logon method is configured as required. This applies to all logon methods that support enrollment (that is, 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 Oracle Enterprise Single Sign-On Administrative Console.

The grace period can be from 0 (no grace period) to 365 days long.

Enrollment Grace Period does not appear as a user setting in Universal Authentication Manager in either local or enterprise mode. The value defaults to zero, and may be overridden by a policy in enterprise mode.

Configuring the Grace Period Policy

Before you publish the Grace Period policy:

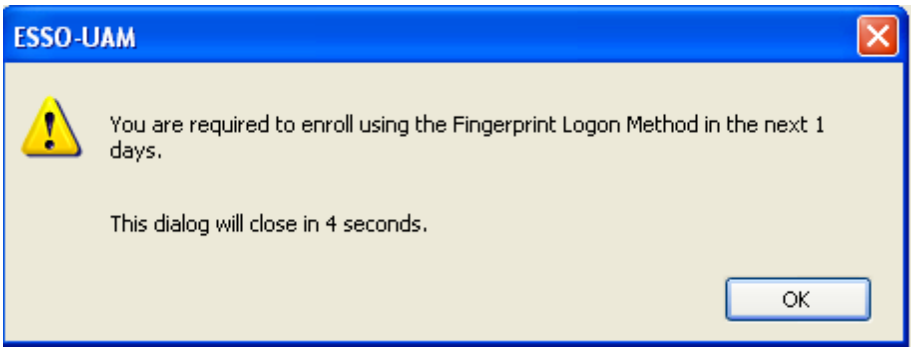
- You must install the Oracle Enterprise Single Sign-On Administrative Console on the system.
- You must install Universal Authentication Manager in enterprise mode on the end-user's system.
- You must install the desired logon method on the end-user's system.
- You must configure the end user's system for synchronization to the repository.

To configure the policy:

1. Launch the Oracle Enterprise Single Sign-On Administrative Console.
2. Either create a new Universal Authentication Manager 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. Assign the policy to a user or group and publish it to the repository as described in Publishing a Policy.
5. Universal Authentication Manager applies the policy during the next synchronization with the repository.

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 Grace Period Policy

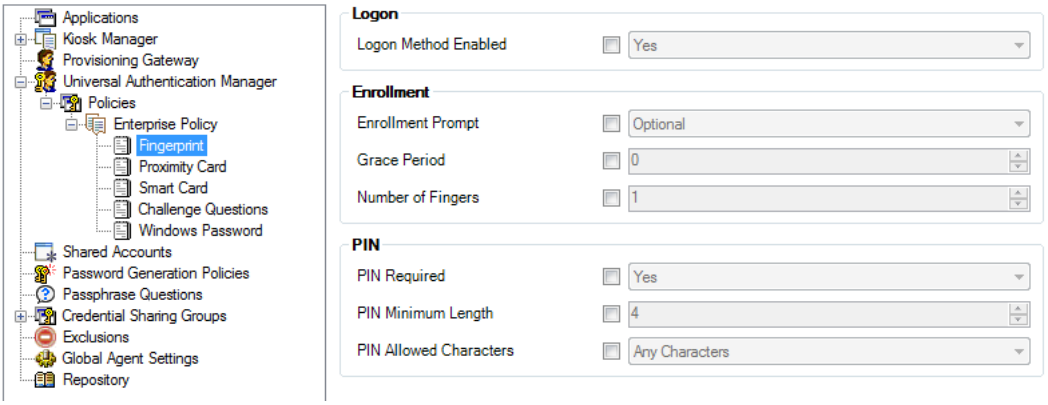
The Enrollment Grace Period will not be in effect (that is, it will be disabled) if any of the following conditions exist:

• The Logon Method Enrollment Prompt policy setting is NOT configured to "Required."

• The Logon Method Enrollment Grace Period policy setting is configured to zero.

Configuring a Fingerprint Policy

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.

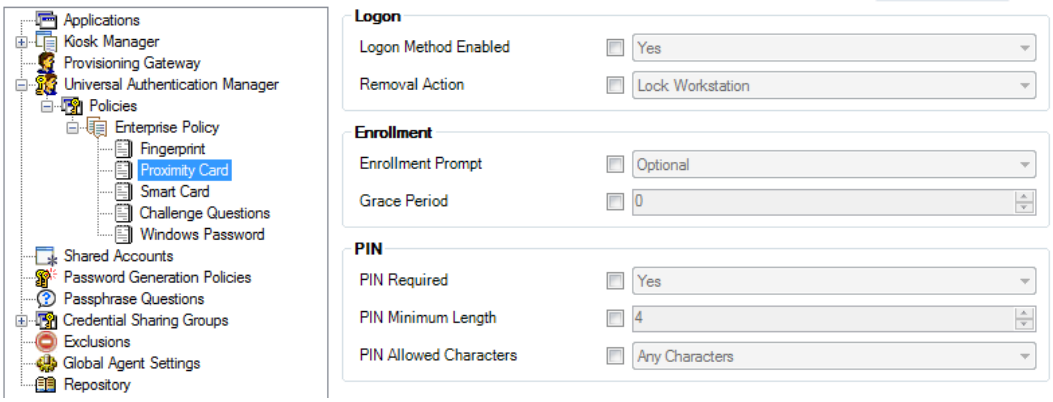


You can configure the following settings:

Logon Method Enabled	Allows you to enable or disable the logon method. 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.
PIN Required	Specifies whether you must submit a PIN in order to be authenticated. Options are **Yes** (default setting) or **No**.
PIN Minimum Length	The minimum allowed length for the PIN. Possible values are 4-16 characters (default setting is 4 characters).
PIN Allowed Characters	Restricts the character type(s) you can use in your PIN. Options are **numeric only**, **alphanumeric**, or **any characters**(default setting).

Configuring a Proximity Card Policy

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.



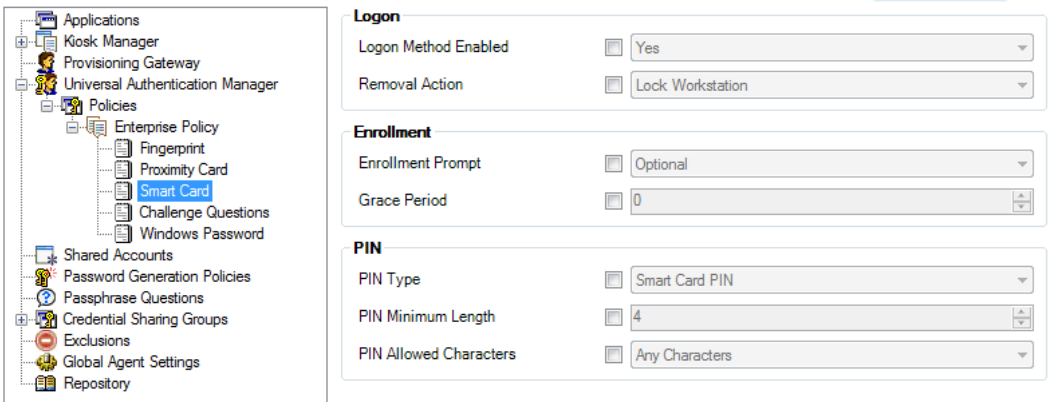
You can configure the following settings:

Logon Method Enabled	Allows administrators to enable or disable the logon method. 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

Configuring a Smart Card Policy

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.



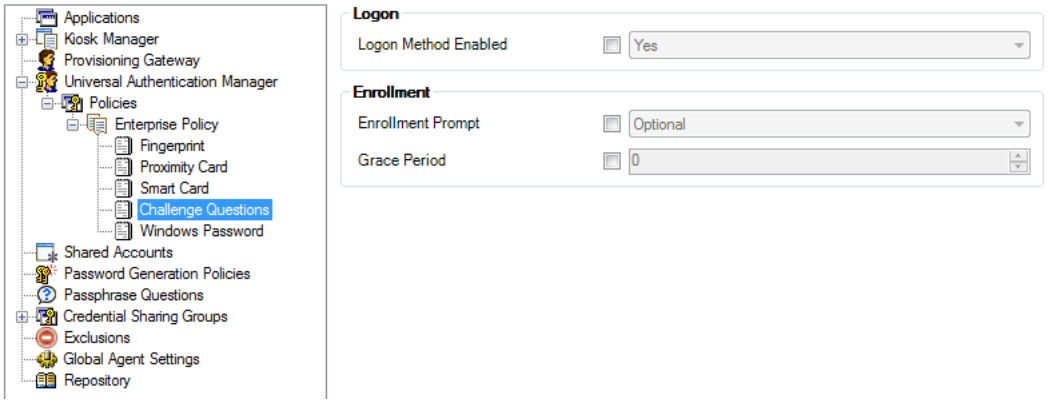
You can configure the following settings:

Logon Method Enabled	Allows administrators to enable or disable the logon method. 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 Type	Specifies whether to use the card's internal preconfigured PIN or create and store a PIN within Universal Authentication Manager's secure data store. Options are **Smart Card PIN** (default setting) or **ESSO-UAM PIN**.
PIN Minimum Length	(ESSO-UAM PIN type only) The minimum allowed length for the PIN. Possible values are 4-16 characters (default setting is 4 characters).
PIN Allowed Characters	(ESSO-UAM PIN type only) Restricts the character type(s) you can use in your PIN. Options are **numeric only**, **alphanumeric**,and **any characters** (default setting).

Configuring a Challenge Questions Policy

When you select **Challenge Questions** for a chosen policy, you are presented with all of the available challenge questions 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.

> If you have configured Universal Authentication Manager to integrate with Password Reset (enterprise mode only), you must configure the enrollment questions through Password Reset. Questions and answers cannot be modified when in local mode.
>
> Additionally, users must select their questions and provide answers by enrolling the Challenge Questions logon method via Universal Authentication Manager; existing Password Reset enrollments cannot be used by Universal Authentication Manager.

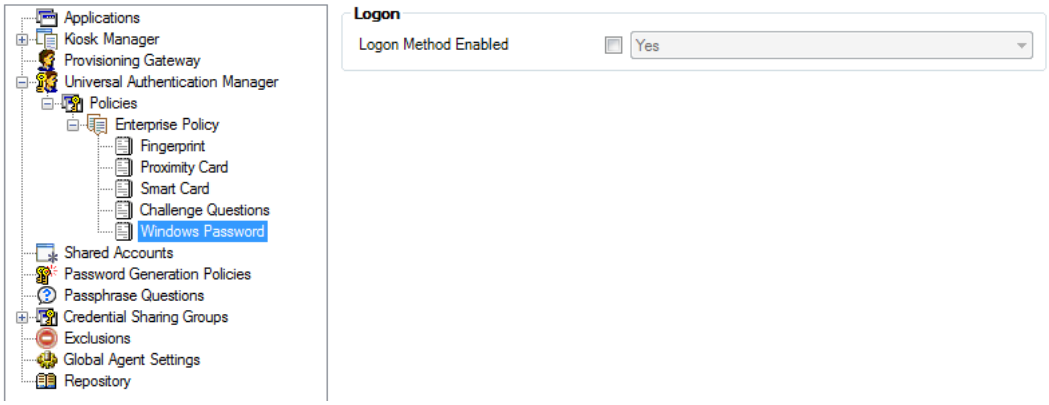


You can configure the following settings:

Logon Method Enabled	Allows administrators to enable or disable the logon method. 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.

Configuring a Windows Password Policy

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 Universal Authentication Manager 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 Universal Authentication Manager method.

Publishing a Policy

The procedure for publishing a Universal Authentication Manager policy is similar to that for publishing Logon Manager configuration objects.

In order to apply a policy to one or more users or user groups, you must:

1. Assign the desired users and/or groups to the target policy.
2. Publish the policy to the repository.

Assigning Users and Groups to a Policy

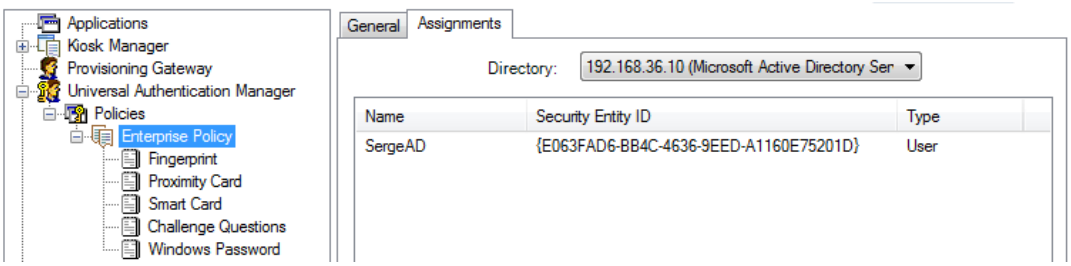
After you have created a new Universal Authentication Manager policy and configured its settings, you can apply the policy to specific users and/or groups by assigning those users or groups to the policy.

When assigning users and/or groups to a policy:

- Ensure that the machine you are using to make the assignments can connect to the Universal Authentication Manager repository.
- Assigning policies to the Domain Users group is not supported; if you assign this group to a policy, the assignment will be ignored.
- You must ensure that each Universal Authentication Manager-enrolled user is assigned exactly one policy, either directly or through membership in a user group. If multiple assignments are made, the results will be non-deterministic.

To assign users and/or groups to a policy:

1. Launch the Oracle Enterprise Single Sign-On Administrative Console.
2. In the left-hand tree, navigate to **Universal Authentication Manager > Policies**.
3. Under the **Policies** node, select the target policy, then select the **Assignments** tab in the right-hand pane.
4. Click **Add**.
5. In the Select User or Group dialog, enter the name of the desired user or group and click **Check Names** to validate it against your domain controller, then click **OK** to assign it to the policy. The assigned user or group appears in the assignments list.



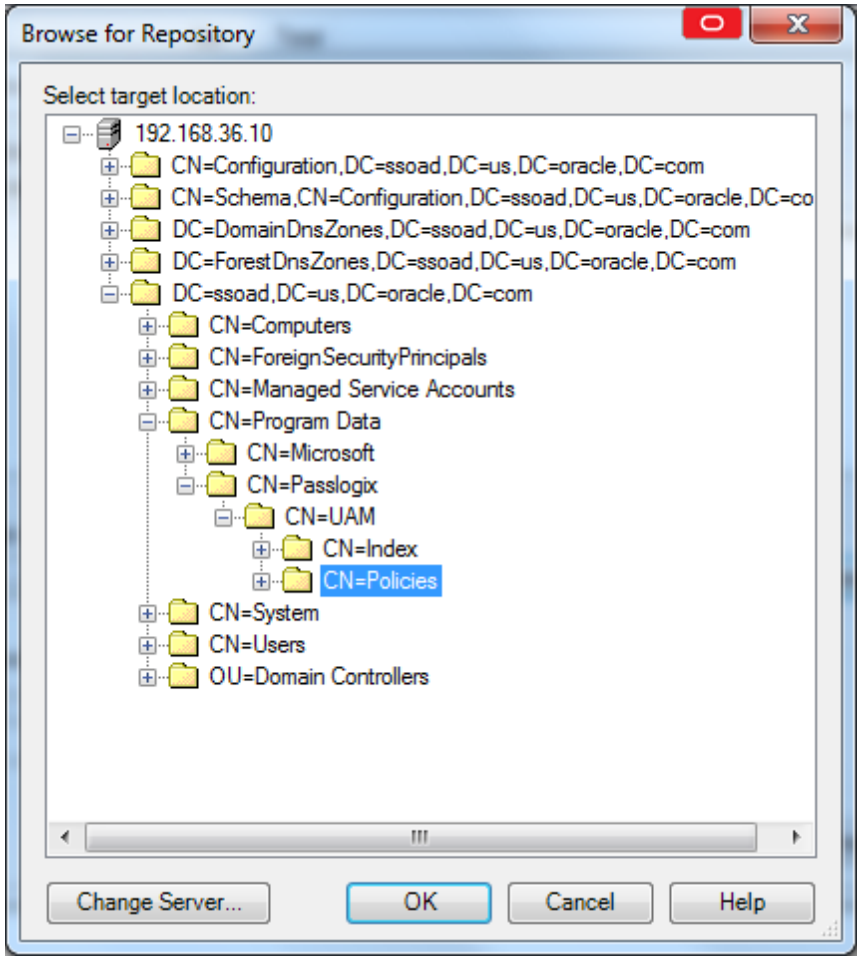
6. Repeat step 5 for any additional users or groups you want to assign to the policy.
7. Publish the policy to the repository.

Publishing a Policy to the Repository

Once you have assigned the desired users and/or user groups to your policy, you can publish it to the repository for propagation to end-user workstations.

To publish a policy to the repository:

1. Launch the Oracle Enterprise Single Sign-On Administrative Console.
2. In the left-hand tree, navigate to **Universal Authentication Manager > Policies**.
3. Right-click the target policy and select **Publish** from the context menu.
4. In the Publish to Repository dialog that appears, do the following:
   a. Ensure that the target policy appears in the "Selected objects to be published" list.
   b. Click **Browse**.
   c. In the repository connection dialog that appears, fill in the required fields and click **OK** to connect.
   d. In the "Browse for Repository" dialog that appears, navigate to and select the Universal Authentication Manager policies container, then click **OK**.

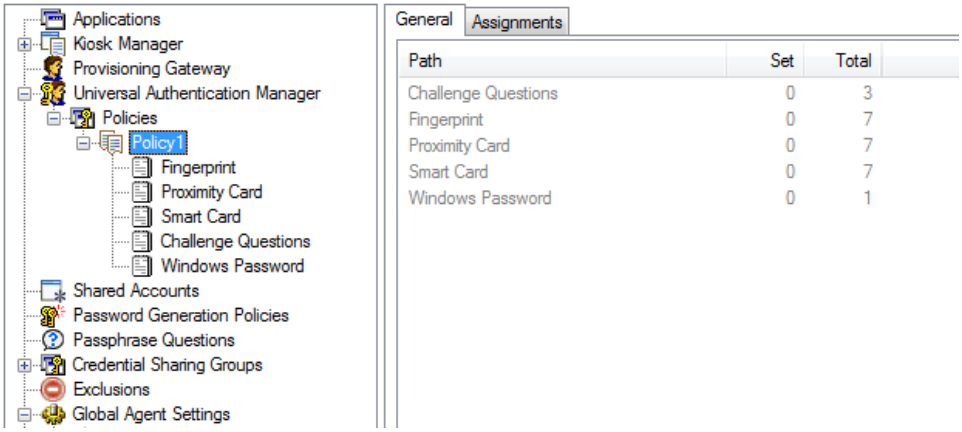


e. Click **Publish**.

Modifying an Existing Policy

To modify the settings for an existing policy that has been published to the repository:

1. Launch the Oracle Enterprise Single Sign-On Administrative Console.
2. In the left-hand tree, right-click the **Repository** node and select **Connect To** from the context menu.
3. In the "Connect to Repository dialog," enter the necessary information and click **OK** to connect. The contents of your repository appear in the right-hand pane.
4. In the right-hand pane, navigate to your Universal Authentication Manager policies container. By default, the path to this container is CN=Program Data, CN=Passlogix, CN=UAM, CN=Policies.
5. Expand your policies container, right-click the desired policy, and select Bring to Console from the context menu. The policy appears under the **Universal Authentication Manager > Policies** node in the left-hand tree.
6. In the left-hand tree, navigate to **Universal Authentication Manager > Policies** and double-click the desired policy.



7. Make your changes in the **General** and **Assignments** tabs, as necessary. To modify the settings for a logon method, select that method in the left-hand tree and make your changes in the right-hand pane.
8. When you have made your changes, you must:
   a. Delete the original policy object from the repository as described in Deleting a Policy. (Policy objects in the repository cannot be overwritten, they can only be created and deleted.)
   b. Publish the updated policy object to the repository in place of the old one as described in Publishing a Policy.

Deleting a Policy

To delete a policy from the repository, do the following:

1. Launch the Oracle Enterprise Single Sign-On Administrative Console.
2. In the left-hand tree, right-click the **Repository** node and select **Connect To** from the context menu.
3. In the "Connect to Repository dialog," enter the necessary information and click **OK** to connect. The contents of your repository appear in the right-hand pane.
4. In the right-hand pane, navigate to your Universal Authentication Manager policies container. By default, the path to this container is CN=Program Data, CN=Passlogix, CN=UAM, CN=Policies.
5. Expand your policies container, right-click the desired policy, and select **Delete** from the context menu.
6. In the confirmation dialog that appears, click **Yes**. The policy is deleted from the policies container.

Troubleshooting a Universal Authentication Manager Deployment

This section describes solutions to issues you may encounter when working with Universal Authentication Manager.

Recovery from Deletion of the Service Account

The Universal Authentication Manager service account is used by every Universal Authentication Manager instance on your network to securely access the repository to read and write data. If the service account is deleted or disabled, all instances will fail to synchronize with the repository and users may not be able to log on because the Universal Authentication Manager authentication 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 Universal Authentication Manager 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.

If the service account is deleted, re-create it with a different name, then follow the steps in Initializing Universal Authentication Manager Storage to reconfigure Universal Authentication Manager to use the recreated account.

Authentication Service Repair Error

If you are working in Enterprise mode and your workstation has been configured so that the Universal Authentication Manager authentication service is logged on as the Universal Authentication Manager 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 Universal Authentication Manager authentication service. In the Control Panel, open **Administrative Tools**. Under Services, right-click the **ESSO-UAM Authentication Service** and click **Stop**.
2. Right-click the **ESSO-UAM Authentication Service** and click **Properties**. On the Log On tab, change the **Log On As** value from the Universal Authentication Manager service account user to the local system account.
3. Go to Add/Remove Programs or Programs and Features in Control Panel, run the Universal Authentication Manager installer and select the Repair option to repair the installation.
4. Change the **Log On As** value back to the Universal Authentication Manager Service Account user. In Control Panel, open **Administrative Tools**. Under **Services**, right-click the **ESSO-UAM Authentication Service** and click **Properties**. On the Log On tab, change the **Log On As** value from the local system account to the Universal Authentication Manager service account user.
5. Restart the Universal Authentication Manager authentication service. From the Control Panel, launch Administrative Tools. Under Services, right-click the **ESSO-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 Universal Authentication Manager logon application. If the user then logs on to the workstation with a Windows password, they will not be prompted to enroll any logon methods. The user sees no PIN prompt or error message. However, users will see the Universal Authentication Manager 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, 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 Universal Authentication Manager as both a smart card and a proximity card. In this case, Universal Authentication Manager 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.

Ensuring Compatibility with Windows Domain Policies

Windows default domain policies are enforced by Universal Authentication Manager. Universal Authentication Manager 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; Universal Authentication Manager conforms to these policies. For example, if a user's password reaches the maximum password age, Universal Authentication Manager still requires the user to change the password before logon is allowed.

AutoLogon Behavior

Universal Authentication Manager supports AutoLogon. For information on how to configure AutoLogon on an end-user workstation, visit Microsoft Support:

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

Windows Password Logon and Unlock

The Universal Authentication Manager Windows XP logon replicates all native Windows XP password logon and unlock flows.

Windows Password Logon and Unlock Errors

The Universal Authentication Manager 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

Universal Authentication Manager integrates with and enhances the Windows Winlogon mechanism (based on GINA technology in Windows XP and Credential Provider technology in Windows 7 and later). Microsoft Windows and Active Directory include numerous security policies and settings that affect the Windows log on and unlock flows. Once installed, Universal Authentication Manager conforms to all Microsoft Active Directory security policies.

Ensure that security policies are not set to require smart cards for logon. This is because Universal Authentication Manager smart card authentication is not based on the PKI Kerberos authentication required by the Windows Group Policy for mandatory smart card logon. If this policy is enabled, Universal Authentication Manager Windows logon will fail.

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 Universal Authentication Manager logon application requires the user to change the password before permitting a logon.

Universal Authentication Manager Authentication Methods and Lockout

Universal Authentication Manager 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 Universal Authentication Manager logon application tracks and increments failed logon and unlock attempts for all supported methods. Accounts that exceed the account lockout threshold are locked by the operating system.

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 a Universal Authentication Manager 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.

Universal Authentication Manager Registry Settings Reference

This section describes the registry settings governing the behavior of Universal Authentication Manager. They are:

Setting Logon Method Display Order

This feature provides the ability to set the order in which logon methods are displayed in the user interface screens throughout Universal Authentication Manager. These settings are initially configured by the Universal Authentication Manager installer; afterwards, they must be configured directly in the Windows 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 Universal Authentication Manager:

Fingerprint

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

Order REG_DWORD 100
```

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
```

Challenge Questions

HKEY_LOCAL_MACHINE\Software\Passlogix\UAM\Authenticators\{393D4B53-EC46-4A38-9E9E-3D6B5141DD34}

Order REG_DWORD 900

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.

Global Universal Authentication Manager Settings

These are general Universal Authentication Manager application configuration settings that control the behavior of various Universal Authentication Manager 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	SZ	Language	N/A	Preferred UI language (system). Set to name of localized subfolder e.g. "en-US" or "fr-FR", etc. Overridden by the user-level setting in HKCU. If neither is specified, the Windows preferred UI language will be used instead. Warning: This setting is always used at logon.	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM
Framework	General	SZ	Language	N/A	Preferred UI language (user). Set to name of localized subfolder e.g. "en-US" or "fr-FR", etc. Overrides the system-level setting in HKLM. If neither is specified, the Windows preferred UI language will be used instead. Warning: This setting is never used at logon.	HKEY_CURRENT_USER\ SOFTWARE\Passlogix\UAM
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 auditing and debug logging on or off.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix

Target	Category	Type	Name	Values	Description	Path
Framework	Logging	DWORD	SimpleLoggerLevel	Audit - Auditing Events (0), Fatal Errors Only (1), Business Logic Errors (2), Warnings - Recoverable Error Conditions (3), Informational - Business Logic Flow (4), Debug - Extra Debugging Information (5) (default), 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	SimpleLoggerAuditPath	Default is c:\uamadt.txt	Specify audit 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	Regular expression to hide matching log entries by source filename. Default is to show all entries.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix

Target	Category	Type	Name	Values	Description	Path
Framework	Logging	SZ	SimpleLoggerMsgShow	N/A	Regular expression to only show matching log entries by log entry contents. Default is to show all entries.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix
Framework	Logging	SZ	SimpleLoggerMsgHide	N/A	Regular expression to hide matching log entries by log entry contents. Default is to show all entries.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix
Framework	Logging	DWORD	SimpleLoggerRemote	Disabled (0) or Enabled (1)	If enabled, add extra columns for console session ID, remote session state and application vs. service process.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix
Framework	Logging	DWORD	SimpleLoggerFormat	TXT (0) or CSV (1)	Controls how the logging file is formatted. Note: Audit log is always in CSV format.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix
Framework	Communication	DWORD	IpcTimeout	Default is 5000 ms Allowed range is 1-60000 ms	Controls the communication timeouts between Universal Authentication Manager Client Applications and the Universal Authentication Manager 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

Target	Category	Type	Name	Values	Description	Path
Framework	Reauthentication	SZ	Default Authenticator	None (default), Fingerprint, Proximity Card, Smart Card, Challenge Questions, 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	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 0 (sync every time) 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 0 (sync every time) 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

Target	Category	Type	Name	Values	Description	Path
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, Proximity Card, Smart Card, Challenge Questions, Windows Password	Default authenticator to use in preference to remembering the last used method.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\ UAM\Gina
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

Target	Category	Type	Name	Values	Description	Path
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
Smart Card	Microsoft Base CSP Provider	DWORD	Enabled	Enabled (1), or Disabled (0) (default)	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	Microsoft Base CSP Provider	DWORD	SessionKeyUseKeyCipherCerts	Enabled (1) (default), or Disabled (0)	Card PIN mode only. If enabled, use any existing Key Encipher (not Smart Card Usage) certificates and key pairs to wrap session keys.	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\BaseCSP
Smart Card	Microsoft Base CSP Provider	DWORD	SessionKeyUseSmartCardCerts	Enabled (1) (default), or Disabled (0)	Card PIN mode only. If enabled, use any existing Smart Card Usage (subset of Key Encipher) certificates and key pairs to wrap session keys.	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\BaseCSP
Smart Card	Microsoft Base CSP Provider	DWORD	SessionKeyUseEssoKeyPair	Enabled (1), or Disabled (0) (default)	Card PIN mode only. If enabled, generate a custom RSA key pair on each smart card to use to wrap session keys. Card must permit key generation.	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\BaseCSP

Target	Category	Type	Name	Values	Description	Path
Smart Card	Microsoft Base CSP Provider	DWORD	SessionKeyRegenerateEssoKeyPair	Enabled (1), or Disabled (0) (default)	Card PIN type only. If enabled, and using custom ESSO key pairs, delete and replace any existing key pairs during every enrollment.	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\BaseCSP
Smart Card	Microsoft Base CSP Provider	DWORD	SessionKeyEssoKeyPairBits	1024-4096 bits. Default is 2048 bits.	Card PIN mode only. If using custom ESSO key pairs, specify the number of bits to use in the RSA key pair. Card must support bit length.	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\BaseCSP
Smart Card	Microsoft Base CSP Provider	DWORD	SessionKeyPreferSmartCardCert	Enabled (1), or Disabled (0) (default)	Card PIN type only. If enabled, prioritize Smart Card Usage certificates ahead of other Key Encipher certificates. If disabled, use Smart Card Usage as last resort.	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\BaseCSP
Smart Card	Microsoft Base CSP Provider	DWORD	SessionKeyPreferEssoKeyPair	Enabled (1), or Disabled (0) (default)	Card PIN mode only. If enabled, prioritize ESSO key pair creation ahead of using existing certificates. If disabled, use custom key pair only if existing certs not found.	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\BaseCSP
Smart Card	Microsoft Base CSP Provider	DWORD	SessionKeyPromptIfMultipleCerts	Enabled (1) (default), or Disabled (0)	Card PIN mode only. If disabled, choose a certificate at random (will attempt to use newest certificate).	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\BaseCSP
Smart Card	Microsoft Base CSP Provider	DWORD	SessionKeyPromptAlways	Enabled (1), or Disabled (0) (default)	Card PIN mode only. If enabled, always prompt to confirm certificate selection even if only a single certificate is available.	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\BaseCSP

Target	Category	Type	Name	Values	Description	Path
Smart Card	Microsoft Base CSP Provider	DWORD	SessionKeyPromptEssoKeyPair	Enabled (1) (default), or Disabled (0)	Card PIN mode only. If enabled, warn and ask the user to confirm before creating a new ESSO key pair on the card.	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\BaseCSP
Smart Card	Microsoft Base CSP Provider	DWORD	SessionKeyAllowAesKeys	Enabled (1) (default), or Disabled (0)	Card PIN mode only. If enabled, will attempt to create AES-256 session keys (in preference to 3DES keys). Will downgrade to 3DES if card does not support AES.	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\BaseCSP
Smart Card	Microsoft Base CSP Provider	DWORD	SessionKeyAllowDesKeys	Enabled (1) (default), or Disabled (0)	Card PIN mode only. If enabled, will attempt to create Triple DES session keys (only if AES not enabled or not supported).	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\BaseCSP
Smart Card	Microsoft Base CSP Provider	DWORD	StatusDelay	Integer 0-10000 milliseconds. 0 disables updates. Default is 500ms.	Card PIN mode only. Time in milliseconds to display low-level card operation updates. Zero will disable low-level updates.	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\BaseCSP
Smart Card	Microsoft Base CSP Provider	DWORD	SessionKeyCertCheckTime	Enabled (1) (default), or Disabled (0)	Card PIN mode only. If enabled, Universal Authentication Manager will reject certificates that are not yet valid or have expired (which may also invalidate existing enrollments).	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\BaseCSP
Smart Card	Microsoft Base CSP Provider	SZ	SessionKeyCertCheckDll	N/A	Full path to custom certificate checker DLL (implementing ICertificateChecker). By default Universal Authentication Manager accepts all certificates.	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\BaseCSP

Target	Category	Type	Name	Values	Description	Path
Smart Card	Microsoft Base CSP Provider	SZ	SessionKeyCertCheckClsid	Default is {9EC6B854-FCAF-4FC1-99D6-99A7903AA357}	Optional CLSID of Cert Check DLL. If blank, the default value is used.	HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM\Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\BaseCSP
Smart Card	General	SZ	DefaultProvider	N/A	Default CSP provider name to use if smart card is not mapped to any provider. For example, "Microsoft Base Smart Card Crypto Provider". Any value other than the Base CSP provider name will be routed to the configured PKCS#11 provider.	HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix\UAM\ Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}\Settings
Smart Card	PKCS#11 Provider	DWORD	Enabled	Enabled (1), or Disabled (0) (default)	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

Target	Category	Type	Name	Values	Description	Path
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
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)	Smart card enrollment behavior.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\ PKCS#11
Smart Card	PKCS#11 Provider	DWORD	SessionKeyUseCspForPki	Enabled (1) (default), or Disabled (0)	Card PIN mode only. Use CSP instead of PKCS11 module for authentication and PKI-specific operations. Must be supported by middleware.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\ PKCS#11

Target	Category	Type	Name	Values	Description	Path
Smart Card	PKCS#11 Provider	DWORD	SessionKeyUseKeyCipherCerts	Enabled (1) (default), or Disabled (0)	Card PIN mode only. If enabled, use any existing Key Encipher (not Smart Card Usage) certificates and key pairs to wrap session keys.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\ PKCS#11
Smart Card	PKCS#11 Provider	DWORD	SessionKeyUseSmartCardCerts	Enabled (1) (default), or Disabled (0)	Card PIN mode only. If enabled, use any existing Smart Card Usage (subset of Key Encipher) certificates and key pairs to wrap session keys.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\ PKCS#11
Smart Card	PKCS#11 Provider	DWORD	SessionKeyUseEssoKeyPair	Enabled (1), or Disabled (0) (default)	Card PIN mode only. If enabled, generate a custom RSA key pair on each smart card to use to wrap session keys. Card must permit key generation.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\ PKCS#11
Smart Card	PKCS#11 Provider	DWORD	SessionKeyRegenerateEssoKeyPair	Enabled (1), or Disabled (0) (default)	Card PIN mode only. If enabled, and using custom ESSO key pairs, delete and replace any existing key pairs during every enrollment.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\ PKCS#11
Smart Card	PKCS#11 Provider	DWORD	SessionKeyEssoKeyPairBits	1024-4096 bits. Default is 2048 bits.	Card PIN mode only.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\ PKCS#11
Smart Card	PKCS#11 Provider	DWORD	SessionKeyPreferSmartCardCert	Enabled (1), or Disabled (0) (default)	Card PIN mode only. If enabled, prioritize Smart Card Usage certificates ahead of other Key Encipher certificates. If disabled, use Smart Card Usage as last resort.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\ PKCS#11

Target	Category	Type	Name	Values	Description	Path
Smart Card	PKCS#11 Provider	DWORD	SessionKeyPreferEssoKeyPair	Enabled (1), or Disabled (0) (default)	Card PIN mode only. If enabled, prioritize ESSO key pair creation ahead of using existing certificates. If disabled, use custom key pair only if existing certs not found.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\ PKCS#11
Smart Card	PKCS#11 Provider	DWORD	SessionKeyPromptIfMultipleCerts	Enabled (1) (default), or Disabled (0)	Card PIN mode only. If enabled, ask user to choose a certificate if multiple certificates of a single type are detected. If disabled, choose a certificate at random (will attempt to use newest certificate).	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\ PKCS#11
Smart Card	PKCS#11 Provider	DWORD	SessionKeyPromptAlways	Enabled (1), or Disabled (0) (default)	Card PIN mode only. If enabled, always prompt to confirm certificate selection even if only a single certificate is available.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\ PKCS#11
Smart Card	PKCS#11 Provider	DWORD	SessionKeyPromptEssoKeyPair	Enabled (1) (default), or Disabled (0)	Card PIN mode only. If enabled, warn and ask the user to confirm before creating a new ESSO key pair on the card.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\ PKCS#11
Smart Card	PKCS#11 Provider	DWORD	SessionKeyAllowAesKeys	Enabled (1) (default), or Disabled (0)	Card PIN mode only. If enabled, will attempt to create AES-256 session keys (in preference to 3DES keys). Will downgrade to 3DES if card does not support AES.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\ PKCS#11
Smart Card	PKCS#11 Provider	DWORD	SessionKeyAllowDesKeys	Enabled (1) (default), or Disabled (0)	Card PIN mode only. If enabled, will attempt to create Triple DES session keys (only if AES not enabled or not supported).	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\ PKCS#11

Target	Category	Type	Name	Values	Description	Path
Smart Card	PKCS#11 Provider	DWORD	StatusDelay	Integer 0-10000 milliseconds. 0 disables updates. Default is 500ms.	Card PIN mode only. Time in milliseconds to display low-level card operation updates. Zero will disable low-level updates.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\ PKCS#11
Smart Card	PKCS#11 Provider	DWORD	SessionKeyCertCheckTime	Enabled (1), or Disabled (0) (default)	Card PIN mode only. If enabled, Universal Authentication Manager will reject certificates that are not yet valid or have expired (which may also invalidate existing enrollments).	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\ PKCS#11
Smart Card	PKCS#11 Provider	SZ	SessionKeyCertCheckDll	N/A	Full path to custom certificate checker DLL (implementing ICertificateChecker). By default Universal Authentication Manager accepts all certificates.	HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Providers\ PKCS#11
Smart Card	PKCS#11 Provider	SZ	SessionKeyCertCheckClsid	Default is {9EC6B854-FCAF-4FC1-99D6-99A7903AA357}	Optional CLSID of Cert Check DLL. If blank, the default value is used.	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 Universal Authentication Manager 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
Fingerprint	General	SZ	ICO:BiometricAuth:112	N/A	Authenticator Icon (128x128)	HKEY_LOCAL_ MACHINE\SOFTWARE\Passlogix\UAM\Authenticators\{16627EE1-FAE3-43B5-B884-D3661649B97D}\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

Target	Category	Type	Name	Values	Description	Path
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:114	N/A	Authenticator Absent Icon (128x128)	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
Proximity Card	General	SZ	ICO:ProxCardAuth:115	N/A	Authenticator Present Icon (128x128)	HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix\UAM\ Authenticators\{4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}\Branding
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

Target	Category	Type	Name	Values	Description	Path
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:112	N/A	Authenticator Absent Icon (128x128)	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
Smart Card	General	SZ	ICO:SmartCardAuth:113	N/A	Authenticator Present Icon (128x128)	HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix\UAM\ Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}\Branding
Challenge Questions	General	SZ	ICO:PassphraseAuth:101	Challenge Questions	Authenticator Name	HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix\UAM\ Authenticators\{393D4B53-EC46-4A38-9E9E-3D6B5141DD34}\Branding
Challenge Questions	General	SZ	ICO:PassphraseAuth:103	N/A	Authenticator Icon (24x24)	HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix\UAM\ Authenticators\{393D4B53-EC46-4A38-9E9E-3D6B5141DD34}\Branding
Challenge Questions	General	SZ	ICO:PassphraseAuth:105	N/A	Authenticator Icon (48x48)	HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix\UAM\ Authenticators\{393D4B53-EC46-4A38-9E9E-3D6B5141DD34}\Branding
Challenge Questions	General	SZ	ICO:PassphraseAuth:106	N/A	Authenticator Icon (128x128)	HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix\UAM\ Authenticators\{393D4B53-EC46-4A38-9E9E-3D6B5141DD34}\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

Target	Category	Type	Name	Values	Description	Path
Windows Password	General	SZ	ICO:WinPwdAuth:105	N/A	Authenticator Icon (128x128)	HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix\UAM\Authenticators\{0C29417D-8A20-48B7-8CC4-D948D384E9B2}\Branding