Oracle® Fusion Middleware

Administering Oracle Enterprise Single Sign-On Suite

11g Release 2 (11.1.2.3)

E54937-01

April 2015

ORACLE®

Oracle Fusion Middleware Administering Oracle Enterprise Single Sign-On Suite, 11g Release 2 (11.1.2.3)

E54937-01

Contents

3   Configuring an Agent Deployment with Anywhere

4   Using the Administrative Console to Configure Password Reset

5 Configuring Strong Authenticators with Universal Authentication Manager

6 Using the Administrative Console to Configure the Reporting Client

7   Reference

8   Troubleshooting

Preface

The *Oracle Fusion Middleware Enterprise Single Sign-On Administrator's Guide* explains how to use the Oracle Enterprise Single Sign-On Administrative Console (hereafter referred to as the Administrative Console) to configure your enterprise's system and Oracle Client applications so that users can manage their passwords effectively.

The Administrative Console lets you configure the following Client applications:

- Oracle Enterprise Single Sign-On Logon Manager (Logon Manager) with Kiosk Manager.
- Oracle Enterprise Single Sign-On Password Reset (Password Reset).
- Oracle Enterprise Single Sign-On Universal Authentication Manager

Additionally, this guide contains instructions for:

- Creating and deploying Oracle Enterprise Single Sign-On Suite using Oracle Enterprise Single Sign-On Anywhere (Anywhere).
- Configuring the Oracle Enterprise Single Sign-On Suite Reporting service to generate reports about virtually all the day-to-day activities of your enterprise.

Finally, this guide provides brief descriptions of the integration of the administrator tasks associated with Provisioning Gateway. See the separate administrator's guide for complete instructions.

Audience

This guide is intended for experienced administrators responsible for the planning, implementation and deployment of Logon Manager. Administrators are expected to understand single sign-on concepts, such as password policies, logon methods, credential sharing groups, and application configuration, as well as have familiarity configuring directory servers, databases and repositories. The person completing the installation and configuration procedure should also be familiar with the company's system standards. Readers should be able to perform routine security administration tasks.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

For more information, see the following documents in the Oracle Enterprise Single Sign-On Suite documentation set:

- *Release Notes*
- *Oracle Enterprise Single Sign-On Suite Installation Guide*
- *Oracle Enterprise Single Sign-On Suite Administrator's Guide*
- *Oracle Enterprise Single Sign-On Suite Secure Deployment Guide*
- *Oracle Enterprise Single Sign-On Suite User's Guide*
- *Deploying Logon Manager with a Directory-Based Repository*
- *Configuring and Diagnosing Logon Manager Application Templates*
- *Oracle Enterprise Single Sign-On Provisioning Gateway Administrator'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.

1

Introduction to Oracle Enterprise Single Sign-On Suite

Oracle Enterprise Single Sign-On Suite is a comprehensive solution for managing enterprise users' password and strong authentication activities for applications that they use for daily productivity, while requiring that they remember only one universal password.

1.1 Suite Components

The suite consists of the following components.

1.1.1 Logon Manager

Logon Manager provides users with one password to log on to every application on both the company network and the Internet. It works "out-of-the-box" (without programming or additional network infrastructure) with virtually any Windows, Web, proprietary, or host-based application, lowering IT and Help Desk costs without the expense and burden of integration.

Logon Manager is intelligent agent software that works by responding to logon requests on behalf of the user, directly from the desktop. The Agent responds to each software applications logon request by providing the correct credentials (that is, username/ID, password, and other fields) directly and automatically. A strong authentication mechanism controls access to the Agent, ensuring access by only the designated user.

Kiosk Manager, a feature that is configurable from the Administrative Console, provides a group of settings that deliver a secure, easy to use, and easy to administer solution to address the needs of traditional single sign-on in a kiosk environment. Kiosk Manager has a client-side agent that suspends or closes inactive sessions and seamlessly shuts down all applications. This feature integrates with Logon Manager and Universal Authentication Manager to provide user identification to the kiosk with a Windows password or any supported primary authenticator.

1.1.2 Password Reset

Password Reset enables workstation users to reset their own Windows domain passwords without the intervention of administrative or help-desk personnel. It provides end users with an alternative means of authenticating themselves by taking a quiz comprising a series of passphrase questions.

Each question is weighted with point values. As the end user answers the quiz questions, Password Reset keeps a running score. Points are added to the score for

each correct response and deducted for each incorrect response. When the end user accumulates sufficient points to meet a preset "confidence level," Password Reset permits the end user to select a new password. If the end user's score does not achieve the required confidence level after all questions have been presented, or if it falls below a preset negative value, the quiz ends and the end user is not permitted to reset the password.

The reset service is available to each end user upon completion of a one-time Enrollment Interview to record passphrase answers. The Administrative Console provides easy configuration of the Enrollment Interview and Reset Quiz, including question text, point values, and confidence-level limits. The console also lets you generate reports of enrollment and reset activity and status.

1.1.3 Provisioning Gateway

Provisioning Gateway provides the ability to remotely add, modify, and delete application credentials directly within each user's Logon Manager credential store, eliminating the need for local credential capture and granting the user instant access to the target application. The Provisioning Gateway Management Console is a standalone, browser-based application. See the separate *Provisioning Gateway Administrator's Guide* for instructions to configure and use this component.

1.1.4 Anywhere

Anywhere provides portable single sign-on (SSO) technology, enabling deployment of Logon Manager and Provisioning Gateway to end users' desktops.

Using the Anywhere Console, the administrator creates a deployment package configured with the Oracle products needed by users of an enterprise, making the package available over a Web server or file share. Users download this deployment package from an HTML interface that is included with the Anywhere package, and which the administrator customizes. Users can then perform installations of the Oracle Enterprise Single Sign-On Suite on their own workstations at the click of a button, with assurance that configurations are correct and ready to run, and without administrator intervention.

1.1.5 Universal Authentication Manager

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. Universal Authentication Manager offers five built-in and configurable authentication methods: smart cards, passive proximity cards, biometric fingerprint and other biometric technologies, and challenge questions. Native Windows passwords are also supported.

1.1.6 Reporting

The Oracle Enterprise Single Sign-On Suite components include a configurable Reporting tool. This tool integrates with Oracle Business Intelligence Publisher to produce customized reports for virtually any event that occurs in the course of regular business operation.

1.2 Suite Administration

Logon Manager, Password Reset, and Universal Authentication Manager settings are configured through the Administrative Console. Anywhere and Provisioning Gateway have standalone administrative consoles. Each component contains its own Reporting settings.

1.3 Overview of the Administrative Console

The Administrative Console incorporates administrative functionality for Logon Manager and Password Reset enables both Agent/Client and server configuration of most options, including:

- Easy creation, management, and deployment of:
  - Application configurations and application configuration lists.
  - Credential sharing groups.
  - Password policies.
  - Bulk-add lists.
  - Agent configuration settings.
  - Customized MSIs.
- Easy setup and management of synchronizer extensions:
  - LDAP Directory Servers, including Oracle Directory Server Enterprise Edition, Oracle Internet Directory, Oracle Unified Directory, Oracle Virtual Directory, Tivoli Directory Server, Novell eDirectory, OpenLDAP Directory Server, and Siemens Dirx.
  - Relational database systems, including Oracle, Microsoft SQL Server, and IBM DB2.
  - Microsoft Active Directory Server systems (including Application Mode).
  - File systems.
- Easy setup of self-service password reset, including:
  - Configuring service storage.
  - Tracking which users have enrolled and/or attempted to reset their passwords.
  - Creating questions for the Enrollment Interview and assigning their point values for the Reset Quiz.
  - Customizing the user interface for the Enrollment Interview and Reset Quiz.
- Easy configuration and management of users authenticating in kiosk environments.
- Easy integration of Reporting with Oracle Business Intelligence Editor to generate reports for every type of event that might occur in the course of regular business operation.

The Administrative Console obsoletes the need for editing configuration files or the registry by hand, with the associated risks of errors such as "fat-fingering" or providing invalid parameters.

The Administrative Console functionality is divided into the areas listed below, with their associated topics.

Task	Console Feature	Related Topics
Creating and managing application configurations	Applications	Creating and Using Templates
Troubleshooting templates	Template Test Manager	Testing Templates
Creating and managing password generation policies	Password Generation Policies	Setting Password Policies
Creating and managing passphrase sets	Passphrase Questions	Using Passphrase Sets
Creating and managing credentials	Credential Sharing Groups	Creating Credential Sharing Groups
	Delegated Credentials	Delegated Credentials Tab (for a Selected Application)
Creating and managing bulk-add lists	Applications > Bulk-Add tab	Bulk Add Tab (for a Selected Application)
Creating and testing Agent configuration settings	Global Agent Settings, Configuration Test Manager	Configuring the Agent with Global Agent Settings
		Using the Configuration Test Manager
Setting up and managing synchronizer extensions	Synchronization	Synchronization
Setting up and managing repositories	Repository	Repositories
Generating MSIs	MSI Generator	Using the MSI Generator
Configuring user authentication in a kiosk environment	Kiosk Manager	Using Kiosk Manager
Creating the Password Reset service	Password Reset	Configuring the Reset Service Account
Creating and configuring questions for a user-initiated password reset	Password Reset	Setting Up the Enrollment Interview
Working with the Reset service	Password Reset Service	Configuring Reset Authentication
Configuring a database for Reporting	Oracle Reporting tool	Oracle Database Configuration Overview
		Microsoft SQL Server Configuration Overview
Integrating Reporting with Oracle Business Intelligence Publisher to create reports	Oracle Reporting tool	Configuring Oracle Business Intelligence Publisher

1.4 Administrative Console Menu Commands for Logon Manager

The following table describes the commands available on the Administrative Console main menu and the corresponding keyboard and mouse shortcuts.

File   Edit   Insert   Repository   Tools   Help

Menu	Command	Description	Shortcut
File	New	Start a new configuration	Ctrl+N
	Open	Open	Ctrl+O

Menu	Command	Description	Shortcut
	Merge	Merge current configuration (applications, password generation policies, credential sharing groups) with a configuration file. **Note:** If the merged file contains items with the same names as those in the current configuration, the Import/Merge Conflict dialog opens. Select the items to import and click **OK**. If the imported file contains a set of Global Agent Settings with the same name as an existing set in the current configuration, the imported set is named *Copy of existing settings*.	
	Save	Save the current configuration to a file (XML).	Ctrl+S
	Save As	Save a copy of the current configuration to a different file.	
	Import	Import configuration from an administrative override object (INI) file or a registration entries (REG) file as a new set of Global Agent Settings. **Note:** If the imported file contains items (applications, policies, groups) with the same names as those in the current configuration, the Import/Merge Conflict dialog appears.	Perform one of these actions: ■ Right-click **Applications** and choose **Import**. ■ Press **Ctrl+I** **Note:** Choose **Import from HKLM** to import Global Agent Settings from the local-machine registry to the Administrative Console as a set named *Live*.
	Export	Export selected applications and all password policies and groups to an entlist.ini file, which is a store of application logons.	Perform one of these actions: ■ Right-click **Applications** and select **Export**. ■ Press **Ctrl+E**.
	Exit	Quit the program.	

Menu	Command	Description	Shortcut
Edit	Delete	Delete the item selected in the left pane. Click **Yes** to confirm or **No** to cancel.	**Del**

Menu	Command	Description	Shortcut
Insert	Application	Add a new application configuration; displays the Add Application dialog.	Right-click **Applications** and select **New Windows App**, **New Web App**, or **New Host App**.
	UAM Policy	Add a new UAM policy; displays the New UAM Policy dialog.	Right-click **Policies** and select **New Policy**.
	Password Generation Policy	Add a new password generation policy; displays the Add Password Policy dialog.	Right-click **Password Generation Policy** and select **New Policy**. Then enter a Policy Name and click **OK**.
	Passphrase Questions	Add a new passphrase set; displays the Add Passphrase Set dialog box.	Right-click **Passphrase Questions** and select **New Passphrase Set**. Then enter a Passphrase Set Name and click **OK**.
	Credential Sharing Group	Add a new credential sharing group; displays the Add Sharing Group dialog.	Right-click **Credential Sharing Group** and select **New Group**. Then: ■ Enter a Group Name and click **OK**. ■ Enter a Policy Name and click **OK**.
	Exclusion List	Add a new exclusion list; displays the Add Exclusion List dialog.	Perform one of these actions: ■ Select the **Exclusions** node in the left pane, and click **Add** at the bottom of the right pane. ■ Right-click the **Exclusions** node, and select **New List** from the contextual menu. ■ Select the **Exclusions** node and right-click in the empty space in the right pane. Then enter a name for the list and click **OK**.

Menu	Command	Description
Repository	Extend Schema	Connect to synchronization repository and create a new synchronization schema (for LDAP and database sync support). Displays the Connect to Repository dialog.
	Initialize UAM Storage	Create static repository containers in which to store Universal Authentication Manager data.
	Use Short Names	Check or uncheck to toggle between displaying and hiding user credential containers in the repository.
	Show User Credential Containers	Check or uncheck to toggle between displaying and hiding Logon Manager user credential containers in the Repository window tree view.

Menu	Command	Description
Tools	Publish to Repository	Opens the Publish to Repository dialog, from which you can select multiple objects to publish simultaneously.
	Export Apps to Agent	Add the application logons in the current Administrative Console session to the list of pre-configured logons for the locally-installed Agent. This option updates the local entlist.ini file, and optionally, the ftulist.ini (first time use) file.
	Write Global Agent Settings to HKLM	Export Global Agent Settings to local machine registry; displays a confirmation message.
	Test Global Agent Settings	Launch the Oracle Test Manager to validate that you have configured Global Agent Settings correctly. See Using the Configuration Test Manager for complete procedures for using this tool.
	Manage Templates	Create, modify, and remove templates for application logons; displays the Manage Templates dialog.
	Update Applications	Update applications based on templates that have been modified since the application's creation; displays the Update Applications dialog.
	Modify Configuration	View or edit the configuration (INI) files for the locally-installed Logon Manager Agent. Choose Applist, or open any FTUList, EntList, MfrmList, or other INI file by name.
	Generate Customized MSI	Launch the Oracle MSI Generator, a wizard-style utility with which you create a custom .MSI file to use for mass deployment to Logon Manager end-users.

1.5 Administrative Console Menu Commands for Password Reset

The table below describes the menu structure and available commands of the Password Reset node of the Administrative Console.

> **Note:**   In order for your new settings to take effect, you must click the **Submit** button at the bottom of each settings tab.

Tree Head	Tab	Description
Password Reset	Admin Web Service URL	Connect to the administrative Web service. After you enter a valid URL, the nodes below become available.

Node	Tab	Description
System	Storage	Configure, prioritize, and initialize storage.
	Reset Service	Monitor and configure reset service accounts.

Node	Tab	Description
Settings	Settings	Configure: ■ Authentication thresholds. ■ Reset lockout. ■ Forced enrollment. ■ User Emails. ■ Reset experience.
	Password Complexity	Configure: ■ Length and repetition constraints. ■ Allowed alphabetic characters. ■ Allowed numeric characters. ■ Allowed special characters.
	Alerts	Configure: ■ E-mail settings. ■ Alert conditions.
	Logging	Configure: ■ Syslog enabling. ■ Event filters.
	Reporting	Configure: ■ Reporting settings. ■ Database settings.
	Enrollment UI	Configure the look and feel of the elements in the Enrollment User Interface, including: ■ Logos. ■ Fonts. ■ Background, border, and foreground colors.
	Reset UI	Configure the look and feel of the elements in the Reset User Interface, including: ■ Logos. ■ Fonts. ■ Background, border, and foreground colors.

Node	Tab	Description
Questions	System Questions	Create system questions and specify the languages in which they will appear.

Node	Tab	Description
Users	Manage Users	Perform user searches using the criteria you specify on this tab.

Node	Tab	Description
Enrollments	Manage Enrollments	Perform enrollment searches based on specified dates; view, export and delete logs.

Node	Tab	Description
Resets	Manage Resets	Perform reset searches based on specified dates; view, export and delete logs.

2

Using the Administrative Console to Configure Logon Manager

This section describes the procedures and settings in the Administrative Console, and how to use them to configure repositories, connections, and Logon Manager for your end-users.

In this chapter, you will learn about the following:

2.1 Overview

Logon Manager uses a patented process for detecting requests for credentials, analyzing the response necessary, responding reliably, logging events, and administering settings.

2.1.1 Architecture/Modules

The Logon Manager component architecture provides maximum flexibility to meet your organization's needs.

The Logon Manager architecture consists of seven areas:

- Authentication
- Encryption
- Intelligent Agent Response
- Core (Including Storage)
- Credential Synchronization
- Event Logging
- Miscellaneous Components

In addition, administration is facilitated by the Administrative Console.

2.1.1.1 Authentication

Authentication is how the system validates users to gain access to Logon Manager. It consists of three layers:

- The authenticator itself
- The authentication service
- The Logon Manager Authenticator API

After the system validates the user, it passes the users validation information to the core shell.

Logon Manager ships with these authenticators:

- Windows Domain (same password used to log on to the network (deprecated as of version 11.1.2)
- Windows Authentication v2
- LDAP Directory Server
- LDAP Directory Server v2
- Authentication Manager
- Entrust Entelligence
- Proximity Card
- Read-Only Smart Card
- RSA SecurID
- Smart Card

You determine which authenticators to support, which to install on each computer, and which to enable for each user. (Default: Windows Domain installs.)

For details, see Configuring the Agent for Windows Authentication.

2.1.1.2 Encryption

Encryption secures user credentials in the data store. The Agent requests that credentials be encrypted/decrypted based on the appropriate Crypto Library algorithm. The Agent automatically migrates credentials to a new algorithm/strength (for example, from Triple-DES to AES).

Logon Manager supports a variety of encryption algorithms and algorithm strengths to suit your corporate, legal, security, performance, and other requirements. The product ships with these popular algorithms:

- AES (MS CAPI) (Default)

- Cobra 128-bit (deprecated)

- Blowfish 448-bit (deprecated)

- Triple-DES 168-bit (deprecated)

- AES 256-bit (deprecated)

- Triple-DES (MS CAPI) (ALL OSs) (deprecated)

- Triple-DES (MS CAPI) (XP/2003 only) (deprecated)

- RC-4 (MS CAPI) (ALL OSs) (deprecated)

- RC-4 (MS CAPI) (XP/2003 only) (deprecated)

Other algorithms can work as encryption modules.

You determine which encryption algorithms a user can use and which encryption new/modified credentials should use.

> **Note:**   As of version 11.1.2, all encryption algorithms are being deprecated in favor of AES (MS CAPI). Other algorithms are listed for upgrade scenarios only.

For details on setting the default algorithm and strength, see the Global Agent Security Settings.

2.1.1.3 Intelligent Agent Response

When an application presents a request for credentials, the Agent detects this event, determines the appropriate action, and responds with the correct credentials. The interface that performs these evaluations is the Intelligent Agent Response. It interfaces with Access Manager to supply the proper credentials to each application. Access Manager acquires the credentials from the Shell.

Windows support installs automatically. You determine whether to install support for Web and/or Host applications. (Default: All modules install, but Host support is disabled.) Logon Manager supports many host emulators. You determine which, if any, the Agent will recognize. (Default: The Agent works with all supported emulators but requires emulator configuration for some emulators.) Oracle recommends that you configure host emulators to work with the Agent before deploying Logon Manager.

For more information on adding additional application configurations, see Creating and Using Templates. For more information on host emulators, see Section 7.2.4, "Configuring Host Emulators."

Logon Manager ships with the configuration information for popular applications built in. It can work with its default installation settings; however, you have the flexibility to tailor its functionality to the specific needs of any organization. Some of the most commonly-customized functions are:

- **Application Templates**, which improve usability by letting users select from a predefined logon list. Applications include Windows applications, host applications, and Web applications.

- **Mobility Support**, to provide location transparency and automatic backup and restore.

- **Event Logging**, which enables Logon Manager to log various events such as logons, password changes, and so on.

- **First-time use**, which customize the user setup process to meet an organizations needs and improve usability.

- **Password policies**, which propagate enterprise security policies, improve security, and (when automated) improve usability.

- **Logon Manager settings**, which control the UI, implement security, enable, disable, and configure features, and more.

Each of these customization decisions impacts multiple stages of planning, deployment, use, and management.

2.1.1.4 Core (Including Storage)

Using your preferred encryption algorithm, the Agent encrypts and stores user credentials locally in the encrypted Local Credential Storage; it never maintains credentials unencrypted on disk or in memory. The credentials are stored in a user-specific secure database file. Within this file are the encrypted records for each set of user credentials, user settings, and additional configuration information.

2.1.1.5 Credential Synchronization

While the Agent stores user credentials and settings locally, it can synchronize the credentials and settings with remote file systems, directories, databases, devices, and so on. Synchronization can be of the entire user database file (which contains all user credentials) or of individual records within the database. The synchronization is triggered by a change to the Local Credential Storage or settings. Synchronization can be extended to any storage mechanism via the Synchronization API.

Agent administration is fully supported via the Synchronization component and allows the administrator to dynamically deliver updated settings and configuration data to the Agent through the central storage mechanism.

The Agent works with a variety of synchronization extensions, providing users access to their credentials from any desktop, and includes the following:

- Microsoft Active Directory

- Microsoft Active Directory Lightweight Directory Services (AD LDS), formerly Microsoft Active Directory Application Mode (ADAM), hereafter referred to as Microsoft AD LDS (ADAM)

- Lightweight Directory Access Protocol (LDAP)

- Database

- File System

Logon Manager supports the most popular LDAP-compliant directory servers, including:

- Oracle Directory Server Enterprise Edition

- Oracle Internet Directory

- Oracle Unified Directory

- Oracle Virtual Directory

- IBM Tivoli Directory Server

- Microsoft Active Directory Server

- Novell eDirectory

- OpenLDAP Directory server

- SQL-compliant relational database system, including:

    - Oracle Database

    - Microsoft SQL Server

    - IBM DB2

    Note: For information about required and supported versions, see the product certification matrix.

Logon Manager also includes a synchronizer extension supporting a file system, such as can be found on a remote network drive share.

You determine which synchronization modules to install on each computer, which modules to enable for each user, and how to configure each extension. (Default: The synchronizer module installs but no synchronization extensions install.) See the following sections for more information about each feature:

- Mobility Configuration

- Storing User Data

- Directory Server Synchronization Support

- File System Synchronization Support

- Database Synchronization Support

2.1.1.6 Event Logging

When notified by the Shell, the Agent can log all SSO system events, including credential use, credential changes, global credential events, Agent events, and Agent feature use. The Agent can also log specified fields. Events can be logged locally or to any external destination through the Event Logging API. These destinations can include an SNMP service, a Windows server (for viewing via the Windows Event log), or even a local XML log file for simplified parsing and reporting.

The Agent can log all events through its Event Logging API.

Logon Manager works with a variety of Event Logging extensions and includes two Event Logging extensions writing to both local and remote servers:

- Local File extension, to an XML file

- Windows Event Logging extension, to a Windows Event Logging server

- Logging events to a database

- Logging events to a Syslog server

Oracle may release additional extensions (for example, Oracle and SNMP), and you can easily write your own extensions.

You determine which Event Logging modules to install on each computer, which modules to enable for each user, how to configure the extensions, how frequently the Agent writes to these extensions, how much data the Agent caches, where the Agent writes the log, and more. (Default: No Event Logging modules install, and no logging occurs)

See Event Logging for details.

2.1.1.7 Miscellaneous Components

Logon Manager also contains the following miscellaneous modules:

- **Backup/Restore.** For users who do not perform any Credential Synchronization, the Backup/Restore component enables archiving and restoration of user credentials.

- **Citrix and Windows Terminal Services Tools.** For environments that require using the Agent within a Citrix Server or Windows Terminal Services environment, additional components are supplied to allow Logon Manager to interact appropriately within each session.

- **Installer Package.** Logon Manager ships within a Windows Installer package that supports the flexibility of that technology for easier deployment and customization.

2.1.2 Common Scenarios

- **First-Time Use.** The Agent can prompt the user for current credentials for predefined applications. You determine which, if any, credentials to request. (Default: The Agent does not request credentials for any applications.)

  For more information, see Bulk-Adding Applications for First-Time Use.

- **User Work Modes.** Logon Manager supports work modes ranging from One Workstation, One or Multiple Users to Frequent Movement Among Many Workstations and from always-connected to frequently-disconnected.

  For more information, see User Work Modes.

- **Usability vs. Security.** Logon Manager lets you choose the balance between usability and security that is appropriate for your organization. The default configuration guarantees your enterprise is secure, but you have the flexibility to adjust these settings as you need. See the *Oracle Enterprise Single Sign-On Suite Secure Deployment Guide* for a complete discussion of Oracle's security recommendations.

  For more information, see Global Agent Settings for User Experience.

- **Packaging/Distribution/Installation.** Logon Manager supports most deployment tools and methods. You determine which components deploy to which desktops.

  For more information on deployment, see Deploying Logon Manager.

2.1.3 Resources

Logon Manager stores all program files, settings, and data in the following places:

- The `%ProgramFiles%\Passlogix\v-GO SSO` directory contains Logon Manager program files. (Default: `C:\Program Files\Passlogix\Logon Manager`).

- The `%ProgramFiles%\Passlogix\v-GO SSO\Console` directory contains Administrative Console program files. (Default: `C:\Program Files\Passlogix\v-GO SSO\Console`).

- The `%ProgramFiles%\Passlogix\SSO File Sync Service` directory contains SSO File Sync Service program files. (Default: `C:\Program Files\Passlogix\SSO File Sync Service`).

- The `%AppData%\Passlogix` directory contains user data files. (Default: depends on OS; Windows 7: `C:\Users\%Username%\AppData\Roaming\Passlogix`).

- The `HKCU` registry tree stores user default settings.

- The `HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix` registry tree stores overriding setting (settings that override user settings) and Logon Manager defaults.

- The `vGOLocator` objects on a directory server point Logon Manager to where each users' credentials are stored (in `vGOConfig` object).

- The `vGOConfig` objects on directory servers and similar objects on File Systems store overriding settings and user data.

> **Note:** Settings in `vGOConfig` objects override registry settings. `vGOConfig` is the default name, but this file can have any name.

2.2 Logon Manager Features

Logon Manager supports your enterprise users' secure single sign-on requirements with the following key features:

Feature	Benefits
Single Sign-On	Requires one password to log on to networks, applications, and Web sites.
Authenticator Choice	Authenticate using a Windows logon or LDAP Directory Server logon. Logon Manager accepts strong authenticators for its primary authentication - including smart cards.)
Mobility Support	Users can log on from any workstation and use their Logon Manager credentials via directory servers, database systems, file systems, and Windows Roaming Profiles. (Logon Manager users can log on using smart cards.)
Workstation Sharing	Multiple users can share the same workstation securely using Kiosk Manager.
Automated Password Change	Users can choose a new password or the Agent can select one automatically using approved password rules (Password Policies).
Strong Authentication	Soft-token based, two-factor authentication protects against unauthorized access.
Event Logging	Automatically log events such as logons, password changes, and so on.
Auto Prompt	Automatically prompts users to configure logons when they encounter a new password-protected application.

Feature	Benefits
Credential Sharing	Multiple applications can share the same credentials.
Central Administration	All configurations and settings are centrally manageable through the Administrative Console.
Automatic Backup/Restore	Automatically back up user credentials to a remote location including a directory server, relational database, or file system, and automatically restore user credentials after a system crash.
User Configuration of Logons	In addition to logons predefined by the administrator, users can add individual logons that they may have to other applications and Web sites.
Customization	Many aspects of the user experience, including user setup, are customizable to tailor the product to the security needs of the organization and technical sophistication of the user population.
Secure Architecture	The Agent is designed to be highly secure, including allowing the Administrator to prevent revealing of any passwords, calling modern encryption algorithms, and using tamper-resistant modules.

2.3 Considerations Before Deploying Logon Manager

The topics in this section discuss important concepts and considerations regarding the deployment and administration of Logon Manager.

Concept	Purpose
User Work Modes	Understanding the different ways to set up the Agent side of supporting users working in different configurations, and how to optimize your configuration for each set of scenarios.
System Configuration	Understanding the different ways to set up the server side of supporting users working in different configurations, and how to optimize your configuration for each set of scenarios.
Software Rollout Basics	Understanding the process and issues surrounding rolling out Logon Manager to an organization.
Administration and Management	Understanding the post-rollout issues for Logon Manager deployments.

2.3.1 User Work Modes

Users access their computers in a variety of work modes:

- Some users are always at a given workstation and are the sole user.

- Some users move frequently among a limited number of workstations (for example, nurses in a department) or move to a different workstation every day or few hours (for example, a call center).

- Multiple users may share a single workstation, for example, in shifts. Such a workstation may be used as a kiosk, that is, by multiple users who log on on using a smart card or other token.

- Some users are not always connected to the network.

Logon Manager supports all these scenarios and can be optimized for each user's most common scenario. (Default: Users are always at a given workstation, but share with others.)

2.3.1.1 One Workstation, One User

When users are always at a given workstation, their credentials can be backed up to a remote location using an SSO synchronizer extension. See Synchronization for more information.

Alternately, the Backup/Restore facility module can store credentials on the workstation without the use of a remote repository. The Backup/Restore module is not installed by default. Users can perform backups manually, or the backup can be automated. See File-Based Backup/Restore for more information.

2.3.1.2 Frequent Movement Among Few Workstations

When users move frequently among a few workstations, but are always on those few workstations, you have two basic options for supporting their Logon Manager credentials.

The recommended option is to utilize a remote SSO repository. Both starting the Agent and any change to credentials force a record-level comparison (synchronization) of all records, ensuring that the user always has the most current credentials possible.

One other option is to configure Automatic Backup to a network file share. With proper configuration, the Agent will perform a silent backup to a remote store (network drive) with each change of credentials (Refresh Task). When the Agent first starts, it will see if the remote store is newer than the local store; if so, it will perform a silent restore; either way, the user will have the current credentials. Because this is a file-level (as opposed to record-level) comparison, this option is not safe if the user logs onto more than one computer at the same time.

2.3.1.3 Frequent Movement Among Many Workstations

When users move frequently among many workstations, you have two basic options for supporting their credentials.

The recommended option is to utilize a remote SSO synchronization repository. Both starting the Agent and any change to credentials force a record-level comparison (synchronization) of all records, ensuring that the user always has the most current credentials possible. In addition, to increase security and to reduce disk space use, enable the o increase security and to reduce disk space use, enable the **Delete Local Cache (on Shutdown)** option in Global Agent Synchronization Settings.

Alternately, if your Windows environment is already set up with Windows Roaming Profiles, user data is automatically available to the user since it is included in the %AppData% file directory. However, due to the bandwidth-intensive nature of Windows Roaming Profiles, it is not recommended for use with SSO credentials.

2.3.1.4 One Workstation, Many Users

A single workstation may be accessed by a number of users, such as a kiosk. A smart card (or other token) and a PIN can be used to log on to a kiosk (Authentication Manager only). To enable these users' access to the remote SSO repository the ssoSCDetect utility can be used to start the Logon Manager Agent and prompt for primary logon whenever a smart card is inserted in the reader. When the card is removed, the user is automatically logged out of the Agent. See Section 7.2.9, "Smart Card Monitor Utility (ssoSCDetect.exe)" for more information.

2.3.1.5 Disconnected

When users use laptops or are in remote locations, they often stay disconnected from the network for long periods of time.

The Logon Manager Agent stores credentials locally, providing full independence for mobile users who cannot rely on a network connection. Logon Manager modules like Storing User Credentials and Settings (see Storing Credentials in the User Object) and Event Logging support occasional reconnecting, ensuring reliability.

With File-Based Backup/Restore, users can save their own data to a floppy or zip drive.

The Logon Manager synchronizer extensions are configured for offline users using Synchronization options, including Disconnected Operation (see Global Agent Synchronization Settings).

2.3.1.6 Security Locked Down vs. User Freedom

You can customize Logon Manager to provide the balance of security appropriate to your organization's policies and risk/trust level. For example, some organizations need to insure that a user cannot deny having taken a given action, whereas others are not as security-conscious. See *Oracle Enterprise Single Sign-On Suite Secure Deployment Guidelines* for a complete discussion of Oracle's security recommendations.

2.3.1.7 Usability: User Flexibility vs. Simplicity

You can customize Logon Manager to provide the balance of usability appropriate to your organization's policies and user skill level. For example, some organizations largely employ users who are confused by all but the simplest user interface, whereas others are staffed by more experienced users and might wish to offer flexibility in their environment.

2.3.1.8 Other Settings

You can customize Logon Manager in many ways, and you can enforce these settings at the user, computer, or group level. (The group level can include the entire enterprise.) See Global Agent Settings in Depth for details.

2.3.1.8.1 Mobility Configuration Some organizations configure their SSO repository components (directory servers, relational databases, file system share) in a very centralized fashion (for example, all user data store objects under one parent object). Other organizations use a decentralized structure (for example, a parent object for each department, location, level of employee). Each has its advantages and disadvantages, depending on your specific current and future network topology. Below are some general advantages and disadvantages.

Centralized

Advantages	Disadvantages
■ Easy to configure globally	■ Hard to load balance
■ Easy to manage	■ Bandwidth-intensive when user population is dispersed and user data isn't locally replicated (for example, retrieving data on a New York server from Tokyo)

Decentralized

Advantages	Disadvantages
■ Granular control (for example, different security for different users)	■ Harder to manage
■ Can reallocate resources easily (for example, move user data objects as the users move closer to different servers, split data among several servers)	■ Easier to make mistakes with one set of data and not realize the disparity

2.3.1.8.2 First-Time Use Scenarios You can control users first-time use scenario from the Logon Manager repository. Determine your first-time use scenarios and then push the object to the Logon Manager repository. If using a centralized environment, only one object is needed; if using a decentralized environment, you can customize the first-time use scenario configuration to meet each group's needs. See Bulk-Adding Applications for First-Time Use for more information.

2.3.2 System Configuration

You can provide Logon Manager configuration settings to users from the Logon Manager repository. Determine your overriding settings and then push them to an object in the Logon Manager repository. If you are using a centralized environment, only one object is needed, providing ideal top-down security controls; if you are using a decentralized environment, you can customize the settings to meet each group's needs.

2.3.2.1 Application Configurations

You can provide application configurations to users from the Logon Manager repository. Determine your application configurations and then push to an object in the Logon Manager repository. If using a centralized environment, you need only one object; if you are using a decentralized environment, you can customize the list of supported applications to meet each groups needs. See Creating and Using Templates for more information.

2.3.3 Software Rollout Basics

You can introduce yourself to Logon Manager by accessing its basic functions; that is, log on to your computer and the Agent provides the logon to all other applications.

To see examples of this, observe the Agent responding to some predefined applications (for example, Microsoft Outlook and Lotus Notes) and some Web sites (for example, Yahoo! and Google.com). Install Logon Manager with its typical configuration and then start these applications.

2.3.4 Administration and Management

After the initial deployment, you can continue managing Logon Manager modules' deployment for updates and upgrades, using the Administrative Console or your own current deployment method.

Logon Manager Configuration

Directory Servers and Database Systems	Using the Administrative Console, modify the `SSOAdminOverride` objects.

Logon Manager Configuration

File Systems	Using your current File System administration/management tool or the Administrative Console modify the overriding settings.
Local	Using a domain management tool, a deployment tool, RegEdit, and so on, modify the HKLM hive.

Application Configuration

Directory Servers and Database Systems	Using the Administrative Console, modify the SSOentlist and (optionally) SSOftulist objects.
File Systems	Using the Administrative Console modify the entlist and (optionally) ftulist files.
Local	Using the Administrative Console, modify the entlist.ini and (optionally) ftulist.ini files.

Settings

Change settings post-rollout	Using the Administrative Console, push overriding settings to the Logon Manager synchronization repository (for example, the directory server, database, file system).
	Using a domain management tool, a deployment tool, RegEdit, and so on, deploy registry changes.

User Data

Directory Services	Using your current directory administration/management tool, move the user object and (if needed) alter or add an SSOLocator object for the user.
File Systems	Using your current network administration/management tool (or even Windows Explorer), move the user file directory tree and (if needed) change the user files' storage location.
Local	Using a domain management tool, a deployment tool, RegEdit, and so on, change the user files' storage location.

Managing User Credentials

Directory Servers	**Deleting User Credentials.** Using your current directory administration/management tool, delete the user object from the directory and delete user credentials by using Windows administrative access to delete the %AppData%\Passlogix file from the user's %AppData%\SSO file directory tree on all computers the user accesses.
	Moving a user object. Using your current directory administration/management tool, move the user object using the directory administrative tool and (if needed) alter or add an SSOLocator object for the user.
File Systems	**Deleting User Credentials.** Using your current network administration/management tool or Windows Explorer, delete the user files from the file system and delete user credentials by using Windows administrative access to delete the %UserName% AML.ini file from the user's %AppData%\Passlogix file directory tree on all computers the user accesses.

Managing User Credentials	
Local	**Deleting User Credentials.** Using a domain management tool, a deployment tool, Windows Explorer, and so on, delete the `%AppData%\Passlogix` file from the user's `%AppData%\SSO` directory on all computers the user accesses.

2.4 Configuring the Server for Logon Manager

The topics below describe how to configure the server for Logon Manager deployment and support for synchronization, and event logging:

- LDAP Directory Server Configuration, including:
  - Oracle Internet Directory
  - Oracle Directory Server Enterprise Edition
  - Oracle Unified Directory
  - Oracle Virtual Directory
  - IBM Tivoli Directory Server
  - Microsoft Active Directory and AD LDS (ADAM)
  - Novell eDirectory
  - Open LDAP Directory Server
  - Siemens Dirx

- File Systems Configuration: for any UNC (Universal Naming Convention)-compliant network drive or device

- Database Synchronization Configuration: for Oracle, Microsoft SQL Server, and IBM DB2 database systems

- Syslog event logging: requires no special configuration of the Agent

2.4.1 LDAP Directory Server Configuration

This section describes how to extend LDAP directory servers to work with Logon Manager. Although this process simplifies some directory-related tasks, it assumes that the administrator has knowledge of the planning and deployment of directory services. This guide only covers concepts specific to Logon Manager deployments.

See Directory Server Synchronization Support for more information about how Logon Manager makes use of directory server resources. Also see *Deploying Logon Manager with a Directory-Based Repository*.

Configuring a directory server for Logon Manager entails using the Administrative Console to extend the schema and set up objects in the directory structure (also see Extending the Database Schema).

When you connect to a directory server, you must provide administrator-privileged authentication information. This information includes the directory type, server name or IP address (IP address may not be valid for Microsoft Active Directory Server), port, SSL-use selection, user ID and password.

Your user ID should be in DN format; for example:

`uid=yourname,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot`

> **Note:** For AD LDS (ADAM) repositories:
>
> The AD LDS (ADAM) server instance must be installed and running before you begin the following procedure.
>
> The naming context for the Application Directory Partition (step 2, below) must be an organization unit (ou). The example given in the AD LDS (ADAM) Setup Wizard panel shows a cn (container name).

1. Extend the directory schema.

   > **Note:** It is considered a good practice to perform a backup of your directory before and after extending the schema. However, it is not necessary to disconnect users to extend the schema, or to reboot the server after the schema is extended.

2. From the **Repository** menu, select **Extend Schema**.

3. In the **Connect to Repository** dialog, enter or select the required connection information, then click **OK**. The Administrative Console binds to the repository, adds attributes and object classes, and confirms successful server configuration.

4. Repeat for each additional server.

5. Create the container object.

   A container object, typically named SSOConfig (class organizationUnit), holds overriding settings and a container object named People. The People container object (class organizationUnit) holds a container object for each user (class SSOUserData, and each of these user container objects holds user credentials and settings (class SSOSecret).

   > **Note:** Use the Administrative Console to create container objects with the proper security, create the People container object with the proper security, and place overriding settings with the proper security in the People container object.

6. In the left pane of the Administrative Console, right-click **Repository** and select **Connect** to from the shortcut menu.

7. Enter or select the required connection information, then click **OK**.

8. In the right pane, navigate to the container object where you will create the People object and overriding settings.

9. If necessary, create a new container object:

   a. Right-click the parent container object, and select **New Container** from the shortcut menu.

   b. Enter a name for the new container object and select it.

   c. Right-click the container object (where the People container object and overriding settings will exist) and choose **Publish to Repository** from the shortcut menu (also see Publishing to the Repository).

   d. Choose the **Data Source** of the overrides and provide the information requested:

o Administrative Console

o Data File

10. When you complete the configuration procedure, the newly-created `People` object and entries for any overriding settings appear in the **Repository** pane. Right-click on any object and choose **Refresh** if necessary.

11. Repeat this procedure for each additional container object.

12. Create locator objects.

   a. In the left pane of the Administrative Console, right-click **Repository** and choose **Connect To…** from the shortcut menu.

   b. Enter or select the required connection information, then click **OK**.

   c. In the right pane, navigate to the container object where you will create the `People` object and overriding setting.

   d. If necessary, create a new container object:

   Right-click the parent container object, and choose **New Container** from the shortcut menu.

   Enter a name for the new container object and select it.

   e. In the right pane, navigate to the container in which you want to add the locator.

   f. Right-click the container and choose **Add Locator Object** from the shortcut menu (also see Adding a Locator Object).

   g. Specify the Locator Name (enter **Default** for all users unless there is one for a specific user).

   h. Navigate to the parent container object of the target `People` container object (or specify its path) and click **OK**. The newly-created `SSOLocator` object appears with the name you specified. Right-click any object and choose **Refresh** if necessary.

   i. Repeat for each additional `SSOLocator` object.

   Note: As described in Directory Structure, Logon Manager looks for an `SSOLocator` object when it connects to the Directory Server, which points to where the Agent can store user credentials. An object named `Default` is required somewhere in the tree. You can create specific `SSOLocatorClass` objects for specific users as needed.

2.4.2 File Systems Configuration

This section describes how to extend File Systems to work with Logon Manager. Although this process simplifies some tasks, it assumes that the administrator has knowledge of the planning and deployment of file system shares. This guide only covers concepts specific to Logon Manager deployments.

Note: See File System Synchronization Support for more information about how Logon Manager makes use of file system resources.

Configuring a File System share for Logon Manager entails using the Administrative Console to set up objects in the directory structure.

> **Note:** When you connect to a File System, you may need to provide Administrator-privileged authentication information. This information includes the synchronizer extension type, UNC path, user ID, and password.
>
> Your user ID should be in domain name format, for example, `yourdomain\yourname`.

2.4.2.1 Creating the Container Object

A container object is typically a file system share in UNC format, for example:

`\\Server\Share`

Or it can be a share with a path, for example:

`\\Server\Share\Path\subPath`

The container object holds overriding settings and a container object named `People`.

- The `People` container object is a file folder that holds a container object for each user (rights: `User=Full; Server\Administrators=Full`),

- Each of these user container objects holds a container object named `SSOUserData`.

- Each `SSOUserData` container object holds user settings in an `SSOSecretData` object (a file) and container objects for each application credential.

- Each of these container objects contains a user's credentials for one application (a file named `SSOSecretData`).

Use the Administrative Console to create container objects with the proper security, to create the `People` container object with the proper security, and to place overriding settings with the proper security in the `People` container object.

1. In the left pane of the Administrative Console, right-click **Repository** and choose **Connect To…** from the shortcut menu.

2. Enter or select the required connection information, then click **OK**.

3. In the right pane, navigate to the container object where you will create the `People` object and overriding settings.

4. If necessary, create a new container object:

   a. Right-click the parent container object, and choose **New Container** from the shortcut menu.

   b. Enter a name for the new container object and select it.

5. Right-click the container object (where the `People` container object and overriding settings will exist) and choose **Publish to Repository** from the shortcut menu (also see Publishing to the Repository).

6. Choose the Data Source of the overrides and provide the information requested:

   - Administrative Console

   - Data File

7. When you complete the configuration procedure, the newly-created `People` object and entries for any overriding settings appear in the **Repository** pane. Right-click on any object and choose **Refresh** if necessary.

8. Repeat this procedure for each additional container object.

2.4.3 Database Synchronization Configuration

This section describes how to configure a relational database server to work with Logon Manager. It assumes that you have basic knowledge of relational database administration and operation. This guide only covers concepts specific to Logon Manager deployments.

> **Note:** See Database Synchronization Support for more information about how Logon Manager makes use of database resources.

Configuring Logon Manager for database synchronization requires using the Administrative Console to extend the database schema and to create the container objects.

1. Extend the database schema.

> **Note:** Perform a backup of your database before and after extending the schema.

   a. Choose **Extend Schema** from the **Repository** menu.

   b. In the **Connect to Repository** dialog, enter or select the required connection information, then click **OK**. You must use administrator-level authentication to connect the Administrative Console to the database server. The Administrative Console connects to the database, creates the necessary objects, and confirms successful configuration.

> **Note:** For SQL Server, when extending the schema, if the database does not exist, the extend schema function will create the database for you. For IBM DB2 Setup instructions, see IBM DB2 Configuration.

2. Repeat for each additional server.

3. Create the container objects.

A container object, typically named `SSOConfig`, holds a default set of overriding settings and a container object named `People`. The `People` container object contains a container object for each user, and each of these user container objects holds user credentials and settings.

Use the Administrative Console to create container objects, to create the `People` container object, and to place overriding settings with the proper security in the `People` container object.

1. In the left pane of the Administrative Console, right-click **Repository** and select **Connect To…** from the shortcut menu.

2. Enter or select the required connection information, then click **OK**.

3. In the right pane, navigate to the container object where you will create the `People` object and overriding settings.

4. If necessary, create a new container object:

   a. Right-click the parent container object, and choose **New Container** from the shortcut menu.

    b. Enter a name for the new container object and select it.

5. Right-click the container object (where the `People` container object and overriding settings will exist) and choose **Publish to Repository** from the shortcut menu (also see Publishing to the Repository).

6. Choose the Data Source of the overrides and provide the information requested:

    ■   Data File

    ■   Administrative Console

7. When you complete the configuration procedure, the newly-created `People` object, and entries for any overriding settings, appear in the Repository pane. Right-click on any object and choose **Refresh** if necessary.

8. Repeat this procedure for each additional container object.

2.4.4 IBM DB2 Configuration

To extend the central repository schema for Logon Manager and prepare IBM DB2 as the central repository, follow the steps in this section.

2.4.4.1 IBM DB2 Setup Requirements

■   You must install the IBM DB2 Client on the local machine.

■   The DB2 client must have OLE DB (Object Linking and Embedding Database) support installed and configured. This support provides a set of interfaces that allow applications to uniformly access data stored in different data sources. To install OLE DB support, run the DB2 setup wizard and navigate to **Client support > Interfaces > OLE DB Support**. See your DB2 documentation for more information.

■   The currently logged-on user (to Windows) who is extending the schema must have the appropriate rights to the database in order to connect to the repository and extend the schema. The DB2 User Account must have "Database Administrator Authority" rights.

■   A DB2 administrator must create a database named "`vGOSSO`."

Refer to the IBM DB2 instructions for detailed information on any of these instructions.

2.4.4.2 Extending the Database Schema

1. Open the Administrative Console.

2. From the **Repository** menu, select **Extend Schema**.

3. From the **Connect to Repository** menu, enter or select the required IBM DB2 connection information:

    ■   **Server name.** Enter the server name.

    ■   **Repository Type.** Select DB2 Database.

    ■   **Port.** The port number needs to be entered only if it is not the default port (normally 50000). If the port is the default, you can leave this field blank.

4. Click **OK**.

> **Note:** You must have administrator-level authentication to connect the Administrative Console to the database server. The Administrative Console connects to the database, creates the necessary objects, and confirms successful configuration.
>
> The Extend Schema function uses the following SQL commands to extend the schema:
>
> CREATE SCHEMA vGOSSO;
>
> CREATE TABLE vGOSSO.SSO_ADMIN (ConfigType VARCHAR(128) NOT NULL, Data CLOB, PRIMARY KEY(ConfigType));
>
> CREATE TABLE vGOSSO.SSO_USERS (UserID VARCHAR(128) NOT NULL, ObjectID VARCHAR(255) NOT NULL, Data CLOB, PRIMARY KEY (UserID, ObjectID));

5. After schema extension, in the DB2 database, grant full rights to SSO_USERS table and its indexes and read-only rights to SSO_ADMIN table and its indexes.

2.4.4.3 Publishing to the Repository

1. In the left pane of the Administrative Console, right-click **Repository** and select **Connect To…** from the shortcut menu.

2. Enter or select the required connection information, then click **OK**.

3. In the right pane, navigate to the root (server name).

4. Right-click on the root and select **Publish to Repository** from the shortcut menu. The People container object will already exist under the root.

5. Choose the Data Source of the Administrative Overrides and provide the information requested:

   - **Administrative Console.** Use this wizard page to export an Agent configuration to a selected synchronizer container using the current Administrative Console settings as the source.

   - **Data File.** Use this wizard page to export an Agent configuration to a selected synchronizer container using one or more data files as the source.

6. When you complete the configuration procedure, entries for any overriding settings appear in the Repository pane. Right-click on any object and choose **Refresh** if necessary.

2.4.4.4 Required Settings for Connecting to IBM DB2 Database

You must set the Required Database Synchronization settings for all database synchronizer extensions.

To add the synchronizer and configure it for IBM DB2:

1. Open the Administrative Console and select a set of Global Agent Settings.

2. Expand **Synchronization > DBExt > Required**.

3. Enter the following information:

   - **Extension location.** Make sure this is checked. It is the `path\filename` of the IBM DB2 database synchronizer extension. Default: `C:\Program Files\LocalDirectory\v-GO SSO\Plugin\SyncMgr\DBEXT\DBExt.dll`)

   - **Servers.** Specify the connection string for the database server in the order to attempt connection for synchronization. Select the checkbox and click the ellipsis ("**...**") button to open the **Edit List** dialog. Enter the full connection string for one database server on each line; end each line by pressing **Enter**. Do not use any other delimiter characters.

     Note: You must specify at least one connection string for the extension to work.

     To connect to an IBM DB2 database, use the following connection string:

     ```
     Provider=IBMDADB2;Data
     Source=vGOSSO;CurrentSchema=vGOSSO;Location=
     <DB2ServerName>[:port];Extended Properties="trusted_
     connection=yes";
     ```

     Where `<DB2ServerName>` is the name of the server and `[:port]` is the optional port.

     ---

4. Expand **Synchronization>DBExt>**. The Advanced Database Synchronization settings control special-case options for all database synchronizer extensions. This setting is not required.

   Append Domain when naming objects enables appending of the user's domain to the username in naming the user's container.

   Example: For the domain `company` and user `user1`, the container is named `user1` with this flag disabled and `user1.company` with this flag enabled. Default is set to **Disable**. Select **Enable** to activate this feature.

2.4.5 Repositories

This section discusses working with repositories that have already been configured for use with Logon Manager. For a full discussion about planning and configuring your repository, see *Deploying Logon Manager with a Directory-Based Repository.*

2.4.5.1 Displaying and Connecting to a Repository

- To display an established connection to a synchronization repository:

  Click **Repository** in the left pane to display the current Logon Manager synchronization repository.

- Or, if no connection is active:

Right-click **Repository** in the left pane and choose **Connect To…** from the shortcut menu.

2.4.5.2 Repository Actions and Options

Right-click an object in the **Repository** window in the right pane to display one of the following shortcut menus of commands and options.

With a Container Selected	
Publish SSO Objects Here	Opens the **Publish to Repository** dialog, which allows you to publish configuration objects, such as application templates and Agent setting overrides to the repository.
Bring Multiple Objects to Console	Displays a list that allows you to select multiple configuration objects that you wish to import into the current Administrative Console settings.
Add Locator Object	Create locator objects (directory servers only).
Create People Container	Creates the `ou=People` container used for application credential storage on directory systems other than Microsoft Active Directory.
New Container	Create a new container within the selected container.
Delete	Remove a container and all objects within.
Refresh	Update the Directory window.
Filter Subnodes…	Opens the **Subnodes Filtering Options** dialog, which allows you to refine the criteria that the Administrative Console uses to display the subnodes of the repository.

With an Override Object Selected	
Configure	Create Administrative Override objects from Administrative Console settings or a data file.
View	Quickly view the selected object, with an option to save it to an `INI` file.
Bring to Console	Import the object to the current Administrative Console settings. ■ If the imported file contains items (applications, policies, groups) with same names as those in the current configuration, the **Import/Merge Conflict** dialog appears. ■ If the imported file contains a set of Global Agent Settings with the same name as an existing set in the current configuration, the imported set is named "Copy of existing settings."
Save as File	Save the object to a local `INI` file.
Delete	Remove the object from the repository.

2.4.5.3 Add User or Group (for Active Directory Role/Group Support)

Use this dialog to select the individual users or user groups to add to the access list for the current configuration item (application logon, password policy, Global Agent Settings, or passphrase set).

Controls

List Names From	Select an Active Directory domain or server.
Names	Lists the names of users and groups for the selected domain or server. Select one or more names to add to the access list.
Add	Copies user(s) and group(s) selected in the Names list to the **Add Names** list. Use **Ctrl+click** or **Shift+click** to select multiple entries.
Members	When a group is selected, the **Names** list displays the Global Group Membership dialog, which lists the members of the selected group.
Search	Displays the Find Account dialog for searching one or more domains for a specific user or group.
Add Names	Display the names of the user(s) or group(s) that you have already selected. Click **OK** to add these names to the access list for the current configuration item. **Note:** You can type or edit user names in this list. However, your entries are checked for invalid account names, and duplicate account selections are automatically removed when you click **OK**.

2.4.5.4 Viewing Global Group Membership (for AD Role/Group Support)

The **Global Group Membership** dialog lists the members of a group selected in the **Add User or Group** dialog. Use this dialog to select the individual members to add to the access-control list for the current configuration item. (Use **Ctrl+click** or **Shift+click** to select multiple entries). Click **Add** to copy the selected names to the **Add Names** list in the **Add User or Group** dialog.

2.4.5.5 Searching for Specific Users or Groups (for AD Role/Group Support)

Use the **Find Account** dialog to search for a specific individual user account or user group in a specific domain or across multiple domains, then add any or all of the search results to the access-control list for the current configuration item (application logon, password policy, Global Agent Settings or passphrase set).

Search for names

Find a User or Group	Enter the name of a user or group to search for. Only exact user/group name matches are allowed.
Search All/Search Only in	Search all available domains (displayed in the list box below) or select specific domains to search. Use **Ctrl+click** or **Shift+click** to select multiple entries.
Search	Begin searching for the user/group name.

Add results to list

Search Results	Lists the user and group accounts that match the search criteria.
Add	Add user(s) and group(s) selected in the **Search Results** list to the Add Names list in the **Add User or Group** dialog. Use **Ctrl+click** or **Shift+click** to select multiple entries.

2.4.5.6 Adding Users or Groups (for LDAP Role/Group Support)

Use this dialog to select the individual users or user groups that are to be added to the access list for the current configuration item (application logon, password policy, Global Agent Settings or passphrase set).

Controls	
Search Base	The base (highest-level) directory to begin searching for user/group accounts. All subdirectories of the base directory are searched. Enter a location or click **Change** to browse the directory tree.
Change	Displays the **Select Search Base** dialog to browse for a base directory for the search.
Search	Begin searching the base directory for users and groups.
Users and Groups	Lists the search results. Select the names to be added to the access list for the current configuration item. Use **Ctrl+click** or **Shift+click** to select multiple entries. Click **OK** when finished to copy your selections to the access list.

2.4.5.7 Selecting a Search Base (for LDAP Role/Group Support)

Use this dialog to browse to and select the base (highest-level) directory to search for user/group names. Click **OK** when finished to return to the **Select Users or Groups** dialog.

2.4.5.8 Browsing for a Repository

This dialog allows you to navigate to a specific target repository container within the currently connected directory server's hierarchy. It also allows you to connect to a different server, if necessary.

To select the target repository container:

1. (Optional) If the directory server to which the Administrative Console is currently connected is not the desired target server, click **Change Server**, fill in the connection information, and click **OK** to connect to the desired server.

2. In the directory tree, navigate to and select the target container.

3. Click **OK**.

2.4.5.9 Connecting to the Repository

To connect the Administrative Console to a synchronization repository:

1. Right-click **Repository** and select **Connect To…** from the shortcut menu.

2. Enter or select the required connection information, then click **OK**.

2.4.5.10 Connection Controls

Menu Option	Description
SyncPath or Server Name	Either: ■ If you selected a directory service for Repository Type, enter or select a server name. or ■ If you selected a database for Repository Type, enter or select an instance name (for Oracle), or the server and instance names separated by a backslash (for SQL Server). or ■ If you selected File Service for Repository Type, enter or select the path to the synchronization folder. **Note:** Select **Edit List** to remove directories/servers from the drop-down list. For SQL Server, if the database server is the only instance on the computer that you are connecting to, then enter the computer name only. If there is more than one database server instance on the target computer, then enter the full connection address (`computerName\dbServerName`). You must specify a file system server as a UNC path, not as a drive-letter and directory path. For example: `\\ServerName\ShareName` not `D:\ShareName`.
Repository Type	Select **File System Sync**, a directory service, or a database server from the drop-down list. If you select **OpenLDAP Directory Server**, and an Extend Schema Status error appears, extend the schema manually
Port	(Directory server only) Enter the port number.
Database	(Database server only) The name of the database to connect to; enter the name of an existing database (default vGOSSO).
Use secure channel (SSL)	Select to enable secure socket layer (directory server only).
User ID	Enter your username.
Password	Enter your password.

2.4.5.11 Creating a New Container

Use the **New Container** prompt to name a new container object at the selected node in the current repository.

To name a new container, enter a container name, then click **OK**.

See Repositories for more information.

2.4.5.12 Editing a Server List

Use this dialog to remove servers that are listed in the **Server Name** drop-down list on the **Connect to Repository** dialog. Select a server and click **Delete**. Click **OK** when finished.

2.4.5.13 Editing a Repository List

The dialog, **Select Objects to Bring to Console**, displays the list of most recently used target repositories and allows you to delete unwanted entries from the list.

To delete an unwanted entry from the list:

1. Select the entry in the list.

2. Click **Delete**.

3. Repeat steps 1-2 for any other unwanted list entries.

4. When you have finished, click **OK**.

2.4.5.14 Subnodes Filtering Options

The subnodes filtering settings control the number of items that display in repository trees. Using filtering, you can refine the criteria that the Administrative Console uses to display the subnodes of these trees, so that they display more manageable results.

You can limit displayed subnodes in two ways:

■ **Filter list.** Uses the asterisk (*) and question mark (?) wild cards.

  The wildcard filter is node-specific. You can use a different wildcard for each node that you want to filter. The wildcard filter is discarded when you switch repository nodes and expires at the end of the Administrative Console session.

■ **Truncate list.** Limits the number of nodes to display.

  Specify a threshold for the maximum number of child nodes to display in a tree. This number governs all repository nodes and remains in effect between Administrative Console sessions. The minimum value is 1; the maximum value is 65,535; and the default value is 1,000. This means that the Administrative Console will display no more than 1,000 entries in a subnode unless you configure it differently.

  If you enter a value less than the minimum or greater than the maximum allowable values, Administrative Console uses whichever limit is closer.

To filter a subnode:

1. Connect to a repository.

2. Right-click on a node in the repository and select **Filter Subnodes…**

3. In the **Subnodes Filtering Options** dialog, do either or both of the following:

   ■ In the **Filter List** field, enter a wildcard expression.

   ■ In the **Truncate** list field, select the maximum number of nodes to display. The maximum number that you can specify is 65,535. The default is 1,000.

4. Click **OK**.

5. Expand the subnode to view the results.

2.4.5.15 Working with Filtered Subnodes

The icon of a filtered subnode contains an *F* next to its standard icon to indicate a filtered state:

If you choose to expand a node containing a number of subnodes greater than the threshold that you set in the Truncate list setting, the Subnodes Filtering Options dialog appears, displaying the following:

Warning: The number of items to be displayed is XXXX (the number you specified), which exceeds the limit defined below.

Click **OK** to expand the subnode using the limit that you previously set, or change the maximum number of nodes to accommodate the list, and then click **OK**.If you did not

set a threshold for this subnode, the Administrative Console uses the system default of 1,000.

2.4.5.16 Importing Multiple Objects to the Administrative Console

The **Bring Multiple Objects to Console** dialog displays, in a flat list, all objects residing in the selected container and all of its child containers, and allows you to select multiple objects for import to the current Administrative Console settings

To select multiple objects from the list and bring them to the Administrative Console:

- **Ctrl+click** each desired object.

   or

1. **Shift+click** the first and last objects in the desired range.

2. Click **OK**.

2.4.5.17 Publish to Repository

This screen allows you to publish configuration objects of your choice to the selected target container, either in a directory-style hierarchy (default), or as a flat configuration file.

> **Note:** For considerations when publishing an Exclusion list, refer to Working with User Exclusions.

To select and publish the desired objects to the repository:

1. Do one of the following:

   - From the tree, right-click on the configuration object that you want to publish, and select **Publish** or **Publish To…**.

      or

   - Select a configuration object from the tree and select **Tools > Publish to Repository**.

2. In the **Available configuration objects** list of the **Publish to Repository** dialog, navigate to and select the desired objects.

   > **Note:** Only categories for which objects have been configured will appear in this list. For example, if no password generation policies exist, the corresponding category will not appear in this list.

3. Click **>>** to move the selected objects to the **Selected objects to be published** list. (To remove an object from this list and not publish it, select the object and click **<<**.)

4. (Optional) If you did not invoke the Publish SSO Objects Here command by right-clicking on the target container, select the desired container from the **Target repository** drop-down list.

> **Note:** If the target container path does not appear in the list, click **Browse** to find and select the desired container.
>
> To remove unwanted entries from this list, select the **Edit list** option from the list.

5. (Optional) If your environment calls for storing configuration objects in flat-format, check the box, **Store selected items in configuration files, rather than as individual objects**.

> **Note:** Selecting this option will overwrite all items stored in existing configuration files, if present, in the target container.

6. (Optional) If you want to create the first-time-use object (`FTUList`), select the corresponding check box.

> **Note:** This option only becomes active if you choose to store your configuration objects in flat format in step 4.

7. Click **Publish**. The Administrative Console publishes the selected objects to the target repository.

> **Note:** Do not attempt to dismiss the dialog or close the Administrative Console until the publishing process completes. The dialog disappears automatically when the objects have been published.
>
> To quickly publish an object or a group of objects, select it in the left-hand tree, right-click it, and select **Publish** (single objects and groups) or **Publish To** (single objects only) from the context-menu.
>
> This will invoke the **Publish to Repository** dialog and automatically add the object(s) to the list of objects to be published. Keep in mind that:
>
> - If you select the **Publish** option, the **Publish to Repository** dialog appears.
> - If you select the **Publish To** option and select a repository, the selected object is automatically published to that repository and the **Publish to Repository** dialog is not displayed. (If you are not currently connected to the selected repository, you will be prompted to authenticate to the directory server.)

2.4.5.18 Publishing to the Repository from the Administrative Console

Use this window to export an Agent configuration to a selected synchronizer container using the current Administrative Console settings as the source. You can export:

- One or more application logons
- A first-time use (bulk-add) object
- A set of Global Agent Settings

2.4.5.19 Exporting Administrative Overrides from the Administrative Console

To export administrative overrides from the Administrative Console:

1. Do one of the following:

   ■ Select **Send All Applications**.

   or

   a. Select **Send Some Applications**, then:

   b. Click **Select Apps**.

   or

   a. From the **Select Applications** dialog, select the applications to send, and click **OK**.

   b. Choose **Send No Apps**.

2. Optionally, select **Create First-Time-Use (FTUList) object**.

3. Optionally, choose a set of Global Agent Settings from the **Admin Overrides** drop-down list.

4. Select **Next**. The wizard displays a summary of the Override configuration.

5. Select **Finish** to complete the export.

2.4.5.20 Displaying the Publish to Repository Window

1. Connect to the Logon Manager repository.

2. In the right pane, right-click a container object and select **Publish to Repository** from the shortcut menu to open the **Publish to Repository** dialog.

3. Select **Administrative Console**.

2.4.5.21 Publishing to the Repository from a Data File

Use this window to export an Agent configuration to a selected synchronizer container using one or more data files as the source. You can export:

■ One or more application logons.

■ A first-time use (bulk-add) object.

■ A set of Global Agent Settings (from an .ini or .reg file).

> **Note:** The Console produces a .REG file compatible only with 32-bit systems. If you are merging the .REG file on a 64-bit system, you must run the following command to move the merged registry data to the correct location within the registry (otherwise, Universal Authentication Manager will not function):
>
> ```
> reg.exe COPY HKLM\Software\Passlogix
> HKLM\Software\Wow6432Node\Passlogix /s
> ```

2.4.5.22 Exporting Administrative Overrides from Data Files

1. Enter the file names (or select **Browse** to select a data file) as the source for each administrative override object you want to export. You can export:

   ■ First-Time Use (from an ftulist.ini file).

- Administrative overrides (from a valid INI or REG file).

- Applications (from an entlist.ini file).

2. Click **Next**. The wizard displays a summary of the override configuration.

3. Click **Finish** to complete the export.

2.4.5.23 Displaying the Wizard Page

1. Connect to the synchronizer repository.

2. From the right pane, right-click a container object and select **Publish to Repository** from the shortcut menu to open the **Publish to Repository** dialog.

3. Select **Data File**.

2.4.6 Configuring Logon Manager Support

Use the **Publish to Repository** dialog to deploy administrative overrides and application configurations to end users using file-system, database, or directory service synchronizers. The objects you can export include:

- One or more application logons.

- A first-time use (bulk-add) object.

- A set of Global Agent Settings.

The **Publish to Repository** dialog helps you export the overrides, from current Administrative Console settings or from one or more data files, to a selected synchronizer container object.

See Synchronization for more information.

2.4.7 Exporting Administrative Overrides to a Synchronizer Container

1. Connect to the Logon Manager synchronizer repository.

2. In the right pane, right-click a container object and select **Publish to Repository** from the shortcut menu to open the window.

3. Choose the Data Source of the administrative overrides and provide the information requested:

- Administrative Console

- Data File

2.4.8 Select Applications, Password Policies, and Session Lists to Publish to Repository

Use the **Publish to Repository** dialog to select application logons, password policies, and Kiosk Manager lists from the current Administrative Console session to deploy to the current synchronization repository. You can choose all applications and policies, select applications and policies individually, or remove items from either list. When your selection is complete, select **Next** to continue.

Lists	Definitions
Applications	Lists the application logon configurations to be deployed.
Password Generation Policies	Lists the password policies to be deployed.

Lists	Definitions
Kiosk Manager Application List	Lists the Kiosk Manager applications lists to be deployed.

2.4.9 Selecting Global Agent Settings to Publish to Repository

Use the **Publish to Repository** dialog to select a set of Global Agent Settings from the current Administrative Console session to deploy to the current Logon Manager synchronization repository.

1. From the list, select a set of Global Agent Settings.

2. Select **Next** to continue.

2.4.10 Including Passphrase Questions to Publish to the Repository

Use the **Publish to Repository** dialog to deploy the passphrase questions from the current Administrative Console session to the current synchronization repository. See Using Passphrase Sets for more information.

Control	Function
Send the Passphrase questions	Select this checkbox to deploy the current set of passphrase questions. Select **Next** to continue.

2.4.10.1 Publish to Repository Summary Page

Use this page to review the configuration. To make changes, use the **Back** and **Next** buttons to display a page. When your configuration is complete, select **Finish**.

2.4.11 Selecting Role/Group Support Mode When Publishing to a Repository

The **Publish to Repository** dialog offers the option to apply role/group access control support for Logon Manager configuration information.

If Standard mode (the default) is selected, configuration information is stored on the directory as standard Logon Manager objects: `EntList` (for logons and policies), `FTUList` (for bulk-add and passphrase questions), and `AdminOverride` (global Agent settings).

Select **Advanced** mode to enable role/group support. All application logons, password policies, global Agent settings, and passphrase question sets are added to the current synchronization repository as individual objects.

Control	Function
Enable Role/Group Support	Select this checkbox to enforce role/group access-control settings for all logons, policies, global Agent settings, and passphrases.
	Clear this checkbox to deploy configurations information without enforcing access control. Click **Next** to continue.

2.4.12 Configuring Applications for an EntList

Use the **Configure Applications** dialog to select the application logons to include in an EntList object for synchronization.

1. Do one of the following:

    ■ Choose **Send All Applications**.

or

■ Choose **Send Some Applications**.

Note: Either of these options overwrites all applications in the selected directory. To create a First-Time-Use list object without overwriting applications in the directory, select **Do not send apps**.

---

2. Click **Select Apps**.

3. In the **Select Application** dialog, select the applications to package and click **OK**.

4. If desired, select **Create First-Time-Use (FTUList) object**.

5. Click **OK**.

To display this dialog for an `EntList` object, connect to a synchronizer repository, right-click an `Entlist` object, then select **Configure** from the shortcut menu.

2.4.13 Adding a Locator Object

Use the **Add Locator Object** dialog to create a locator—a directory object that points the Agent to the container in which user credentials are (or can be) stored. You can create a default locator for all end users or a locator for a specific end user.

See Create locator objects for more information.

Control	Function
Locator Name	Enter default to create a locator for all users. To create a locator for a specific end user, enter the user's distinguished name.
Forwarding Location	Navigate to the container where user credentials are stored and click **OK**.
Store data under the user objects (AD only)	(Active Directory only) Select this checkbox to store the user's credentials (or all users if Locator Name is "default") in the container under the respective user object, rather than in a specific Forwarding Location.
	This setting requires updating the directory schema and modifying the directory-root security settings. To do this, use the **Enable Storing Credentials under User Object** command on the Repository menu. You can use this setting to specify individual users whose credentials are to be stored under their respective User objects. All other user credentials will be stored as specified by the default locator.
	To store all users' credentials under their respective user objects without using a locator object, use the **Enable Storing Credentials under User Object** setting (under `Synchronization\Selected Active Directory sync\Advanced`).

To display this dialog:

1. Connect to the synchronizer directory.

2. In the right pane, select the container in which you want to add the locator.

3. Right-click the container and choose **Add Locator Object** from the shortcut menu.

2.4.14 View Object

Use this dialog to view the contents of the selected configuration object. To save the object to an INI (text) file, click **Save To**. See Repositories for more information.

> **Note:** You can edit the displayed configuration information, but your changes can only be saved to an INI file, not to the object itself.

2.5 Synchronization

Synchronizer extensions allow you to synchronize credentials between an end user's local store (on a workstation) and a store in a remote SSO repository (file system share, relational database or directory server). You can also use these extensions to deploy Administrative Overrides of local Agent settings, application logon configurations (overriding entlist.ini and to be merged with applist.ini), and bulk-add lists (overriding ftulist.ini). See Overriding Configuration Objects for more information.

Synchronizer extensions communicate with directory servers, database servers, file systems, and other storage devices. Each type of extension has its own configuration requirements.

2.5.1 Supported Synchronizers

Logon Manager supports the following synchronizer extensions:

- Microsoft Active Directory Server, including AD LDS (ADAM).

> **Note:** If users will be synchronizing with an Active Directory or AD LDS (ADAM) repository from outside of the corporate network, you must allow RPC protocol-based connections through the corporate firewall; otherwise, users will be unable to synchronize with the repository.

- LDAP-compliant directory servers, including Oracle Internet Directory, Oracle Directory Server Enterprise Edition, OpenLDAP Directory Server, IBM Tivoli Directory Server, and Novell eDirectory.
- Relational databases, including Oracle DB, Microsoft SQL Server, and IBM DB2.
- Network file systems.

Synchronizer extensions are capable of performing the following tasks:

- Connecting to (or binding with) a destination device/resource/store.
- Retrieving any overriding settings (administrative overrides, application configuration information, and first-time use configuration information).
- Synchronizing the local user store (credentials) with the remote store.

Logon Manager supports using each extension multiple times, which allows you to support multiple configurations. For example, if the LDAP Directory Server and File System synchronizer extensions are installed, the Agent will synchronize credentials with, and download overriding settings from, both an LDAP Directory Server and a File System.) See Multiple Synchronizer Extensions for more information.

2.5.2 Directory Server Synchronization Support

The Administrative Console supports any LDAP directory server, including:

- Oracle Internet Directory

- Oracle Directory Server Enterprise Edition

- Oracle Unified Directory

- Oracle Virtual Directory

- Open LDAP Directory Server

- IBM Tivoli Directory Server

- Microsoft Active Directory

- Microsoft AD LDS (ADAM)

- Novell eDirectory

- Siemens Dirx

Logon Manager uses directory server resources for administrative configuration, mobility, and backup. Administrators can deploy configuration overrides to provide new registry, `entlist.ini`, and `ftulist.ini` (bulk-add) settings or to update existing settings. Users can store credentials (for backup) and move among multiple computers (for mobility). When Logon Manager connects to a directory server, it utilizes a specific directory structure to determine where the user's credentials and overriding settings reside.

> **Note:** Each Directory Server presents platform-specific configuration issues. These are addressed in the individual configuration topics.

2.5.3 Directory Structure

Within each directory, Logon Manager utilizes the following object structure:
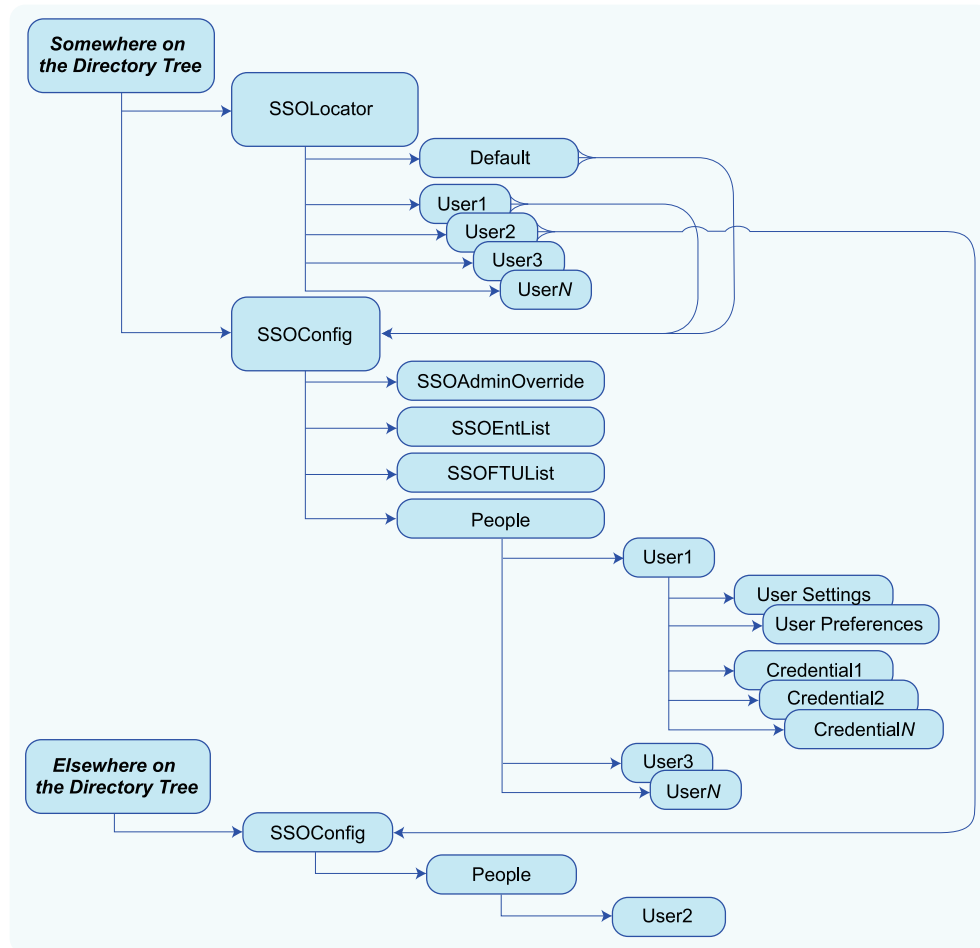
When a user first connects to a directory server, the system is configured to locate a specific path on the directory tree. Using the process described in the next section, the Agent is able to find the `SSOConfig` object, which contains overriding settings, and a People object, which contains the user's settings, preferences, and credentials.

2.5.4 Finding and Creating User Objects

The Agent must locate the specific object in which to store and retrieve the user's credentials. After the first successful connection, the Agent records the objects DN in the user's registry at:

`HKCU\...\Extensions\SyncManager\%Extension%:Root`

where `%Extension%` can be any name as specified in the synchronizer's Global Agent Setting for Sync Order. However, for the first connection from a given workstation, if the user's object is moved, or if the user registry does not contain this information, the Agent must search for the user's object.

Logon Manager uses three methods to search for the proper location to store user credentials on a directory server. Each method looks at the specified distinguished name; the latter two then each walk the directory tree toward the root, to look for a parent object with relevant information.

■ The first method is to look for the user object (`CN=%UserName%,OU=People`) in a specified place.

- The second method is to look for a user-specific pointer object (CN=%UserName%,OU=SSOLocator) to the right place; and if the object is not present, walk the tree until the Agent finds the object or checks the root.

- The third method is to look for a default pointer (CN=default,OU=SSOLocator) to the right place; and if the object is not present, walk the tree until the Agent finds the pointer to the object or checks the root.

If none of these methods succeeds, the user cannot store credentials on the Directory Server (any existing local credentials will be usable).

> **Note:** The %UserName% variable is set automatically in Microsoft Active Directory from the users system username/ID. For LDAP Directory Servers, the %UserName% variable is set from the username/ID with which the user performs a bind to the Directory Server.

2.5.4.1 Method 1: Logon Manager Looks for the User Object

Logon Manager first looks for the user object, CN=%UserName%, inside an OU=People object, specified by the Root registry key (see above).

If that registry key is set to:

OU=SSOConfig,OU=QA,OU=Eng,OU=Company,DC=com,

then the Agent looks for:

CN=%UserName%,OU=People,OU=SSOConfig,OU=QA,OU=Eng,OU=Company,DC=com.

If the Root registry key is not set, the Agent looks in:

HKLM\…\Extensions\SyncManager\%Extension%

for User Paths (see LDAP Synchronization Settings) or Naming Attribute string (see LDAP Special Purpose Synchronization Settings), which points to where the Agent should look.

For example, if UserPath1 is set to:

CN=users,DC=Company,DC=com

then the Agent looks for:

CN=%UserName%,OU=People,OU=SSOConfig,OU=QA,OU=Eng,OU=Company,DC=com

2.5.4.2 Method 2: Logon Manager Looks for a User Pointer

If the user object is not present, Logon Manager next looks for an SSOLocator object in the same object as the SSOConfig object. Therefore, continuing the example above, the Agent looks for:

CN=%UserName%,OU=SSOLocator,OU=QA,OU=Eng,DC=Company,DC=com

If the user pointer is not present, then the Agent walks the tree, toward the root, looking first in:

CN=%UserName%,OU=SSOLocator,OU=Eng,DC=Company,DC=com

and then

CN=%UserName%,OU=SSOLocator,DC=Company,DC=com

If an `SSOLocator` object exists with the users `CN`, it points to where the user's credentials will be stored; the Agent records this information in the user's `Root` registry key, and future logons look in that location.

Note that the pointer can indicate any location in the Directory Tree; for example, a pointer at:

`CN=%UserName%,OU=SSOLocator,OU=Eng,DC=Company,DC=com`

can point to a user object at:

`CN=%UserName%,OU=People,OU=SSOConfig,OU=Sales,DC=Company,DC=com.`

2.5.4.3 Method 3: Logon Manager Looks for a Default Pointer

If a user pointer object is not present, Logon Manager next looks for a default object inside each `SSOLocator` object. Continuing the example above, the Agent looks for

`CN=default,OU=SSOLocator,OU=QA,OU=Eng,DC=Company,DC=com`

If an `SSOLocator` object exists with the `CN=default` object, it points to where the user's credentials will be stored by default; the Agent records this information in the user's `Root` registry key, and future logons look in that location. An example of a default object is:

`OU=People,OU=SSOConfig,OU=Sales,DC=Company,DC=com.`

2.5.5 File System Synchronization Support

The Administrative Console supports file system synchronization with any network drive/device that can be addressed by UNC (Universal Naming Convention). File system synchronization can also be used to support a kiosk user scenario, where multiple users share a single workstation.

2.5.5.1 File System Structure

When a user first connects to the file system, the computer is configured to locate a specific path. The Agent is then directed to find the `vGOConfig` object, which contains overriding settings and a `People` object, which contains the user's settings, preferences, and credentials.

2.5.6 Database Synchronization Support

The Administrative Console supports synchronization of user credentials, application logons, and Global Agent Settings between client workstations and a relational database server. Supported servers include Oracle Database, Microsoft SQLServer, and IBM DB2. For a full list of supported servers, see the Oracle certification matrix.

In this type of synchronization, Logon Manager configuration objects and user data containers are stored on the server as database records in Logon Manager-specific tables:

- SSO_ADMIN stores, as records, the configuration objects you create in the Administrative Console:

  - `EntList` (application logons), `FTUList` (Setup Wizard configurations)

  - `AdminOverride` (Global Agent Settings)

    During synchronization, all workstation users read their logons and overrides from this table; only the administrator, using the Administrative Console, can write to it. These configuration object are depicted in the Administrative

Console in the same hierarchal layout as for file system and directory server synchronizers.

- SSO_USERS stores user credentials, preferences, and synchronization states as records. During synchronization, users read and write to their own records. Only the record for the user currently logged on can be accessed. In the Administrative Console, the records for each user are depicted within the user container.

  When Logon Manager connects to the database server, it reads the configuration objects and overriding settings (from SSO_ADMIN) and synchronizes the user data (in SSO_USERS).

The procedure for configuring database synchronization is similar to that for other synchronization methods:

1. Extend the database schema to create the two tables described above.

2. Create the container objects:

   - An SSOConfig object

     This object contains overriding settings.

   - A People object

     This object holds the user containers for each user's settings, preferences, and credentials.

2.5.7 Multiple Synchronizer Support

Logon Manager supports synchronizing to multiple synchronizer extensions and multiple configurations of the same extension. In either scenario, the Agent attempts to complete synchronization with the first extension and then with each subsequent extension.

Overriding settings can exist on each extension. See Working with Multiple Sets of Overriding Settings for an explanation of how the Agent handles multiple extensions with overriding settings.

> **Note:** Instances to %AD%, %LDAP%, and %File% refer to the respective extensions, and %Extension% refers to any of those extensions.

2.5.8 Multiple Synchronizer Extensions

Logon Manager supports using multiple synchronizer extensions simultaneously. For example, the Agent could first synchronize with a Microsoft Active Directory Server, then with an Oracle Directory Server Enterprise Edition, and then with the File System synchronizer. With Authentication Manager, the Agent could then synchronize with a smart card.

To enable this:

1. Install Logon Manager with the desired synchronizer extensions.

2. In the Administrative Console, select an existing set of Global Agent Settings or create a new set.

3. In the left pane, expand **Global Agent Settings**, right-click **Synchronization**, and select **Manage Synchronizers**.

4. In the **Synchronizers** dialog, select **Add**, name this extension, select the extension type (for example, Active Directory, File System, or LDAP), then click **OK**.

5. Repeat the previous step for additional synchronizer extensions, and reorder as desired.

6. For each synchronizer: select it in the left pane and confirm in the right pane that **Path** is selected and the location specified is correct.

> **Note:** Oracle recommends that you set the `DisplayName` registry entry to help users distinguish between the multiple extensions.

2.5.9 Multiple Configurations of the Same Synchronizer Extension

Logon Manager supports using a given extension with multiple configurations. For example, one LDAP Directory Server configuration could be for an Oracle Directory Server Enterprise Edition, and another LDAP Directory Server configuration could be for Novell eDirectory.

To enable this:

1. Install Logon Manager with the desired synchronizer extensions.

2. In the Administrative Console, select an existing set of Global Agent Settings or create a new set.

3. In the left pane, expand **Global Agent Settings**, right-click **Synchronization**, and select **Manage Synchronizers**.

4. In the **Synchronizers** dialog, select **Add**, name this extension, select the extension type **LDAP**, then click **OK**.

5. Repeat the previous step for additional synchronizer extensions, and reorder as desired.

6. For each synchronizer: select it in the left pane and confirm in the right pane that Path is selected and the location specified is correct.

> **Note:** Oracle recommends that you set the `DisplayName` registry entry to help users distinguish between the multiple extensions.

2.5.10 Overriding Configuration Objects

Synchronizer extensions can download overriding configurations for Global Agent Settings (administrative overrides), application configuration information (`EntList`), and first-time use scenarios (`FTUlist`). Each of these objects has a local equivalent, as detailed in the following table.

Settings Type	Local Equivalent	Directory Server/ Database Object Name	File System Object Name
Administrative Overrides	Registry entries under `HKLM`	`SSOAdminOverride`	*AdminOverride*
Application logon configuration information	The `entlist.ini` file	`SSOentlist`	*entlist*
First-time-use configuration information (including bulk-add information)	The `ftulist.ini` file	`SSOftulist`	*ftulist*

The latter two types of objects are similar in format and layout to their local equivalents, `entlist.ini` and `ftulist.ini`. The first type of object has the following syntax:

`[HKLM\Software\Passlogix]`

REQUIRED: `RegistryPath\RegistryPath:KeyName=TYPE:Value`

This format is exported by the Administrative Console.

Example 1

```
[HKLM\Software\Passlogix]
Shell:AutoBackupPath=STRING:\\FS\Home
Shell:ShowAccessBtn=DWORD:1
Extensions\AccessManager:ReauthOnReveal=DWORD:0
```

> **Note:** In directory server installations, this configuration information can be enabled with support for role group-based access.
>
> Certain settings, such as server URLs, must not be overridden and are thus permanently excluded from administrative override objects. See Configuring the Agent with Global Agent Settings for a complete list of entries that are excluded from being overridden.

2.5.11 Working with Multiple Sets of Overriding Settings

The Agent attempts to retrieve each type of overriding settings from each extension until it finds an extension that has at least one of each. After an overriding setting is downloaded, the Agent does not query other extensions for that overriding setting.

2.5.11.1 Sample Scenarios

Example

- Order: Ext1,Ext2,Ext3,Ext4.

- Ext1 has Admin Overrides.

- Ext2 has Admin Overrides, an `entlist.ini` file, and an first-time use information file.

- Ext3 has no Admin Overrides.

- Ext4 has Admin Overrides, and an first-time use information file.

Scenario A

- Ext1 connects; downloads Admin Overrides; and synchronizes.

- Ext2 connects; downloads application configuration information and first-time use configuration information; and synchronizes.

- Ext3 connects and synchronizes.

- Ext4 connects and synchronizes.

Scenario B

- Ext1 fails.

- Ext2 connects; downloads Admin Overrides, application configuration information, and first-time use configuration information; and synchronizes.

- Ext3 connects and synchronizes.

- Ext4 connects and synchronizes.

Scenario C

- Ext1 fails.

- Ext2 fails.

- Ext3 connects and synchronizes.

- Ext4 connects; downloads Admin Overrides and first-time use configuration information; and synchronizes.

2.5.12 Selective Backup/Restore

The Agent can be configured to compare the local store of user credentials with a remote backup file and write the newer set over the older set. This selective backup/restore, or synchronization, can be triggered from the command line (and thus from an "at," or timed, job) or by configuring certain Agent events (for example, the Startup task, the Refresh task, and so on).

> **Note:** Individual sets of credentials are not compared; for this more-granular level of synchronization, see Synchronization.

2.5.13 Command-Line Synchronization

To trigger a command-line synchronization, run the Agent from the command line (even when the Agent is currently running) using the following syntax:

```
ssoshell.exe /mobility /sync [path] /silent
```

Where

```
[path]
```

is the actual path to the directory where the backup file may exist. (Default: the last directory to which a command line backup file was stored, or where `Shell:AutoBackupPath` points.)

```
/silent
```

means do not show the Backup/Restore Wizard when performing the backup/restore.

To perform a completely-silent synchronize with a network share at `\\FS\Backup\Private`:

```
ssoshell.exe /mobility /sync \\FS1\Backup\Private /silent
```

To synchronize to the last-used location, or to where `Shell:AutoBackupPath` points:

```
ssoshell.exe /mobility /sync /silent
```

2.6 Setting Password Policies

Logon Manager allows administrators to set policies that control automatic password generation. Password policies simplify user logons while ensuring the organization's security.

Most applications have constraints for passwords: how long they can or must be, whether they must or must not include numbers or symbols, and so on. Logon Manager's password generation feature improves application logon security by automatically creating passwords made up of random characters according to

predefined sets of constraints, stored as password policies. Each policy can apply to multiple applications or subscribers.

Using predefined password policies, you can completely automate password changes and implement sophisticated security schemes, including complex passwords, frequent password changes, and application-specific passwords unknown to users.

> **Note:** If the policy you create makes a password difficult or impossible, Logon Manager will try to create a password for up to five seconds and then notify the user that it was unable to generate a password. You can preview the passwords a particular policy generates by clicking **Test Policy**.

2.6.1 Creating Password Generation Policies

Click **Password Generation Policy** in the left pane. This option displays the currently available password generation policies and provides access to policy settings.

See Setting Password Policies for more information.

To add a new password policy:

1. Do one of the following:

   - Click **Add** in the right pane.

     or

   - In the left pane, right-click **Password Generation Policy** then click **New Policy** on the shortcut menu.

2. Enter a Policy Name and click **OK**. The Policy Subscribers tab appears in the right pane, where you can add applications that will use the new policy.

To modify a listed password policy's configuration:

- Click a policy, then click **Edit**. The **Policy Subscribers** tab appears in the right pane.

To delete one or more password policies:

- Select a policy (use **Ctrl+click** or S**hift+click** to select multiple entries), then click **Remove**.

2.6.2 Adding a Password Policy

Use this dialog to add and name a new password generation policy.

- Enter a Policy Name and click **OK**.

To display this dialog:

- Right-click **Password Generation Policy** and choose **New Policy** from the shortcut menu.

  or

- Choose **Password Generation Policy** from the **Insert** menu.

2.6.3 Working with a Selected Password Policy

The list under Password Generation Policies represents configured password generation policies. You can use the tabs in the right pane to view or modify a policy's properties, add or remove applications that use the policy, or change security settings.

See Setting Password Policies for more information.

To view or edit a password policy:

1. Click **Password Generation Policies** in the left pane

2. Select a policy from the list in the right pane, then click **Edit**. The Policy Subscribers tab appears in the right pane.

or

1. In the left pane, click the plus sign (**+**) next to the Password Generation Policies icon (or double-click **Password Generation Policies**) to display the configured policies.

2. Click a policy icon to select it. The Policy Subscribers tab appears in the right pane.

Control	Function
Add	Create another policy.
Delete	Delete the selected policy.
Add Note	Attach notes about this policy for future reference.

2.6.4 Managing Policy Subscribers

Use the **Policy Subscribers** tab to add or manage the applications that use the selected password generation policy.

See Setting Password Policies for more information.

To add applications to a policy:

1. Click **Add**. The **Select Application** dialog appears.

2. Select the applications that will use this policy. (Use **Ctrl+click** or **Shift+click** to select multiple entries.)

3. Click **OK**.

To remove applications from a policy, select a policy (use **Ctrl+click** or **Shift+click** to select multiple entries) and click **Remove**.

Click **Add Notes** to enter notes.

To display this tab:

1. Click **Password Generation Policies** in the left pane.

2. Select a policy from the list in the right pane, then click **Edit**.

3. The **Policy Subscribers** tab appears in the right pane.

2.6.5 The Password Constraints Tab

Use the **Password Constraints** tab to set or modify the allowed type, number, position, and repetition of characters in passwords. These constraints apply to new passwords that Logon Manager automatically generates for applications that subscribe to the selected policy.

To view a set of test passwords based on the passwords constraints for this policy, click the **Test Policy** button.

See Setting Password Policies for more information.

To set password constraints:

1. Do one of the following:

   ■ Select a password policy.

   or

   ■ Create a new password policy.

2. Click the **Password Constraints** tab in the right pane.

3. Select constraint options from the displayed controls.

2.6.5.1 Password Constraint Options

The following tables list the various password constraint options and their possible values.

Password Length	Options
Minimum Length	Minimum number of characters a password most contain: 1-128, default: 8
Maximum Length	Maximum number of characters a password can contain: 1-128, default: 8

Repeating Characters	Options
Maximum repeated non-consecutive characters	Maximum number of times a given character can be repeated in a password (in any position): 0-127, default: 7
Maximum repeated consecutive characters	Number of times a given character can be repeated consecutively (adjacent to itself): 0-127, default: 7

Alphabetic Characters	Options
Allow Uppercase Characters	Check to allow uppercase characters to be included in a password, and enter or select the minimum quantity to permit.
Allow Lowercase Characters	Check to allow lowercase characters to be included in a password, and enter or select the minimum quantity to permit.

Numeric Characters	Options
Allow Numeric Characters	Check to allow numeric characters to be included in a password, and enter or select the minimum and maximum quantity to permit.
Can Start Password	Check to allow password to begin with numeric characters. Default: numeric characters are allowed to begin a password.
Can End Password	Check to allow password to end with numeric characters. Default: numeric characters are allowed to end a password.

Special Characters	Options
Allow Special Characters	Check **Allow Special Characters** to allow non-alphabetical and/or non-numeric characters, and enter or select the minimum and maximum quantity to permit. Default: special characters are not allowed.
Can Start Password	Select to allow password to begin with a special character. Default: special characters are not allowed to begin a password.
Can End Password	Select to allow password to end with special a character. Default: special characters are not allowed to end a password.

Other Characters
Check to allow other characters to be included in a password.

Excluded Characters
Enter the specific characters to exclude from a password.

Previous Password Constraints	Options
Password must not be the same as previous password	Select to prevent reusing the previous password.
Limit the amount of characters that are the same as the previous password	Select to limit repetition of characters from the previous password.
Number of characters that can be the same from the previous password	If some number of characters from the previous password is permissible, select the maximum number of characters to allow.
	Note: Logon Manager recognizes multiple occurrences of a character as the same character and will therefore permit more than one occurrence of that character in the new password.
	So, if the previous password contained three "A"s, and you specify that one character from the previous password can repeat, Logon Manager will allow more than one instance of "A" in the new password.

Test Policy
Displays the **Test Password Policy** dialog, which lets you generate and view a set of test passwords based on the current policy settings.

2.6.6 Testing a Password Policy

Use the **Test Password Policy** dialog to generate a set of test passwords based on the currently-selected password policy. This lets you preview how the Agent will respond to a password change request from an application that subscribes to this policy. You can choose the number of test passwords to generate.

If the password constraints you have set are contradictory or too restrictive to generate any passwords, a message appears explaining how many passwords failed the test and why.

2.6.6.1 Generating a Test Password

Use this screen to generate a list of passwords that conform to your policy and determine if the policy adequately addresses your needs.

1. Select or enter the **Number of test passwords to generate**.

2. Click **Generate Passwords**. The sample passwords display in the output window.

3. When you are finished, click **Cancel** or the **X** in the upper right corner to close the dialog.

To display this dialog:

1. Do one of the following:

    ■ Select a password policy

        or

    ■ Create a new password policy.

2. Click the **Password Constraints** tab in the right pane.

3. Set or modify the constraint settings, then click **Test Policy**.

2.7 Using Passphrase Sets

To enhance security, you can create groups of questions to present to the user upon a password reset request. Create, configure, modify, and delete, these groups, called Passphrase Sets, using the Passphrase Questions screens.

Note: This feature is used only with Windows Authenticator v2, LDAP Authenticator v2, and in Authentication Manager with the Smart Card authenticator (SCAuth).

For increased security, the current authenticator checks the SecondaryAuth.dll signature to verify its authenticity before loading it. If you choose to use a secondary authentication extension other than the one that ships with the product, you must submit it to Oracle for signing before you can implement it.

2.7.1 Adding a Passphrase Set

To add a passphrase set:

1. Do one of the following:

    ■ In the left pane, right-click **Passphrase Questions** and select **New Passphrase** from the shortcut menu.

        or

    ■ Right-click in the right pane and select **New Passphrase** from the shortcut menu.

        or

    ■ Click the **Add** button at the bottom of the right pane.

        or

    ■ From the **Insert** menu, select **Passphrase**.

2. In the **Add Passphrase Set** dialog, type a passphrase set name and click **OK**.

3. Use the **Questions** tab in the right pane to add questions to the current passphrase set.

2.7.2 Deleting a Passphrase Set

To delete a passphrase set, do one of the following:

1. In the left pane, select **Passphrase Questions**.

2. From the list of passphrase sets in the right pane, select a set and click the **Delete** button.

   or

   Select a set, right-click, and select **Delete** from the shortcut menu.

or

1. Double-click **Passphrase Questions** in the left pane, or click the "**+**" sign to expand the menu.

2. From the expanded **Passphrase Questions** menu, right-click an existing passphrase set, and select **Delete** from the shortcut menu.

2.7.3 Modifying a Passphrase Set

To modify a passphrase set:

1. Double-click a passphrase set under the **Passphrase Questions** menu. The questions in that set display in the **Questions** tab in the right pane.

   - To add a question to the set, click the **Add** button and type your question into the **Add a Question** dialog. Then click **OK**.

   - To edit a question in the set, select it and click the **Edit** button. Make changes to the question in the **Add a Question** dialog. Then click **OK**.

   - To delete a question in the set, select it and click the **Remove** button. Logon Manager asks you to confirm the deletion. Click **OK**.

2.7.4 Setting the Default Passphrase Set

Use this option to designate a Passphrase set as the default. The default set contains passphrase questions that users answer during First-Time Use (FTU). The FTU wizard is invoked when:

- A user starts the Agent for the first time after installation.

  or

- The administrator deploys an `ftulist` object (for example, the `ftulist.ini` file).

On first-time use, Logon Manager users select a passphrase question and supply an answer. This stored passphrase answer can be used to reset Logon Manager authentication if the user later changes the primary logon password. The next time single sign-on re-authentication is required, the user enters the new password, and Logon Manager displays the passphrase question to confirm the user's identity.

The Agent uses only one passphrase set. You must decide which set of questions you want the user to answer and designate that set as the default passphrase set. The set you designate as the default is the only one written to the ftulist.

If you import an ftulist to the Administrative Console and change the passphrase set before you re-export the ftulist to the repository, the passhprase set is not included in the export unless you reset it as the default.

To assign a default passphrase set, do one of the following:

- In the right pane, right-click on the set name, then select **Set As Default** from the shortcut menu.

  or

- In the left pane, right-click on the set name, then select **Set As Default** on the shortcut menu.The passphrase set name will appear in bold type in both the right and left panes, indicating that it is the default set.

2.7.5 Working with the Questions Tab

Use the **Questions** tab to manage questions and settings in the selected passphrase set. To display this tab, from the left pane, select **Passphrase Questions** and select the **Default Set** displayed in bold.

To add questions to a passphrase set:

1. Select a language from the drop-down menu.

2. Click **Add** or select **Passphrase** from the **Insert** menu.

3. In the **Add Question** dialog, enter a question.

4. Select or enter a minimum length for the reply.

5. Click **OK**.

The following table lists the ways you can configure a set of passphrase questions.

Control	Function
Language	Select language for passphrase questions.
Default Question	Lists current default passphrase question, which is checked by default. When a new passphrase question is added the default passphrase is unchecked. When checked, the default passphrase is disabled for the current passphrase set. When unchecked the default passphrase is enabled for the current passphrase set.
Enabled Question	Lists current passphrase questions. Checked items are the enabled passphrases for the current set. To disable a passphrase click the checkbox to clear it. To modify a passphrase question, double-click it, or select it and click **Edit**.
Add	Add a new passphrase question. Displays the **Add Question** dialog
Remove	Delete the selected passphrase question. Displays a confirmation prompt.
Edit	Modify the selected passphrase question. Displays the **Edit Question** dialog.
Set This Passphrase Set as Default	Sets the current set as the default. The default passphrase set name in the left pane displays in bold.

Control	Function
Remove or Disable?	After a passphrase question has been created, deployed, and put into use by end-users, it should not be deleted. Users who have selected a passphrase question that has been deleted will not be able to change their passwords without losing access to their Logon Manager credentials. Instead, to remove an in-use passphrase question (and keep it from being displayed during first-time use), disable the question by clearing its checkbox in the list in the **Questions** tab.

2.8 Working with Credential Sharing Groups

Credential sharing groups are sets of applications that share the information of one or more fields to facilitate account management, allowing users to apply a credential change made in one application to other specified applications automatically. For each group that you create, you can include any number of applications and designate which credentials they have in common.

When Logon Manager handles a credential change for any application that is a member of the sharing group, it automatically applies the credential change to all other group members. Any number or combination of Windows, mainframe/host, and Web applications can share a single credential. When using the Windows (Domain) or Directory Server (LDAP) authenticator, selected applications can share a single credential with the authenticator as well.

Applications will share credentials for only their initial deployment to the Agent unless you enable credential sharing groups. Set this parameter in the Required Password Change settings. You can permit or prohibit users' control over which of their applications share credentials in the Global Agent Password Change Settings.

For example, an enterprise might have a new Web interface to an old mainframe application. One way to share the credential between these two is to use a credential sharing group. Some applications share a common credential (for example, an Intranet application and an e-mail application). These applications should be in the same credential sharing group.

> **Note:** The Windows authenticator password is in a predefined group named Domain.
>
> The LDAP Directory Server authenticator is in a predefined group named LDAP.

2.8.1 Adding Predefined Applications to a Credential Sharing Group

The Administrative Console does not currently support adding predefined applications (those included in the default configuration file `applist.ini`) to credential sharing groups. You must do this manually by creating identically-named sections in `entlist.ini` (the custom-application configuration file) that identifies the sharing group. The following example adds an Internet Explorer pop-up application to the credential sharing group *OurServer*:

Example

```
[~Internet Explorer Pop-up XP]
Group=OurServer
```

2.8.2 Creating Credential Sharing Groups

Click **Credential Sharing Groups** in the left pane. This option displays the currently available credential sharing groups and provides access to group settings. Credential sharing is enabled by default.

See Settings for a Selected Credential Sharing Group for the procedure to configure a group.

To create a credential sharing group:

1. Select **Credential Sharing Groups** in the left pane to display current password groups in the right pane.

2. Do one of the following:

   ■ Click **Add** in the right pane.

     or

   ■ In the left pane, right-click **Credential Sharing Groups**, then select **New Group** on the shortcut menu.

3. In the **Add Sharing Group** dialog, enter a Group Name and click **OK**.

4. With a group selected, click **Add** in the right pane to add applications to the group. See Adding Applications to a Credential Sharing Group for more information.

2.8.3 Viewing or Editing a Sharing Group

To view or edit a credential sharing group:

1. Select **Credential Sharing Groups** in the left pane.

   ■ Select a group from the list in the right pane, then click **Edit**.

     or

   ■ In the left pane, click the plus sign (**+**) next to the Credential Sharing Groups icon (or double-click **Credential Sharing Groups**) to display the configured groups.

2. Do one of the following:

   ■ Select a group icon. The list of applications for this group appears in the right pane.

     or

   ■ Right-click a group icon to display a shortcut menu with these options:

     – **Delete.** Delete the selected group.

     – **Rename.** Rename the selected group.

2.8.4 Deleting a Credential Sharing Group

To delete a credential sharing group, select the group (use **Ctrl+click** or **Shift+click** to select multiple entries), then click **Remove**.

> **Note:** You cannot delete the default groups, Domain or LDAP.

2.8.5 The Domain Sharing Group

The domain sharing group is the predefined credential sharing group for the Windows authenticator.

See Adding Applications to a Credential Sharing Group for more information about using this panel.

To select the domain credential sharing group:

1. Select **Credential Sharing Groups** in the left pane.

2. Select **Domain** from the list in the right pane, then click **Edit**.

or

1. In the left pane, click the plus sign (**+**) next to the Credential Sharing Groups icon (or double-click **Credential Sharing Groups**) to display the configured groups.

2. Click **Domain**.

2.8.6 The LDAP Sharing Group

The LDAP sharing group is the predefined credential sharing group for the Directory Service authenticator.

To select the LDAP credential sharing group:

1. Select **Credential Sharing Groups** in the left pane.

2. Select **LDAP** from the list in the right pane, then click **Edit**.

or

1. In the left pane, click the plus sign (**+**) next to the Credential Sharing Groups icon (or double-click **Credential Sharing Groups**) to display the configured groups.

2. Click **LDAP**.

2.8.7 Settings for a Selected Credential Sharing Group

Logon Manager provides flexibility and granularity for you to control how credential sharing groups work. You can configure the following options:

- Sharing any or all fields for a group of applications:
  - Username
  - Password
  - Third Field
  - Fourth Field

  > **Note:** Administrators should take care to avoid resetting the Password field value when Microsoft Windows 7 users are logged on.

- Pre-filling all shared fields when a user first encounters an application in a sharing group, thus requiring the user to enter information only for fields that are not shared by the group.

- Automatically creating an account when a user encounters an application for which all credentials are pre-determined.

- Designating a key field; that is, a field that the Administrative Console uses when updating shared credentials, changing credentials only for accounts with the same key value.

See Creating Credential Sharing Groups for more information.

The following table lists the controls to configure a credential sharing group.

Group account management	
Shared credentials	List of fields that can be included in a credential sharing group. Check the appropriate boxes. ▪ Username ▪ Password ▪ Third Field ▪ Fourth Field
Key credential within group	Designates a field that indicates to the Administrative Console to update shared credentials only for accounts that share this field value. If the user wants to create an account that is not constrained by the key field, that account must have a new key field to avoid updating all existing accounts.
Pre-fill shared credentials	Specifies that shared fields be pre-populated with the shared credentials when the user creates a new account for an application. **Note:** This setting is enabled by default.
Automatically create accounts when all credentials are known	Specifies that Logon Manager should create an account automatically when the user encounters an application that has all fields pre-determined. In order for Logon Manager to complete account creation, you must also enable the "Auto-Submit" setting. Otherwise, the "New Logon" dialog appears as usual. **Note:** This field is available only if Key credential within group is set to **None**.

2.8.8 Adding Applications to a Credential Sharing Group

To add an application to a credential sharing group:

1. Click **Add**. The Select Application dialog appears.

2. Select the applications to include in the selected group. (Use **Ctrl+click** or **Shift+click** to select multiple entries.)

3. Click **OK**.

2.8.9 Editing Applications in a Credential Sharing Group

To edit a applications in a credential sharing group:

1. Select a group from the left pane, and click **Add**.

2. Select the applications that you want to add to this group. (Use **Ctrl+click** or **Shift+click** to select multiple entries.) Click **OK** after you finish making your selections.

3. In the Shared credentials section, under Group account management, check the boxes next to **Username**, **Password**, **Third Field**, and **Fourth Field** as required.

4. To specify a field as the key credential field, select from the **Key credentials within group** dropdown list.

5. Optionally, if you did not specify a key credential (by selecting **None** in the previous step):

   - Check **Pre-fill shared credentials** if you want Logon Manager to fill shared credentials automatically.

   - Check **Automatically create accounts when all credentials are known** if you want Logon Manager to create an account without prompting the user with the **New Logon** dialog.

     Note: **Pre-fill shared credentials** and **Automatically create accounts when all credentials are known** are unavailable if you select a key credential.

     In order to create accounts automatically when all credentials are known, you must also enable **Auto-Submit** for the application.

2.8.10 Removing Applications from a Credential Sharing Group

To remove an application from a credential sharing group

1. Select an application to remove from the selected group. (Use **Ctrl+click** or **Shift+click** to select multiple entries.)

2. Click **Remove**.

2.9 Working with User Exclusions

Using the Exclusions settings, you can prevent specific users from saving credentials for specific applications. The process for creating and publishing an exclusion list follows the same workflow as that for other objects in the Administrative Console.

Note: Use exclusions only for applications for which you want some, but not all, users excluded.

If you want to exclude an application from the entire enterprise, turn on the Global Agent Setting, **Limit user to predefined applications for...** under User Experience > Application Response > Initial Credential Capture. Any application for which you do not create a template will be excluded globally.

Ordinarily, when Logon Manager first detects an application, it prompts the user to enter the credentials to be stored and automatically injected for future use. Using exclusions, if the user enters a username that you have added to the exclusion list for a specific application, Logon Manager does not permit the user to save credentials.

After you publish an exclusion list to Logon Manager:

- Users can log on to applications manually, using excluded credentials, but the Agent does not respond to the application with credentials on the exclusion list, and users cannot save credentials that appear on the exclusion list.

- Excluded credentials that the user already has saved, prior to the policy being put in place, will no longer be presented to the application, and those excluded credentials are deleted from the user's credential list.

■ Silent credential capture will not capture excluded credentials.

2.9.1 Creating an Exclusion List

To create a new Exclusion list, in the Administrative Console:

1. Do one of the following:

   ■ From the **Insert** menu, select **Exclusion List**.

   ■ Select the **Exclusions** node in the left pane, and click **Add** at the bottom of the right pane.

   ■ Right-click on the **Exclusions** node, and select **New List** from the contextual menu.

   ■ Select the **Exclusions** node and right-click in the empty space in the right pane.

2. Enter a name for the list in the **Add Exclusion List** dialog.

The exclusion list name appears under the Exclusions node of the tree in the left pane. The right pane contains three tabs associated with each exclusions list:

■ Exclusion subscribers

■ Excluded usernames

■ Security

Use these tabs to configure each exclusion list.

2.9.2 Publishing an Exclusion List

The procedure for publishing exclusions is identical to that for publishing any other configuration object. For the procedure to publish an exclusion list, see Publish to Repository.

2.9.2.1 Special Considerations for Active Directory Users

Active Directory users who publish exclusion lists must be members of the "SSOExclusionAdmins" Global Security Group, if the group exists. Logon Manager handles the SSOExclusionAdmins group as follows:

■ If you are using Active Directory and the SSOExclusionAdmins group exists, a user must be a member of this group to publish exclusions.

■ If you are using Active Directory and the SSOExclusionAdmins group does not exist, or if you are using another directory service, anyone with publishing rights can publish an exclusion list.

■ If you are using Active Directory, the SSOExclusionAdmins group exists, and a non-group member attempts to publish several objects that include an exclusion object, the other objects will be published without the Exclusion object.

2.9.2.2 Publishing Exclusion Lists with Configuration Files

You cannot publish exclusion lists as standalone configuration (`entlist.ini`) files. When you publish configuration files (that is, you have checked the box in the **File mode** section of the Publish to Repository screen), exclusion lists are published as a subset of an application for which you've configured exclusions.

2.9.3 Add Exclusion List Dialog

Use this dialog to add and name a new exclusion list.

Enter an **Exclusion List name** and click **OK**.

To display this dialog:

- Right-click **Exclusions** and choose **New List** from the shortcut menu.

  or

- Choose **Exclusion List** from the **Insert** menu.

2.9.4 Working with a Selected Exclusion List

From the left pane, select the list you want to work with. Use the tabs in the right pane to view this list's properties, add or remove applications and users to which the list applies, or change security settings.

See Working with User Exclusions for more information.

2.9.4.1 Selecting an Exclusion List for Viewing or Editing

To view or edit an exclusion list:

1. Click **Exclusions** in the left pane.

2. Select an **Exclusion list** from the list in the right pane, then click **Edit**; or double-click the **Exclusion list name** in the right pane. The Exclusion Subscribers tab appears in the right pane.

or

1. In the left pane, click the plus sign (**+**) next to the Exclusions icon (or double-click **Exclusions**) to display the created Exclusion lists.

2. Click an **Exclusion list** to select it. The **Exclusion Subscribers** tab appears in the right pane.

Option	Function
Add	Create another Exclusion list.
Remove	Delete the selected list.
Add Notes	Attach notes about this list for future reference.

2.9.4.2 Exclusion Subscribers

Use this tab to add applications to an exclusion list.

1. Select an **Exclusion list** from the **Exclusions** node in the left pane.

2. Click **Add** on the bottom of the tab.

3. In the **Select Application** screen, select the application that you want to add to the list. Use **Shift+Click** or **Ctrl+Click** to add multiple selections.

4. Click **OK**. The applications you selected appear in the tab window.

2.9.4.3 Excluded Usernames

Use this tab to add users to an exclusion list.

1. Select an **Exclusion list** from the **Exclusions** node in the left pane.

2. Click **Add** on the bottom of the tab.

3. In the Excluded Usernames screen, select the users that you want to add to the list. Use **Shift+Click** or **Ctrl+Click** to add multiple selections.

4. Click **OK**. The users you selected appear in the tab window.

2.10 Using Shared Accounts

Use this node to manage shared account rights for users. It contains two tabs:

- **Default Rights**
- **Admin Rights**

These tabs provide the same settings, but differ in which users you assign these rights.

Default Rights

Use this tab to define the shared account rights for each new application. This feature sets standard rights for each application. After each application is created, change the rights as needed.

Controls

Element	Description
Directory	Select the target directory server.

Access Information

Element	Description
Name	Lists the groups or users who currently have access to this item.
ID	Lists the user's account name.
Access	Indicates the permissions that have been granted to the user or group (Add Logon, Modify Logon, or Delete Logon). To change a user's or group's access rights, right-click the user or group and select **Add Logon**, **Modify Logon**, or **Delete Logon** from the shortcut menu.

Actions

Element	Description
Copy Permissions to	Use this button to easily apply the shared account rights for the current application to multiple applications. Clicking this button displays a dialog listing all the applications. Select the applications that you want these shared account rights to be copied to. Use **Ctrl+click** to select multiple entries. Click **OK**.
Add	Displays the **Add User or Group** dialog (for Active Directory or AD LDS (ADAM)) to select the users or groups who should have access to the currently selected item.
Remove	Removes selected users or groups from the list. Select a user or group to remove; use **Ctrl+click** to select multiple entries.

Element	Description
Add User or Group dialog	The **Select User or Group** dialog varies based on the directory server being used:
	For AD/AD LDS (ADAM), use this control to select the individual users or user groups that are to be added to the access list for the current configuration item (Add Logon, Modify Logon, Delete Logon).

Controls

Element	Description
Search Base	The base (highest-level) directory to begin searching for user or group accounts. All subdirectories of the base directory are searched. Enter a location or click **Change** to browse the directory tree.
Change	Displays the **Select Search Base** dialog to browse for a base directory for the search.
	Use this dialog to browse to and select the base (highest-level) directory for user or group names. Click **OK** when finished.
Search	Begin searching the base directory for users and groups.
Users or Groups	Lists the search results. Select the names to be added to the access list for the current configuration item. Use **Ctrl+click** or **Shift+click** to select multiple entries. Click **OK** when finished to copy your selections to the access list.
Active Directory or ADAM	Use this dialog to select the individual users or user groups that are to be added to the access list for the current configuration item (Add Logon, Modify Logon, Delete Logon).

Controls

Element	Description
List Names From	Select an Active Directory domain or server.
Names	Lists the names of users and groups for the selected domain or server. Select one or more names to add to the access list.
Add	Copies users and groups selected in the **Names** list to the **Add Names** list. Use **Ctrl+click** of **Shift+click** to select multiple entries.
Members	When a group is selected, the **Names** list displays the **Global Group Membership** dialog, which list the members of the selected group.
Search	Displays the **Find Account** dialog for searching one or more domains for a specific user or group.
Add Names	Display the names of the users or groups for whom you have added so far. Click **OK** to add these names to the access list for the current configuration item.
	Note: You can type or edit user names in this list. However, entries are checked for invalid account names and duplicate account selections are automatically removed when you click **OK**.

2.11 Storing User Data

Logon Manager stores user credentials locally in the ...\Application Data\Passlogix folder. Global Agent Settings are stored in the Local Machine registry key (HKLM); settings modified the user are stored in the Current User registry key (HKCU).

Logon Manager can also perform a complete backup of credentials and settings to a file (.bkv). The backup can be performed manually by the user, or automatically by administrative configuration). For details on this feature, see File-Based Backup/Restore.

Logon Manager can also synchronize individual user credentials with these remote sources, including file-systems, databases, and directory servers. These remote sources can provide the Agent with application logons. First-time-use (setup) information and administrative overrides (Global Agent Settings). For details on this feature, see Synchronization.

2.11.1 Storing Credentials in the User Object

> **Note:** This section applies to Active Directory only.

With Active Directory installations, you can configure Logon Manager to store user data under the user object, rather than in the standard vgoconfig container. To do this, take the following steps:

1. Use the **Enable Storing Credentials under User Object** command (on the Repository menu) to update the directory schema to allow user-credential containers as children of user objects. This command also modifies the directory-root security settings to grant users the rights to create the credential containers.

2. Do one of the following:

   - Select the **Store data under the user objects** option (see Adding a Locator Object) to create a vgolocator object ("default" for all users that use this locator, or for specific user by distinguished name) that points to the user objects.

   - Use the Location for storing user credentials Agent setting (in the Active Directory Synchronization Settings) to configure the Agent to disregard the vgolocator object and always store credentials under the user object.

2.11.2 File-Based Backup/Restore

If the Backup/Restore module is installed, the Administrative Console can perform a complete backup/restore of user credentials and settings to or from another location. The backup/restore can be performed manually (by the user) or automatically (by administrative configuration). Also, a selective backup/restore (writing the newer information over the older information) can be performed automatically (by administrative configuration).

> **Note:** If the Backup/Restore module is installed, the user can perform a manual backup, store to any location (even a floppy drive), and select any password (even a one-character password).

2.11.2.1 Automatic Backup

You can configure the Agent to perform a full backup of user credentials and settings. This backup can be triggered from the command line (and thus from an "at," or timed, job) or by configuring certain Agent events (for example, the Startup task, the Refresh task, and so on).

2.11.2.2 Command-Line Backup

To trigger a command-line automatic backup, run the Agent from the command line (even when the Agent is currently running) using the following syntax:

```
ssoshell.exe/mobility /backup [path] /silent
```

where:

`[path]` is the actual path to the directory where the backup file is placed. The default is the last directory where a command line backup file was stored.

and:

`/silent` indicates to hide the operation when performing the backup.

To perform a completely silent backup to a network share at `\\FS\Backup\Private`:

```
ssoshell.exe /mobility /backup "\FS1\Backup\Private" /silent
```

To back up to the last-used location:

```
ssoshell.exe /mobility /backup /silent
```

2.11.2.3 Event-Driven Automatic Backup

To configure the Agent to perform an automatic backup upon certain Agent events, determine the command line string needed to perform the desired backup. Then, set the appropriate task. For example, to perform a backup with every change in credentials, set a task to run **When logons change (add, delete, copy, modify)** (under User Experience > Custom Actions) to the command line string.

2.11.2.4 Forced Restore

The Agent can be configured to perform a full restore of user credentials and settings, replacing any existing data. This restore can be triggered from the command line (and thus via a remote "run" command) or by configuring certain Agent events (for example, the startup task).

2.11.2.5 Command-Line Forced Restore

To trigger a command-line forced restore, run the Agent from the command line (even when the Agent is running) using the following syntax:

```
ssoshell.exe /mobility /restore [path] /silent
```

where:

`[path]` is the path to the directory where the backup file exists. The default is the last directory where a command line backup file was stored.

and:

`/silent` indicates to hide the operation when performing the restore.

To perform a completely silent restore from a network share at `\\FS\Backup\Private`:

```
ssoshell.exe /mobility /restore "\FS1\Backup\Private" /silent
```

To restore from the last-used location:

```
ssoshell.exe /mobility /restore /silent
```

2.11.2.6 Event-Driven Forced Restore

To perform a forced restore upon certain Agent events, determine the command line string needed to perform the desired restore. Then, set the appropriate task. For

example, to perform a restore at startup, set a task to run **After Agent starts** (in the Global Agent Custom Actions Settings) to the command line string.

2.12 Creating and Using Templates

> **Note:** For a complete discussion of configuring and diagnosing templates, see the guide, *Configuring and Diagnosing Logon Manager Application Templates*.

Logon Manager recognizes and responds to a wide array of logon scenarios. Users can configure each logon in advance or as they encounter them. When a user configures a logon, the Agent displays a list of predefined applications. Users select an application from this list or create a logon for an unlisted application.

Predefined applications simplify configuration for the user and increase the reliability of both recognizing and responding to logon and password-change requests.

Preconfigured application logons for many popular Windows applications are included with the Administrative Console in the form of templates that contain all or part of the logon's configuration. You can also convert the application logons that you create into templates through the Administrative Console. The `applist.ini` file (located in the installation directory in the `Plugin\LogonMgr` directory) includes predefined logons for network and web pop-up logon dialogs boxes and for many online service providers.

Templates provide two practical benefits for creating and managing pre-configured logons:

- You can store, share, and reuse a group of specific logon settings as a starter set for creating new logons based on the template. Your templates appear as options in the **Add Application** dialog.

- If you make changes to a template's source logon, you can easily apply your changes to any logon based on that template, by using the Update Applications command on the Tools menu.

You use a template to create a logon by selecting it from the Applications drop-down list in the **Add Application** dialog. You are prompted if additional information is needed to complete the configuration.

You can update application logons with any changes made in their originating templates. Open the Administrative Console XML file containing the applications and select the **Update Applications** command from the Tools menu.

To create a template:

1. Select an existing application logon in the **Manage Templates** dialog from the Tools menu.

2. Choose the logon settings (for the application and for individual forms) that you want to be able to override later; use the Tab in the Edit Template dialog (click **Edit** in the **Manage Templates** dialog). For Web and Windows applications, you can also choose a setting that the template user must provide in order to complete the logon configuration (on the **Supply Info** tab).

3. Save the current file to the **Templates** folder under the Administrative Console program directory (typically, this is `C:\Program Files\Passlogix\SSO Administrative Console\Templates`).

> **Note:** When creating templates, take precautions to ensure that no complete template name exactly matches the first part of another template name. If the Agent finds two templates, one of whose names is a subset of the other, the Agent recognizes the template with the shorter name.
>
> For example, if two templates are named ABC and ABD, this issue does not occur. But if one template is named ABC, and one is named ABC_D, the Agent recognizes only the ABC template, and ignores the ABC_D template, regardless of which application is opened.

To add templates to Logon Manager:

1. Create the application logons using the Administrative Console configuration features.

2. Create and deploy an entlist as an `INI` file or equivalent synchronization object.

3. Use **Export to INI** file to create an `entlist.ini` file.

4. Use **Publish to Repository** to create an entlist synchronization object.

5. Do one of the following:

   - If you are using synchronization to deploy application logons, do not use the Location of `entlist.ini` file setting. The synchronizer automatically locates `entlist.ini` and `ftulist.ini` in the user's `%AppData%\Passlogix` directory.

   - If you are not using synchronization to deploy application logons, use the **Location of entlist.ini file** setting in the Global Agent Synchronization settings.

   > **Note:** The administrator must create `entlist.ini`; the Agent does not create it automatically.

2.12.1 Managing Templates

Use this dialog to create, modify, and remove templates for application logons. To display this dialog, on the **Tools** menu, click **Manage Templates**.

2.12.1.1 Creating a Template for a Running Application

You can create a new template, or edit an existing one, on-the-fly for a Windows or Web application while the application is running.

> **Note:** This procedure applies only to Windows and Web applications. If you attempt this procedure for a host or mainframe application, the Host/Mainframe Form Wizard launches.

In order to perform this procedure, both the Administrative Console and the Logon Manager Agent must be running, and you must configure the Agent settings to display the **Title Bar Button** menu.

2.12.1.1.1 Creating a Template for a Running Windows Application

To create a template for a running Windows application:

1. Launch the application for which you want to create a template.

2. Select **Create Template** from the application's **Title Bar Button** menu.

Two things happen:

- In the application's window, Logon Manager detects the credential fields and highlights them.

- A condensed version of the Form Wizard appears. Enter information for the following fields:

  - **Form Name.** This field is pre-filled with the name of the selected application. You can leave this as it is or change it if you want to.

  - **Form Type.** Select the form type from the drop-down menu:

    Logon

    Logon Success

    Logon failure

    Password change

    Password change success

    Password change failure

  - **Add to Template.**

    This field defaults to the New Template selection. Alternatively, the drop-down menu contains the list of all configured Windows application templates to which you might want to add this form.

  - **Edit Fields/Hide Details.**

    Toggle this button to expand the window to display the entire Form Wizard, or collapse the window to the simpler Form Wizard.

2.12.1.1.2 Creating a Template for a Running Web Application

To create a template for a running Web application:

1. Launch the application for which you want to create a template.

2. Select **Create Template** from the application's **Title Bar Button** menu.
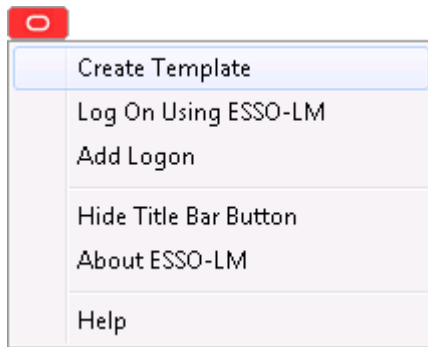
3. The Web Form Wizard launches.

4. In the Web page, Logon Manager detects the credential fields and highlights them.

5. A condensed version of the Form Wizard appears. Enter information for the following fields:

   ■ **Form Name.** This field is pre-filled with the name of the selected application. You can leave this as it is or change it if you want to.

   ■ **Form Type.** Select the form type from the drop-down menu:

   Logon

   Logon Success

   Logon failure

   Password change

   Password change success

   Password change failure

   ■ **Add to Template.**

   This field defaults to the New Template selection. Alternatively, the drop-down menu contains the list of all configured Windows application templates to which you might want to add this form.

   ■ **Edit Fields/Hide Details.**

   Toggle this button to expand the window to display the entire Form Wizard, or collapse the window to the simpler Form Wizard.

2.12.1.2 Creating a New Template for Applications That Are Not Running on Your Workstation

You can create a template for an application, even if it is not running or installed on your workstation. To create a new template in this scenario:

1. Click **Add** to create a new template from an application logon.

2. From the **Select Applications** dialog, select the application on which to base the template.

3. Click **OK**. In the **Edit Template** dialog, specify the settings that must be supplied by an administrator, and the template's overriding settings.

2.12.1.3 Modifying an Existing Template

To modify an existing template, select an application from the list and click **Edit**. In the **Edit Template** dialog, modify the settings that must be supplied by an administrator, and the template's overriding settings.

2.12.1.4 Deleting a Template

To delete a template, select an application from the list and click **Remove**.

2.12.1.5 Adding Application Templates to Logon Manager

To add templates to Logon Manager:

1. Create the application logons using the Administrative Console's configuration features.

2. Create and deploy an entlist as an `INI` file or equivalent synchronization object.

   - Export to an `INI` file to create an `entlist.ini` file.

   - Publish to the repository to create an entlist synchronization object.

3. Do one of the following:

   - If you are using synchronization to deploy application logons, do not use the Location of `entlist.ini` file setting. The synchronizer automatically locates `entlist.ini` and `ftulist.ini` in the user's `%AppData%\Passlogix` directory.

   - If you are not using synchronization to deploy application logons, use the Location of `entlist.ini` file setting in the Synchronization Global Agent Settings.

   > **Note:** The administrator must create `entlist.ini`; the Agent does not create it automatically.

2.12.2 General Guidelines for Setting Up Applications

Setting up and configuring applications is easiest when you do the following:

- Have the target applications on the same workstation as the Administrative Console.

- Minimize the number of other applications running during configuration.

- To facilitate creating application configurations and testing:

  - Configure your workstation not to use a synchronizer extension.

  - When the application logon request causes the Agent to respond, tell the Agent to ignore it.

  - In the Administrative Console, create the application configuration and then use **Export Apps to Agent** (on the Tools menu) to overwrite the local `entlist.ini` file.

  - Keep Logon Manager visible, and select **Refresh** whenever you finish exporting from the Administrative Console.

  - Bring up the application logon dialog to see if your new configuration works properly within the Agent.

2.12.3 Adding Windows Applications

The easiest and most precise way to configure Windows applications is by using The Windows Form Wizard.

Before you begin Windows logon configuration, review the General Guidelines for Setting Up Applications.

2.12.3.1 Special Issues and Settings

Some Windows applications interact in unusual ways or have special requirements. For these scenarios, the Administrative Console offers these additional configuration options.

2.12.3.1.1 Special Configuration Settings The following table lists configuration settings to consider when creating Windows templates.

Tab	Setting	Consideration
Fields	SendKeys	Use the SendKeys option for Windows applications that: ■ Cannot receive credentials from the Windows message queue or by other techniques the Agent normally uses to send credentials. ■ Do not use standard Windows controls that have Control IDs. ■ Dynamically generate controls or do not use Windows controls at all (for example, Flash applications).
Miscellaneous Tab (for a new or selected logon form)	Allowable Class	Use the Allowable Class option to identify logon or password-change window classes that must be present in order to execute this logon. This is useful for applications that present logon or password-change windows with non-standard class names.
	Ignore this Window Class	Use the Ignore Window Class option for applications that: ■ Use hidden logon or password-change dialogs. or ■ Present duplicate dialogs.
	Attach to window's Message Queue	Use the **Attach to…** option to keep the focus on the target logon window while sending credentials.
	Preset Focus	Use the **Preset Focus** options to have the Agent set the focus on a field before entering data in it.
Miscellaneous Tab (for a selected application)	Service Logon	Select the **Service Logon** option to let the Agent detect an application that runs as a Windows service (that is, in the System space, rather than the User space).
	Third/Fourth Field Label	Use these options to specify the text labels the Agent should use to display these additional fields.

Tab	Setting	Consideration
	File extension for Icon	Use this option to provide a Windows file extension to associate with a logon; this lets the Agent map an icon to it.

2.12.4 Adding Web Applications

Logon Manager detects and responds to logon and password-change requests for predefined Web applications. Much like Windows and host/mainframe applications, administrators define Web applications by including a section in entlist.ini.

The Agent recognizes specific strings of data at specified locations within the HTML code of a Web page. This data tells the Agent how to detect the Web site's logon and password-change screens, where to enter the user credentials, and how to submit those credentials.

The easiest and most precise way to configure Web applications is by using the Web Form Wizard. Before you begin this procedure, refer to the General Guidelines for Setting Up Applications.

> **Note:**   Web applications can have the logon and password change forms on the same page, on different pages within the same URL, or at different URLs. Furthermore, logons can be in the same form at different URLs, or on different forms at different URLs.
>
> If you add a configuration for a site where the user's local store already includes a logon, your new configuration will override the user's. The user will need to re-enter credentials for this application.
>
> The user can still view the old logon in Logon Manager.

2.12.5 Adding Host/Mainframe Applications

Logon Manager provides single sign-on functionality to host/mainframe applications through host emulators that:

- Implement HLLAPI (high-level language application programming interface).

  or

- Have a built-in scripting language that can display a dialog.

The host emulator enables an end user to connect the Windows workstation to a mainframe, AS/400, OS/390, Unix, or other host-based session. Logon Manager recognizes a terminal screen by looking for specific strings of data at specific screen locations.

In order for Logon Manager to recognize host emulators, enable mainframe support by selecting MFEnable in the Global Agent Settings for Host/Mainframe Application Response.

All host/mainframe applications must be predefined. The Logon Manager end user has no means to define host/mainframe applications. The administrator must also configure the host emulators themselves in order for Logon Manager to recognize them. Any host emulator can use application logons created by any other host emulator. See Section 7.2.4, "Configuring Host Emulators," for procedures to configure specific emulators.

> **Note:** Logon creation is easiest using a host emulator that allows you to select text and that displays the row and column coordinates of your selection.
>
> For information on configuring an emulator that does not support HLLAPI but does have a scripting language, contact Oracle.

For emulators that do not implement HLLAPI or have a scripting language, you can, in some cases, configure the host/mainframe application as a Windows application (to detect the form by its window title) and using SendKeys to supply user credentials. See Windows applications Special Configuration Settings for more information.

The easiest, and most precise way to configure host/mainframe applications is by using the Host/Mainframe Form Wizard. Before you begin this procedure, refer to the General Guidelines for Setting Up Applications.

2.12.5.1 Configuring a Host/Mainframe Application Manually

The following procedure describes the steps for manually configuring or modifying a host/mainframe logon. Refer to the specific dialogs and controls for more information. Before you begin this procedure, see the General Guidelines for Setting Up Applications and Creating a Template Using an Open Application for the procedure to select an application from a list of open applications.

1. Start the application and configure the host emulator. See Section 7.2.4, "Configuring Host Emulators," for more information.

2. In the Administrative Console, do one of the following:

   - Create a new host/mainframe application logon.

     or

   - In the left pane, click **Applications** and select a host/mainframe application. Click the **General** tab in the right pane.

3. In the **Identification** tab of the **Host/Mainframe form-configuration** dialog:

   a. Select a logon form from the list and click **Edit**.

   b. Specify one or more **Text Matching** captions, so that this page can be identified uniquely from other pages. Specify the identifying **Text string** of the caption and its starting **Row** and **Column** numbers.

   c. Specify the **Fields** for credentials. Click **Edit** (under **Fields**) to display the **SendKeys (Host/Mainframe)** dialog. Specify the starting **Row** and **Column** for each field and the keystrokes to send.

4. If the terminal response time requires a pause between credential field entries, select the **Options** tab and enter the number of milliseconds to pause in **Delay Field**.

5. Repeat the steps above for each additional logon screen.

6. To add password change information, repeat the process with the **Password Change** tab and the password change dialog in the target application.

2.12.5.2 Adding Java Applications and Applets

You can configure Java application logons and Java applet logons (in Web pages) by using the The Windows Form Wizard. The procedures for creating and deploying are generally identical for Java and Windows applications.

> **Note:** In order for the Agent to detect and use Java application logons, the Java Runtime Environment (JRE) must be installed on the workstation prior to installing Logon Manager. If JRE is not already present when Logon Manager is installed, the Agent's Java Helper component is not available for installation.

Before you begin Java logon configuration, refer to the General Guidelines for Setting Up Applications for configuring applications.

2.12.5.3 Adding Telnet Applications

Logon Manager supports Telnet sessions using HLLAPI (high-level language application programming interface) implemented by a mainframe/host emulator. For the most current list of supported emulators, see the Oracle certification matrix:

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-100350.html.

Configuring a logon for a Telnet application is essentially identical to adding host/mainframe applications in general, but with these exceptions:

- Host applications generally display text captions and data fields in fixed positions, which lets Logon Manager detect a screen as a logon form using Text Matching and absolute row/column coordinates. By contrast, a Telnet application, including its logon screen, appears in a scrolling text window. The screen position of the text caption for Logon Manager to match (and begin the logon) should be set as a row number relative to the cursor (negative for above, positive for below) and an absolute column number. See the example in the next section.

- If one or both of the caption's coordinates are unpredictable, you can use an asterisk (*) for the row setting to match text in any row (and a fixed column), for the column setting to match text in any column (and a row relative to the cursor), or for both settings to match text anywhere on screen.

- When supplying credentials for a Telnet logon, Logon Manager ignores the row and column coordinate settings for field-matching. However, the settings must be present in the logon configuration. Use one (1) as the value for both row and column coordinates for all credential fields in a Telnet logon.

- In order to ensure that the Telnet logon credentials are filled in properly, Logon Manager is enabled with timing logic. The **Delay Field** setting (on the Options tab for configuring a host/mainframe logon form) indicates the time in milliseconds that the Agent should pause between each action.

> **Note:** See Section 7.2.4, "Configuring Host Emulators," for additional information on HLLAPI configuration.

2.12.5.4 Adding a Telnet Application Logon

The easiest, and most precise way to configure Telnet applications is by using the Host/Mainframe Form Wizard. Before you begin this procedure, refer to the General Guidelines for Setting Up Applications.

2.12.5.5 Configuring a Telnet Application Logon Manually

The following procedure describes the steps for manually configuring or modifying a Telnet logon. Refer to the specific dialogs and controls for more information. Before

you begin this procedure, refer to the General Guidelines for Setting Up Applications.

1. Start the application and configure the host emulator.

2. In the Administrative Console, do one of the following:

   ■ Create a new Host/Mainframe application logon.

     or

   ■ In the left pane, click **Applications** and select a host/mainframe application.

3. Click the **General** tab in the right pane.

4. Select a logon form from the list and click **Edit**.

5. In the **General** tab of the **Host/Mainframe form-configuration** dialog:

   a. Specify one or more Text Matching captions, so that this page can be identified uniquely from other pages. Specify the identifying **Text** string of the caption and its starting **Row** and **Column** numbers.

   The row numbers should be relative to the current cursor position and can be negative integers. See the example below.

   The column number is an absolute position.

   You can also use an asterisk (*****) for the row or column as a wildcard.

   b. Specify the Fields for credentials. Under **Fields**, click **Edit**. In the Edit SendKeys Fields and Actions dialog, select each field, and set the **Row** and **Column** for each field to one (1). If needed, specify any additional keystrokes that should follow each field entry.

6. If the terminal response-time requires a pause between credential field entries, select the Options tab and type the number of milliseconds to pause in **Delay Field**.

7. Repeat the steps above for each additional logon form.

8. To add Password Change information, repeat the process with the Password Change tab and the password change dialogs in the target application.

Text Matching Example

Because the text in a Telnet application scrolls, the row positioning must be set relative to the cursor's row, which is always row one (1). Therefore, the row coordinate for a caption ("Welcome to VAX/VMS_V6.1") that is two rows above the cursor is negative two (-2). The column setting of the start of the caption text is an absolute coordinate; in the example here, nine (9).

Screen text column	
	123456789022345678903234567890123
Row#	123456789012345678901234567890123
-4	
-3	
-2	Welcome_to_VAX/VMS_V6.1_
-1	
1	Username: _
2	

Screen text column
3
4

For Logon Manager to identify this sample screen, you would set these text matching criteria (using the Text Matching dialog):

Match 1	
Text	Welcome to VAX/VMS V6.1
Row	-2
Column	9

Match 2	
Text	Welcome to VAX/VMS V6.1
Row	-2
Column	9

2.12.6 Bulk-Adding Applications for First-Time Use

After the initial product installation, the First-Time Use Wizard requests various items of information to complete the setup process. If multiple authenticators are installed, the user is prompted to choose a Primary Logon Method. In addition, Logon Manager can also prompt the user for application usernames/IDs and passwords to quickly populate the user's store.

> **Note:** In order to use Bulk-Add, you must enable First-Time Use.

The configuration settings for the First-Time Use Wizard are specified in the `ftulist.ini` file. You can have Logon Manager prompt users to provide credentials (username/ID, password, third field) for their existing logons. Combining first-time use configuration with predefined logons ensures that users reap the benefits of single sign-on immediately after installation. Alternatively, users can configure their individual logons as they encounter each application.

> **Note:** All Logon Manager configuration files (including `entlist.ini` and `ftulist.ini` can be created and edited only through the Administrative Console.

2.12.6.1 Specifying Applications to Bulk-Add

> **Note:** Applications must be individually configured to be used in a bulk-add. See Bulk-Adding Applications for First-Time Use.

1. Select **Applications** in the left pane, then select the **Bulk-Add** tab in the right pane.

2. Click **Add**.

3. From the **Select Application** dialog, select the applications to add to this group. (Use **Ctrl+click** or **Shift+click** to select multiple entries.)

4. Click **OK**.

5. Enter or edit the Date Stamp in `yyyymmdd` format (for example `20130615` for June 15, 2013). If this date is later than the last date that a given Agent completed setup, then the Agent activates the Setup Wizard to add the new logons.

To enable a logon for Bulk-Add:

1. Select **Applications** in the left pane, then select an application.

2. Click the **Bulk-Add** tab in the right pane.

3. Select **Enable Bulk-Add capability for this application**.

4. If the user must re-enter one or more fields for confirmation, then select the appropriate **Confirm** settings.

2.13 Creating New Applications

The **Applications** tab displays application configuration information and provides access to logon settings.

Click **Applications** in the left pane to display these tabs in the right pane:

- The Applications List displaying currently configured logons.

- The Bulk Add (multiple logon deployment) controls.

Right-click **Applications** in the left pane to display a shortcut menu with these options:

Menu Option	Function
New Windows App	Configure a new Windows application. Displays the **Add Application** dialog.
New Web App	Configure a new Website application. Displays the **Add Application** dialog.
New Host App	Configure a new mainframe application. Displays the **Add Application** dialog.
Import	Open stored application configurations in a `.REG` or `.INI` file.
Export	Save one or more application configurations in an `.INI` file.

2.13.1 The Applications List

This menu option displays a list of applications with logons configured for use with Logon Manager.
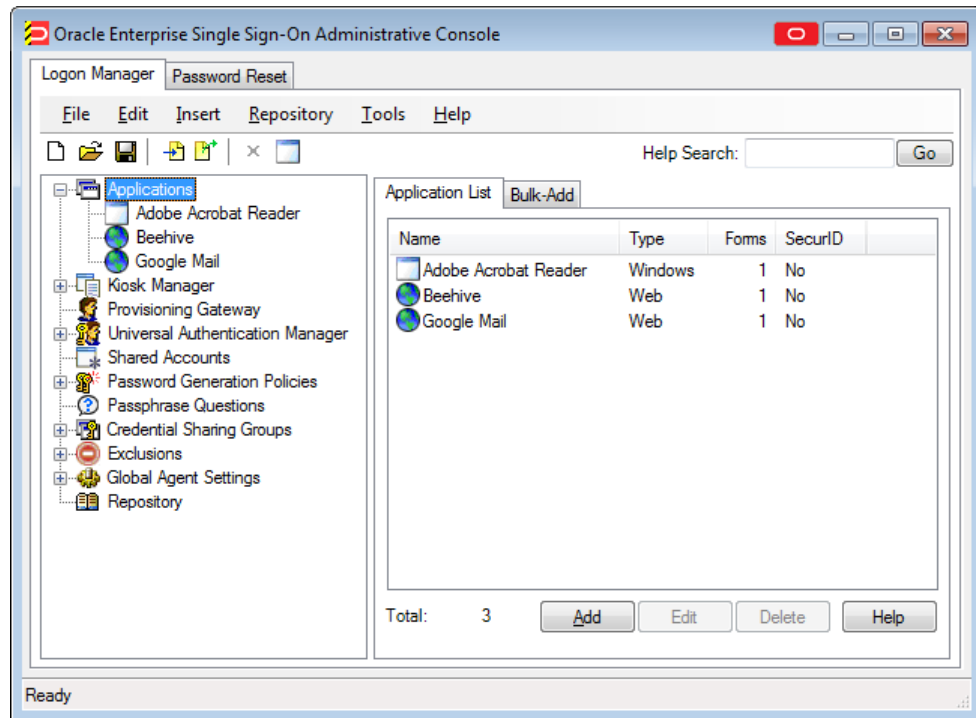
To use this tab:

■ Click **Applications** in the left pane, then click the **Applications List** tab in the right pane.

■ To add new applications click **Add**.

■ To modify a listed application's logon configuration, click an application, then click **Edit**.

■ To delete one or more logon configurations, click an application (use **Ctrl+click** or **Shift+click** to select multiple entries), then click **Delete**.

2.13.2 Adding an Application

Use the **Add Application** dialog to begin configuring a new application logon. You can define an application logon from scratch or you can use a stored template that provides pre-configured values for some or all logon settings.

To add an application:

1. Enter a **Name** for the new logon.

2. Select an **Application Type**:

    ■ Windows

    ■ Web

    ■ Host/Mainframe

3. Do one of the following:

    ■ Select a template from the **Application** drop down list and click **Next** to provide any additional information needed to complete the logon.

    ■ Leave the Application selection as New *[type]* Application and click **Finish** to create an entirely new logon.

4. If this application requires authentication by RSA (SecurID/SoftID) token, select the **RSA securID** check box.

5. Click **Finish**.

The Form Wizard for the selected Application Type launches. See The Windows Form Wizard, Web Form Wizard, or Host/Mainframe Form Wizard for more information.

To display the **Add Application** dialog, do one of the following:

- Right-click **Applications** in the left pane, then choose the application type (**Windows**, **Web** or **Host/Mainframe**) from the shortcut menu.

  or

- Click **Add** in the Applications list.

2.13.2.1 Adding an Application from a Template

Use this wizard page to supply application logon configuration settings that are not provided by the application logon template. Settings that must be supplied to complete the logon are marked in the left pane with a red **X**.
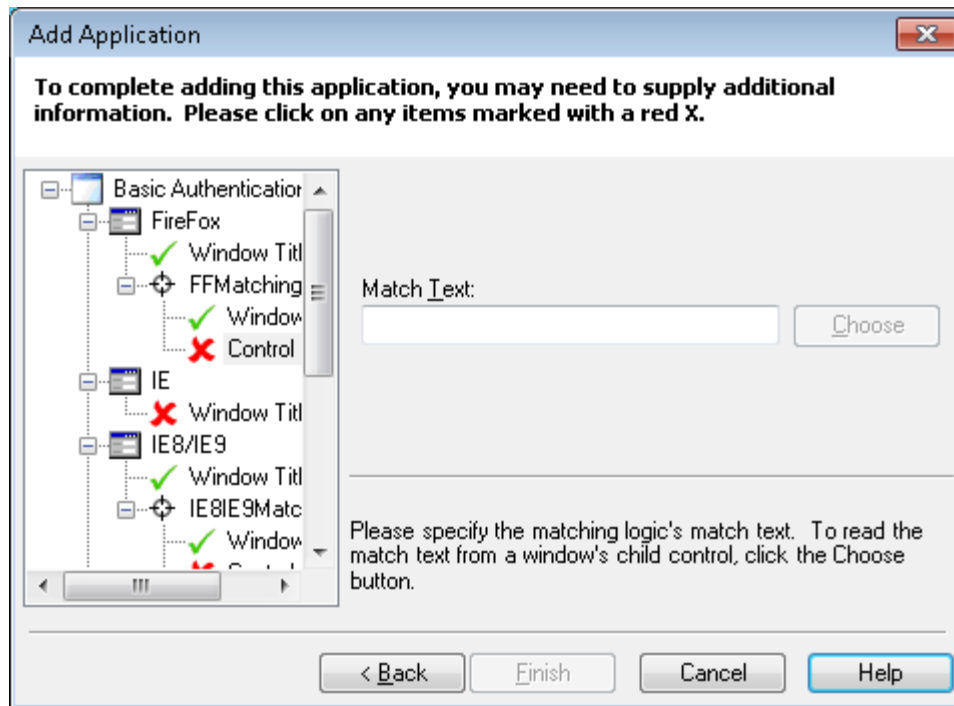
1. In the left pane of the dialog, click a logon setting item that is marked by a red **X**. The corresponding dialog for supplying the setting appears in the right pane.

2. Enter or choose the requested setting. A green check mark replaces the red **X** when the setting is completed.

3. Click **Finish** to close the wizard and add the new application.

To display this page:

1. Do one of the following:

- Right-click **Applications** in the left pane, then choose the application type (**Windows**, **Web** or **Host/Mainframe**) from the shortcut menu.

  or

- Click **Add** in the **Applications** list.

2. In the **New Application** dialog, select a template from the **Application** drop down list and click **Next**.

2.13.3 Creating a New Windows or Java Application Template

You can create a new Windows application template using the **Applications** menu or the **Add Application** icon in the Administrative Console, or directly from the window of an open application.

2.13.3.1 Creating a Template Using the Administrative Console

To create a Windows or Java application template using the Administrative Console:

1. In the left pane, right-click **Applications** then select **New Windows App** from the shortcut menu. The **Add Application** dialog appears with the **Windows** option selected.

2. Enter a **Name** for the new logon and click **OK**. The Windows Form Wizard (for configuring new logon forms) appears.

or

1. Click the **Add Application** icon on the Administrative Console toolbar.

2. Select an application from the **Select Window** screen. The Windows Form Wizard (for configuring new logon forms) appears.

Continue to The Windows Form Wizard for more information.

2.13.3.2 Configuring a Template Manually

To create a Windows or Java application template manually:

1. Enter the **Name** of the application.

2. In the **AppPathKey** group, click **Add**.

3. In the **Add AppPathKey** dialog, enter a valid application key (usually the application executable's name, such as Eudora.exe). Click **OK**.

4. In the Window Titles group click **Add**, then enter the Window title or click **Choose** to open the **Select Window** dialog, where you can select a title from a currently-running application window.

5. Click **OK**.

2.13.3.3 Creating a Template Using an Open Application

You can create a new template on-the-fly for a Windows application while the application is running.

In order to perform this procedure, both the Administrative Console and the Logon Manager Agent must be running, and you must configure the Agent settings to display the Title Bar Button menu.

1. Launch the application for which you want to create a template.

2. Select **Create Template** from the application's Title Bar Button menu.

Two things happen:

- In the application's window, Logon Manager detects the credential fields and highlights them.

- A condensed version of the Form Wizard appears. Enter information for the following fields:

    – **Form Name.** This field is pre-filled with the name of the selected application. You can leave this as it is or change it if you want to.

    – **Form Type.** Select the form type from the drop-down menu:

    Logon

    Logon Success

    Logon failure

    Password change

    Password change success

    Password change failure

    – **Add to Template.** This field defaults to the New Template selection. Alternatively, the drop-down menu contains the list of all configured Windows application templates to which you might want to add this form.

    – **Edit Fields/Hide Details.** Toggle this button to expand the window to display the entire Form Wizard, or collapse the window to the simpler Form Wizard.

Continue to for more information.

2.13.4 The Windows Form Wizard

Use the Windows Form Wizard to perform any of these tasks:

- Configure new logons for Windows applications or for Java applets and applications

- Add new forms to existing logons

- Create forms for automatic password changes

- Create forms for supporting a password confirmation field displayed in a separate window

- Create forms for automatic detection of password change success and failure

The Windows Form Wizard lets you use the application itself to identify its forms, the individual fields, and the submit **OK** button.

Before you begin this procedure, refer to the General Guidelines for Setting Up Applications for configuring applications. Also see Adding Windows Applications for specific information about configuring Windows application logons.

To display the Windows Form Wizard, do one of the following:

- Create a new Windows or Java application logon.

  or

- In the **Identification tab (Windows)**, click **Wizard**.

To configure a form:

1. Start the target application and navigate to the target form. Arrange the Administrative Console and target application windows so that you can see both at the same time.

2. In the Form Wizard, select the type of form you want to configure. The available options are:

   - **Logon.** Configures a logon form.

   - **Logon success.** Configures a form that detects a match during silent credential capture. In the presence of this form, the Agent delays credential capture until it verifies the user's entries and displays the **Logon Success** dialog. If this form is not present, the Agent captures credentials immediately after the user enters them and clicks **OK**.

   - **Logon failure.** Configures a form that detects a non-match during silent credential capture. In the presence of this form, the Agent delays credential capture until it verifies the user's incorrect entries and displays the **Logon Failure** dialog. If this form is not present, the Agent immediately informs the user that the credentials are incorrect, displaying either the **New Logon** dialog or the **Retry Logon** dialog to allow the user to re-enter credentials.

   - **Password change.** Configures a password change form.

   - **Password confirmation.** Configures a new password confirmation form for applications that display their "Confirm password" field in a separate window.

   - **Password change success.** Configures a form that serves as a match for the target application's password change success message. Since this form does not inject credentials, the **Credentials** page of the Windows Form Wizard is skipped. When the password change success message is detected, Logon Manager will automatically save the new credentials.

   - **Password change failure.** Configures a form that serves as a match for the target application's password change failure message and reinjects credentials when the password change failure message is detected. If you select this option, you will be presented with the **Credentials** page of the Windows Form Wizard in which you will configure the necessary fields.

     Refer to *Configuring and Diagnosing Logon Manager Application Templates* for a full discussion on using the forms above.

3. Specify whether the application that you are configuring is running on the **Local Computer** or a **Remote Computer**. If you select **Remote Computer**, enter the path to the application.

> **Note:** Logon Manager must be running on the computer you select.

4. In the **Application Window** list, select the window to configure. Note that a blinking outline indicates the application window you select.

   Use the **Application type:** dropdown menu to filter the list. An application is classified as either:

   - A standard Windows application.

   - A Java, SAP, or Modern UI application.

5. Confirm that you have selected the correct window, then click **Next**.

6. In the **Credential Fields** page list, click the **Detect Fields** button. The Wizard attempts to detect and configure the credential fields and marks them accordingly:

   - Username/ID

   - Password (Logon forms only)

   - Old Password (password change forms only)

   - New password (password change forms only)

   - Confirm new password (password change and password confirmation forms only)

   - Submit button

7. Confirm that the Wizard has selected the correct fields. You can modify a selection, if necessary:

   a. Select a field to configure; for example, the logon window's user ID field. In the application's window, a blinking outline indicates the field corresponding to your current selection.

   b. Confirm that you have selected the correct field, then right-click the selected item and choose the field type (for example, UserID) from the shortcut menu. The corresponding icon appears to the left of the item. To deselect an item, right-click the item and choose **None** from the shortcut menu.

   > **Note:** Password change success forms do not inject credentials and thus do not require you to configure any fields. In such cases, proceed to step 8, as the **Credential Fields** page will not be displayed.
   >
   > The **Class** and **Text** columns provide cues to the fields. For example, text boxes appear as "Edit" Class; password fields usually have the Text value *** HIDDEN ***.

8. Repeat this process for each field required to complete the logon form. You can configure up to four fields in all.

9. Confirm that you have configured the necessary fields and button, then click **Next** A summary page appears, listing your configuration.

10. Do one of the following:

    - Click **Back** to return to a previous page and make corrections.

    - Click **Finish** to complete the logon configuration and close the Form Wizard.

2.13.4.1 Selecting the Window Title

Use the **Select Window** dialog to choose the title of an application's logon or password change window.

Select the logon or password change window and click **OK**.

Control	Function
Window List	Displays the windows of currently applications. Click on the column heads to sort the list.
Show hidden window	Select to include hidden windows in the Window list.

2.13.4.2 The Windows Form Wizard Application Tab

Use this Form Wizard page to select the application's logon or password/PIN change window.

Control	Function
Window List	Displays the windows of currently available applications. Click on the column heads to sort the list.
Show hidden window	Select to include hidden windows in the Window list.
Refresh	Updates the list.
Back	Go back to the previous Wizard page.
Next	Go forward to the next Wizard page.

2.13.4.3 The Windows Form Wizard Credential Field Tab

Use this Form Wizard page to select the fields of the application's logon or password change window.

Control	Function
Credential Fields	Displays the fields of the currently selected application window. Click on the headers (Class, ID or Text, to sort the list. Right-click a field in the list to display a shortcut menu of field types and the submit control: ■ UserID ■ Password ■ Third Field ■ Fourth Field ■ Confirm New Password ■ OK (submit control)
Refresh	Updates the field list.
Use "Send Keys" for this form, do not use Control IDs	Indicates that the Agent should transmit logon data to this form as a series of keystrokes, rather than by addressing individual fields by Control ID. See SendKeys for more information.
Use ordinals instead of Control IDs	Indicates that the Agent should transmit data to this form as a series of numbered Control IDs assigned by Logon Manager, rather than addressing individuals fields generated by native Control IDs.

Control	Function
Detect Fields	Scans the field list and attempts to match them with field types. Note that although Detect Fields is usually accurate with typical applications, the fields should be verified for proper field types.
Refresh	Updates the field list.
Back	Go back to the previous Wizard page
Next	Go forward to the next Wizard page.

The Summary screen displays the results of the Wizard. Do one of the following:

- Click **Finish** to save your settings and close the Wizard.

   or

- Click **Back** to return to a previous page and modify your settings.

2.13.4.4 Windows Form Wizard for RSA SecurID Applications

Use the Windows Form Wizard to perform any of these tasks:

- Configure new logons for RSA SecurID Windows applications

- Add new forms to existing RSA SecurID logons

- Create forms for automatic PIN changes

- Create forms for supporting a PIN confirmation field displayed in a separate window

- Create forms for automatic detection of PIN change success and failure

The Windows Form Wizard lets you use the application itself to identify its forms, the individual fields, and the submit **OK** button.

Before you begin this procedure, refer to the General Guidelines for Setting Up Applications for configuring applications. Also see Adding Windows Applications for specific information about configuring Windows application logons.

To display the Windows Form Wizard, do one of the following:

- Create a new Windows or Java application logon. Be sure to select the **RSA SecurID** check box in the **Add Application** dialog.

   or

- In the **Identification** tab (for a Windows form), click **Wizard**.

To configure a form:

1. Start the target application and navigate to the target form. Arrange the Administrative Console and target application windows so that you can see both at once.

2. In the Form Wizard, select the type of form you want to configure. The available options are:

   - **SecurID Logon.** Configures a SecurID logon form.

   - **PIN Change.** Configures a PIN change form.

   - **Confirm PIN.** Configures a new PIN confirmation form for applications that display their "Confirm PIN" field in a separate window.

- **Logon Success.** Configures a form that serves as a match for the target application's Logon Success message. Since this form does not inject credentials, the **Credentials** page of the Windows Form Wizard is skipped. When the logon success message is detected, Logon Manager will automatically save the new credentials.

- **Logon Failure.** Configures a form that serves as a match for the target application's logon failure message and reinjects credentials when the logon failure message is detected. If you select this option, you will be presented with the **Credentials** page of the Windows Form Wizard in which you will configure the necessary fields.

- **PIN Change Success.** Configures a form that serves as a match for the target application's PIN change success message. Since this form does not inject credentials, the **Credentials** page of the Windows Form Wizard is skipped. When the PIN change success message is detected, Logon Manager will automatically save the new credentials.

- **PIN Change Failure.** Configures a form that serves as a match for the target application's PIN change failure message and reinjects credentials when the PIN change failure message is detected. If you select this option, you will be presented with the Credentials page of the Windows Form Wizard in which you will configure the necessary fields.

3. In the **Application Window** list, select the window to configure. Note that a blinking outline indicates the application window you select.

4. Specify whether the application is running on the **Local Computer** or a **Remote Computer**. If you select **Remote Computer**, enter the path to the application.

> **Note:** Logon Manager must be running on the computer you select.

---

5. In the **Application Window** list, select the window to configure. Note that a blinking outline indicates the application window you select.

   Use the Application type: dropdown menu to filter the list. An application is classified as either:

   - A standard Windows application.

   - A Java, SAP, or Modern UI application.

6. Confirm that you have selected the correct window, then click **Next**.

7. In the **Credential Fields** page, for each credential field:

   a. Select a field to configure; for example, the logon window's user ID field. In the application's window, a blinking outline indicates the field corresponding to your current selection.

   b. Confirm that you have selected the correct field, then right-click the selected item and choose the logon field type (for example, UserID) from the shortcut menu. The corresponding icon appears to the left of the item. To deselect an item, right-click the item and choose **None** from the shortcut menu.

> **Note:** New PIN Acceptance forms do not inject credentials and thus do not require you to configure any fields. In such cases, proceed to step 7, as the **Credential Fields** page will not be displayed.
>
> The **Class** and **Text** columns provide cues to the fields. For example, text boxes appear as "Edit" Class; PIN fields usually have the Text value *** HIDDEN ***

8. Repeat this process for each field required to complete the logon form. You can configure up to four fields in all.

9. Confirm that you have configured the necessary fields and button, then click **Next**. A summary page appears, listing your configuration.

10. Do one of the following:

    ■ Click **Back** to return to a previous page and make corrections.

    ■ Click **Finish** to complete the logon configuration and close the Form Wizard.

2.13.4.4.1 Credential Field (Windows Form Wizard for RSA-securID Applications) Use this Form Wizard page to select the fields of the application's logon or password change window.

Element	Function
Credential Fields	Displays the fields of the currently selected application window. Click on the headers (Class, ID, or Text, to sort the list. Right-click a field in the list to display a shortcut menu of field types and the submit control: ■ SecurID Username ■ Passcode ■ Tokencode ■ Next Passcode ■ Next Tokencode ■ Confirm New PIN ■ SecurID Other Field ■ OK (submit control)
Refresh	Updates the field list.
Use "Send Keys" for this form, do not use Control IDs	Indicates that the Agent should transmit logon data to this form as a series of keystrokes, rather than by addressing individual fields by Control ID. See SendKeys for more information.

Element	Function
Refresh	Updates the field list.
Back	Go back to the previous Wizard page
Next	Go forward to the next Wizard page.

2.13.4.5 The Windows Form Wizard Identification Tab

Use the **Identification (Windows)** tab to modify program and window information about a Windows application logon configuration.

■ Configure a logon manually by adding, editing, or deleting entries in the **AppPathKeys** and **Window Titles** lists.

or

■ Use The Windows Form Wizard to define windows, titles and fields by pointing and clicking.

To display this tab, do one of the following:

1. Create a new Windows application logon.

or

1. In the left pane, click **Applications** and select a Windows application.

2. Click the **General** tab in the right pane.

3. Select a logon form from the list and click **Edit**.

The Windows form-configuration dialog appears, displaying the **General** tab.

Control	Function
Form name	Name of the application logon form.
AppPathKeys	The Windows registry key identifying an application associated with this logon to match against running processes. (Usually the application executable's name.)
Window Titles	Text matched against logon window titles to identify logon requests. Click **Choose** to select a title from a currently-running application window.
Disabled	Select to disable this Windows template. This can be used with the Sort Order feature to disable certain Web pop-ups.
	This feature is useful in a situation where an application has hundreds of windows titles defined using regular expressions (see Regular Expression Syntax for more information) or wild cards, but a few of those window titles should not be responded to.
	Rather than creating hundreds of templates to respond to, an administrator can define the window title to match (with regular expressions or wild cards), and exclude those that should not be matched by creating a disabled template for them.
Wizard	Start the Windows Form Wizard for configuring an application visually.

2.13.4.6 The Windows Form Wizard Fields Tab

Use the **Fields (Windows)** tab to define how the Agent interacts with the fields of the logon form. You can identify one of the following for the currently-selected application form:

■ Up to four logon fields (user ID, password, etc.), using Control IDs

■ A series of keystrokes (with optional timings) that fill-in and submit the logon form, using SendKeys.

To display this tab, do one of the following:

1. Create a new Windows application logon.

or

1. In the left pane, click **Applications** and select a Windows application.

2. Select the **General** tab in the right pane.

3. Select a logon form from the list and click **Edit**.

4. In the Windows form-configuration dialog General tab, click the **Fields** tab.

Control	Function
Transfer Method (choose one)	■ Use standard Windows Control IDs to identify and transmit credentials to a field. Click **Add** to add a field and enter its Control ID, or **Edit** to modify existing field settings.
	■ Configure fields by transmitting a keystroke series to the form. Click **Edit** to enter or change the series.
	■ Configure fields by transmitting a keystroke series to the form using Journal Hook. Click **Edit** to enter or change the series.
Fields	Fields with transfer methods configured for this logon form. You can:
	■ Select a field and click **Edit** to modify Control ID, SendKeys, or SendKeys using Journal Hook settings.
	■ Click **Add** to add a field (for Control ID only).

2.13.4.6.1 The ControlID Dialog Use the Control ID dialog to identify the fields and the submit button of a logon form in order to configure the Manager's response.

Control	Function
Field	Select the credential data that the control represents, or identify the control as the **Submit** (**OK**) button.
	■ UserID
	■ Password
	■ Third Field
	■ Fourth Field
	■ OK (submit control)
Control ID	Enter the Control ID of the selected field or button.
Skip field if control is disabled	Select this option to prevent the Agent from entering data if the selected field is set not to accept user entry.

To display this dialog, do one of the following:

1. Create a new Windows application logon.

or

1. In the left pane, select **Applications** and select a Windows application.

2. Select the **General** tab in the right pane.

3. Do one of the following:

■ Select a logon form from the list and click **Edit**.

or

■ Click **Add** to configure a new form.

4. From the **Windows form configuration** dialog **General** tab, do one of the following:

■ Click the **Fields** tab, select **Control IDs** as the Transfer Method, then click **Edit**.

or

■ Click the **Matching** tab, click **Add**, then click **Control ID**.

2.13.4.7 SendKeys for a Windows Application Logon

Use the **SendKeys** dialog to specify a series of keystrokes that Logon Manager should transfer to the logon form.

Use the SendKeys option for Windows applications that:

- Cannot receive credentials from the Windows message queue or by other techniques the Agent normally uses to send credentials.

- Do not use standard Windows controls that have Control IDs.

- Dynamically generate controls or do not use Windows controls at all (for example, Flash applications).

The **New Actions** list box in the right pane of the **SendKeys** dialog provides the keystroke options for each action. Highlight the action for which you want to configure SendKeys, and select or type the options you need on for each action. Click the **Insert** button to add the key or action to the series.

> **Note:**   **For East-Asian Language Applications:** When adding information using SendKeys in an East Asian-language (Chinese, Japanese, Korean) application template, you must insert an **Enter** key press preceding the **Tab** key that advances to the next field. The **Enter** key signals the Input Method Editor that you have completed the field and allows the IME to differentiate the credentials fields.
>
> Journal Hook SendKeys for East-Asian languages is not compatible with Logon Manager.

Your selections appear in the **Current Actions** list in the left pane:

- To change the order of the series, select an item and click the **Up** or **Down** arrows to move it.

- To delete an item, select it, and click **Delete**.

- To edit an item, select it, and click **Edit**. The **Edit Action** dialog opens. Edit the fields as necessary and click **OK**.

New Action	Control	Function
Fields	Field Type	Select a credential item from the list to add to the series. ■ UserID ■ Password ■ Third Field ■ Fourth Field ■ Old Password ■ New Password ■ Confirm New Password
	Character to insert after field	Select a keystroke to insert automatically after the field is filled: ■ None (no keystroke) ■ Enter (to submit the form) ■ Tab (to advance the cursor) Also see Special Keys, below.

New Action	Control	Function
	Inject directly into control	Injects the credential directly into the control. Click the ellipsis ("**…**") button to open the **Choose Control ID** dialog. **Note:** When using SendKeys, the application is treated as a Windows application. The controls that appear in the **Choose Control ID** dialog indicate whatever Windows controls Logon Manager can find.
	Insert	Add the current selection to the series.
Click	Click at a coordinate	Simulates a mouse click at the X, Y coordinate specified. X: Choose the X coordinate for the mouse click. Y: Choose the Y coordinate for the mouse click. Relative to the: Select where the mouse click will be relative to: ■ Screen ■ Active Window Mouse button: Select which mouse button will be clicked: ■ Left ■ Middle ■ Right
	Click on a control	This option is similar to clicking at a specified coordinate, except that Logon Manager determines where the control is and simulates a click in the center of the control. Click the ellipsis ("**…**") button to open the **Choose Control ID** dialog. **Note:** When using SendKeys, the application is treated as a Windows application. The controls that appear in the **Choose Control ID** dialog indicate whatever Windows controls Logon Manager can find.
	Insert	Add the click selection to the series.
Run Task	Command line to run	Enter a Command line to be executed. This feature allows you to run a program in the middle of entering keystrokes. ■ Window Handles can be appended to the command line to inform the script of the window handle currently being worked on: `$(HWND)` ■ Environment Variables can also be appended to the command line: `$(USERDOMAIN)\$(USERNAME)` Click the ellipsis ("**…**") button to open the **Choose Control ID** dialog. **Note:** Virtual key codes cannot be used within the command line (the initial backquote character will terminate the command line).
	Expected return code	Enter the expected return code. The rest of the SendKeys script is discarded if this value is not returned.

New Action	Control	Function
	Time out (sec.)	Enter the number of milliseconds to wait for the task to complete. The rest of the Sendkeys script is discarded if this timeout is reached. The maximum timeout period is five (5) seconds.
	Insert	Add the task to the series.
Delay	Length of delay (in seconds)	Type or select a delay between keystrokes.
	Insert	Add the delay to the series.
Set Focus	Set focus to control	Sets the focus to the control. Click the ellipsis ("**…**") button to open the **Choose Control ID** dialog.
		Note: When using SendKeys, the application is treated as a Windows application. The controls that appear in the **Choose Control ID** dialog indicate whatever Windows controls Logon Manager can find.
	Insert	Add the focus to the series.
Text	Enter text to insert	Type any literal text to add to the series.
	Insert	Add the text to the series.
Special Keys	Category/Keys	Choose a keystroke category (for example, Movement keys) from the left list, then a specific key (for example, Page Down) from the right list.
	Key Press	Insert the key as a single keystroke (default).
	Key Down/Up	Insert the key as a pair of actions: key-press and key-release. This option lets you insert other keystrokes between these actions to indicate one or more keys held down as another is typed, as for a "hot key" combination that moves the focus to a specific text box.
		For example, to insert the keystroke Alt+P, select the **Key Down/Up** option, then select **Modifier** for the Category and **Alt** for the Key. and click **Insert**. This inserts two actions: [Down:Alt] and [Up:Alt].
		Select the **Text** tab and enter **P** in the text box. In the left pane, select **[Up:Alt]** and click **Insert**. The **P** is inserted between the two **Alt-key** actions, producing **Alt-P**.
	Insert	Add the keystroke to the series.

To display this dialog, do one of the following:

1. Create a new Windows application logon.

or

1. In the left pane, click **Applications** and select a Windows application.

2. Click the **General** tab in the right pane.

3. Do one of the following:

   ■ Select a logon form from the list and click **Edit**.

   or

- Click **Add** to configure a new form.

  The **Windows form-configuration** dialog opens, displaying the **General** tab.

4. Click the **Fields** tab, select **SendKeys** as the Transfer Method, then click **Edit**.

2.13.4.8 Kiosk Manager SendKeys (for a Windows Application)

Use the **SendKeys** dialog to specify a series of keystrokes that Kiosk Manager should transfer to the logon form.

> **Note:** See Adding Telnet Applications for information about configuring logons for Telnet applications.

The tabs in the right pane of the SendKeys dialog provide the keystroke options. Select or type the options you need on each tab. Click the **Insert** button to add the key or action to the series.

Your selections appear in the list in the left pane. To change the order of the series, select an item and click the up or down arrows to move it. To delete an item, select it and click **Remove**.

Controls

Tab	Function	Input
Text tab	Enter text to insert	Type any literal text to add to the series.
	Insert	Add the text to the series.
Delay tab	Length of delay (in seconds)	Type or select a delay between keystrokes.
	Insert	Add the delay to the series.

Tab	Function	Input
Special Keys tab	Category/Keys	Choose a keystroke category (for example, Movement keys) from the left list, then a specific key (for example, Page Down) from the right list.
	Key Press	Insert the key as a single keystroke (default)
	Key Down/Up	Insert the key as a pair of actions: key-press and key-release. This option lets you insert other keystrokes between these actions to indicate one or more keys held down as another is typed, as for a "hot key" combination that moves the focus to a specific text box.
		For example, to insert the keystroke "Alt+P", choose the **Key Down/Up** option, then select **Modifier** for the Category and **Alt** for the Key. and click Insert. This inserts two actions: [Down:Alt] and [Up:Alt]. Select the **Text** tab and type **P** in the text box. In the left pane, select [**Up:Alt**] then click **Insert**. The P is inserted between the two Alt-key actions, producing "Alt-P."
	Insert	Add the keystroke to the series.

2.13.4.9 Matching Tab for Configuring a Windows Application

Use the **Matching (Windows)** tab to distinguish among similar forms within the same Windows application. The supported form types, referred to here as target forms, are:

- Logon

- Password Change

- Password Confirmation

- Logon Success

- Logon Failure

- Password Change Success

- Password Change Failure

> **Note:** Unlike the "Logon," "Change Password," "Confirm," and "Ignore" match types, these matches cannot be explicitly selected by the user. They are determined by form type.

Controls

Element	Function
Allowable Class	Click **Choose** to identify the logon or password-change window class that must be present in order to execute this logon. This is useful for applications that present logon or password-change windows with non-standard class names. Displays the **Select Window** dialog.
Regular Expression	Select whether the Allowable Class uses a regular expression.
Ignore this Window Class	Click **Choose** to select the logon or password-change window to ignore when executing a logon. This is useful for applications that use hidden logon or password-change dialogs or that present duplicate dialogs. Displays the **Select Window** dialog.
Regular Expression	Select if the ignored Window Class uses a regular expression.
Attach to window's Message Queue	Select to hold on to the target window while sending credentials.
Preset Focus	Select to set the focus on a logon field before the Agent places data in the field.
System Logon	(Reserved)
Use WM_CHAR messages to fill controls	Some applications require that you enter passwords via a keyboard and not set text commands. Enabling this setting simulates keyboard entry in an alternate way by setting text within controls.
Allow fallback from ControlIDs to SendKeys	Indicates whether to use SendKeys to enter credentials if direct injection using ControlIDs fails. Default is Yes.
Sort Order	Specify the order in which Logon Manager searches templates for window class titles containing regular expressions. By setting sort order, you increase the efficiency of your search without eliminating less precise matches. If you do not assign a sort order to a template, Logon Manager checks templates in ascending order (lower values are checked first). Default is 1000.

The Agent uses the match criteria you supply to distinguish among similar forms. This lets the Agent apply a single set of user credentials appropriately to these multiple forms. You can use also use matching to identify forms that the Agent should ignore.

Do one of the following:

- Click **Add** to create a new matching criterion.

  or

- Select a **Match** and click **Edit**.

  The **Matching** dialog appears.

  Note: The easiest and most efficient way to create match criteria is by using the **Control Match Wizard**. The Wizard lets you specify match criteria by selecting elements from the target form itself. You can also create and modify match criteria manually.

To display this tab, do one of the following:

- Create a new Windows application logon.

or

1. In the left pane, click **Applications** and select a Windows application.

2. Click the **General** tab in the right pane.

3. Select a form from the list and click **Edit**.

4. Select the **Matching** tab.

2.13.4.10 The Windows Form Wizard Matching Dialog

Use this dialog to create match criteria that the Agent uses to distinguish among similar target forms that use the same credential data. This lets the Agent apply a single set of user credentials appropriately to these multiple forms. To display this dialog, from the **Matching** tab (for configuring a Windows logon form) click **Add**.

The easiest and most efficient way to create match criteria is through the Control Match Wizard. The Wizard lets you specify match criteria by selecting elements from the target form itself. You can also create and modify match criteria manually.

2.13.4.11 Creating Match Criteria Using the Wizard

Click **Wizard** and follow the onscreen instructions.

2.13.4.12 Creating or Modifying Match Criteria Manually

To create or modify matching criteria manually:

1. Enter a **Match name** and select the **Type** of target form.

2. Add or edit the Window Titles that the target form displays, or select **Use Titles** from **Main**.

3. Add or edit the Control Matching items; these are criteria based on the properties of form objects (such as a text caption or a control class). Together these items uniquely identify the target form.

4. Add or edit the **Control IDs** of the target form's credential fields.

5. Click **OK**.

Control	Function
Match Name	Enter or edit the name for the Match
Type	Select the type of form to match: ■ Logon ■ Change Password ■ Confirm (Password) ■ Ignore ■ Logon Success ■ Logon Failure ■ Password Change Success ■ Password Change Failure **Note:** Unlike the Logon, Change Password, Confirm, and Ignore match types, these matches cannot be explicitly selected by the user. They are determined by form type.
Windows Titles	Click **Use Titles from Main** to copy the Windows Titles in the General tab for this logon or click **Add** to enter titles manually.
Control Matching	Click **Add** (or select a matching item and click **Edit**) to display the **Control Matching** dialog.

Control	Function
Control ID	Click **Add** (or select a Control ID item and click **Edit**) to display the **Control ID** dialog.
Wizard	Start the Control Match Wizard.

2.13.4.13 Add or Edit a Title on the Windows Matching Tab

Use this dialog to add or modify the text string that the Agent uses to detect specific application windows (for example, for logon entry or password change) by their window title.

2.13.4.13.1 Specifying a Window Title for Matching To specify a window title for matching:

1. Select one of the following (see Matching Expressions).

    ■ Exact match

    ■ Use wildcards (does not apply to Kiosk Manager)

    ■ Use regular expression (does not apply to Kiosk Manager)

2. Type (or edit) the **Window Title** or a matching expression.

3. Click **OK**.

2.13.4.13.2 Matching Expressions For applications that have varying text in their URLs, you can use substrings or regular expressions to specify how to match the variable text.

Element	Usage
Wildcards	■ **?** (question mark) matches any single character.
	■ ***** (asterisk) matches zero or more occurrences of any character.
	Note: This does not apply to Kiosk Manager.
Regular Expressions	You can also use the set of regular expressions to specify a string pattern that the Agent should recognize as a match.
	Note: This does not apply to Kiosk Manager.

2.13.4.13.3 Matching Environment Variables For applications that include the user's name in the URL (as derived from the DOMAINUSER environment variable in the workstation operating system), select **Exact** as the matching criterion, and use one of the following substitution tokens in the match string:

Variable	Usage
%DOMAINUSER%	User name exactly as derived from the environment variable
%UC%%DOMAINUSER%	User name converted to all upper case
%LC%%DOMAINUSER%	User name converted to all lower case

Example

The following Window Title entry matches a password-change window title that includes the username:

```
Password Expired - %UC%%DOMAINUSER%
```

2.13.4.14 Control Matching

Use the **Control Matching** dialog to specify a match criterion based on the properties of a target-form control (such as a text caption or a control style).

Control	Function		
Control ID	Type the numeric identifier of the control.		
Match Condition	Select one property of the control, select a relation (**Equals** or **Not Equal**, **Equals regular expression**, **Not equals regular expression**), and type or select the condition that should (or should not) be met. The valid conditions for each property are:		
	Class	**Edit** or **Static** control.	
	Style	A decimal numeric identifier for the aggregate of styles applied to the control.	
	Text	A literal string.	

Click **OK** to save and exit the dialog or **Cancel** to exit without changes.

2.13.4.15 Control ID Dialog (Windows Fields Tab)

Use the **Control ID** dialog to identify the fields and the **Submit** button of a logon form in order to configure the Agent's response.

Control	Function
Field	Select the credential data that the control represents, or identify the control as the **Submit** (**OK**) button. ■ UserID ■ Password ■ Third Field ■ OK (submit control) ■ Fourth Field
Control ID	Enter the Control ID of the field or button.
Control Type	Select the control type: ■ Edit (text box) ■ Combo (drop-down list box) ■ List

> **Note:**   In most cases, you can use the Windows Form Wizard to identify fields and Control IDs.

2.13.4.16 Control Match Wizard

Use the Control Match Wizard to define match criteria by choosing from the windows and controls of the target application. The Agent uses match criteria to identify a target form, such as a password-change dialog, that is similar to the currently selected logon. The Agent then supplies data to the matched target form using the same credentials as the original logon. You can also use match criteria to specify target forms similar to the current logon that the Agent should ignore.

To create match criteria using the Wizard:

1. Start the target application and navigate to the target form. Arrange the Administrative Console and target application windows so that you can see both at the same time.

2. Select a form **Match Type**, then follow the onscreen instructions or help topics.

   ■ Ignore

   ■ Logon

   ■ Password Change

   ■ Password Confirm

See the Matching Tab for Configuring a Windows Application for more information.

To display the Control Match Wizard:

1. From the **Matching** tab, select **Add** (for configuring a Windows logon form). The Matching dialog appears.

2. Click **Wizard**.

2.13.4.17 Ignore App Window

Use this Wizard page to choose the application window that the Agent should recognize.

1. Select the application window that the Agent should ignore from the Window List.

2. Click **Next** to display the Match Fields page.

Control	Function
Window List	Displays the windows of currently applications. Click on the column heads to sort the list.
Show hidden window	Select to include hidden windows in the Window list.
Refresh	Updates the list.
Back	Go back to the previous Wizard page.
Next	Go forward to the next Wizard page.

2.13.4.18 Ignore Match Fields

Use this Wizard page to choose a set of match fields: one or more window objects that uniquely identify the application window that the Agent should recognize. You can identify a match field by its Class (the type of control, such as Edit or Static), its Style (the aggregate of its properties identified by a number), or its Text.

1. In the field list, right-click a field and select the match criteria.

2. Click **Next** to display the **Summary** page.

Control	Function
Match Fields	Displays the fields of the currently selected application window. Click on the headers (**Class**, **ID**, **Text** or **Style**) to sort the list. Right-click a field in the list to display a shortcut menu of match criteria: ■ None (deselect field) ■ Class ■ Style ■ Text
Use ordinals instead of Control IDs	Indicates that the Agent should transmit data to this form as a series of numbered Control IDs assigned by Logon Manager, rather than addressing individuals fields generated by native Control IDs.
Refresh	Updates the list.
Back	Goes back to the previous Wizard page.
Next	Goes forward to the next Wizard page.

2.13.4.19 Logon App Window

Use this Wizard page to choose the application window that the Agent should recognize.

1. Select the application window that the Agent should recognize as a logon form from the Window List.

2. Click **Next** to display the Match Fields page.

Control	Function
Window List	Displays the windows of currently applications. Click on the column heads to sort the list.
Show hidden window	Select to include hidden windows in the Window list.
Refresh	Updates the list.
Back	Go back to the previous Wizard page.
Next	Go forward to the next Wizard page.

2.13.4.20 Logon Match Fields

Use this Wizard page to choose a set of match fields: one or more window objects that uniquely identify the application window that the Agent should recognize. You can identify a match field by its Class (the type of control, such as Edit or Static), its Style (the aggregate of its properties identified by a number), or its Text.

1. In the field list, right-click a field and select the match criteria

2. Click **Next** to display the **Credentials** page.

Control	Function
Match Fields	Displays the fields of the currently selected application window. Click on the headers (**Class**, **ID**, **Text**, or **Style**) to sort the list. Right-click a field in the list to display a shortcut menu of field types: ■ None (deselect field) ■ Class ■ Style ■ Text
Use ordinals instead of Control IDs	Indicates that the Agent should transmit data to this form as a series of numbered Control IDs assigned by Logon Manager, rather than addressing individuals fields generated by native Control IDs.
Refresh	Updates the list.
Back	Go back to the previous Wizard page.
Next	Go forward to the next Wizard page.

2.13.4.21 Logon Credential

Use this Wizard page to identify the field in which the Agent should supply credential data.

1. In the field list, right-click a field and select the credentials.

2. Click **Next** to display the Summary page.

Control	Function
Credential Fields	Displays the fields of the currently selected application window. Click on the headers (**Class**, **ID**, **Text**, or **Style**) to sort the list. Right-click a field in the list to display a shortcut menu of field types: ■ None (deselect field) ■ UserID ■ Password ■ Third Field ■ Fourth Field
Use ordinals instead of Control IDs	Indicates that the Agent should transmit data to this form as a series of numbered Control IDs assigned by Logon Manager, rather than addressing individuals fields generated by native Control IDs.
Refresh	Updates the list.
Back	Go back to the previous Wizard page.
Next	Go forward to the next Wizard page.

2.13.4.22 Password Change App Window

Use this Wizard page to choose the application window that the Agent should recognize.

1. Select the application window that the Agent should recognize as a password-change form from the Window list.

2. Click **Next** to display the Match Fields page.

Control	Function
Window List	Displays the windows of currently applications. Click on the column heads to sort the list.
Show hidden window	Select to include hidden windows in the Window list.
Refresh	Updates the list.
Back	Go back to the previous Wizard page.
Next	Go forward to the next Wizard page.

2.13.4.23 Password Change Match Fields

Use this Wizard page to choose a set of match fields: one or more window objects that uniquely identify the application window that the Agent should recognize. You can identify a match field by its Class (the type of control, such as Edit or Static), its Style (the aggregate of its properties identified by a number), or its Text.

1. In the field list, right-click a field and select the match criteria

2. Click **Next** to display the **Credentials** page.

Control	Function
Match Fields	Displays the fields of the currently selected application window. Click on the headers (**Class**, **ID**, **Text**, or **Style**) to sort the list. Right-click a field in the list to display a shortcut menu of field types: ▪ None (deselect field) ▪ Class ▪ Style ▪ Text
Use ordinals instead of Control IDs	Indicates that the Agent should transmit data to this form as a series of numbered Control IDs assigned by Logon Manager, rather than addressing individuals fields generated by native Control IDs.
Refresh	Updates the list.
Back	Go back to the previous Wizard page.
Next	Go forward to the next Wizard page.

2.13.4.24 Password Change Credential

Use this Wizard page to identify the field in which the Agent should supply credential data.

1. In the field list, right-click a field and select the credentials.

2. Click **Next** to display the Summary page.

Control	Function
Credential Fields	Displays the fields of the currently selected application window. Click on the headers (**Class**, **ID**, **Text**, or **Style**) to sort the list. Right-click a field in the list to display a shortcut menu of field types: ▪ None (deselect field) ▪ UserID ▪ Old Password/PIN ▪ New Password/PIN ▪ Confirm Password/PIN

Control	Function
Use ordinals instead of Control IDs	Indicates that the Agent should transmit data to this form as a series of numbered Control IDs assigned by Logon Manager, rather than addressing individuals fields generated by native Control IDs.
Refresh	Updates the list.
Back	Go back to the previous Wizard page.
Next	Go forward to the next Wizard page.

2.13.4.25 Password Confirm App Window

Use this Wizard page to choose the application window that the Agent should recognize.

1. Select the application window that the Agent should recognize as a password-confirmation form from the Window list.

2. Click **Next** to display the **Match Fields** page.

Control	Function
Window List	Displays the windows of currently applications. Click on the column heads to sort the list.
Show hidden window	Select to include hidden windows in the Window list.
Refresh	Updates the list.
Back	Go back to the previous Wizard page.
Next	Go forward to the next Wizard page.

2.13.4.26 Password Confirm Match Fields

Use this Wizard page to choose a set of match fields—one or more window objects that uniquely identify the application window that the Agent should recognize. You can identify a match field by its Class (the type of control, such as Edit or Static), its Style (the aggregate of its properties identified by a number), or its Text.

1. In the field list, right-click a field and select the match criteria

2. Click **Next** to display the Credentials page.

2.13.4.27 Password Confirm Credential

Use this Wizard page to identify the field in which the Agent should supply credential data.

1. In the field list, right-click a field and select the credentials.

2. Click **Next** to display the **Summary** page.

Control	Function
Credential Fields	Displays the fields of the currently selected application window. Click on the headers (**Class**, **ID**, **Text**, or **Style**) to sort the list. Right-click a field in the list to display a shortcut menu of field types: ■ None (deselect field) ■ UserID ■ Old Password/PIN ■ New Password/PIN ■ Confirm Password/PIN
Use ordinals instead of Control IDs	Indicates that the Agent should transmit data to this form as a series of numbered Control IDs assigned by Logon Manager, rather than addressing individuals fields generated by native Control IDs.
Refresh	Updates the list.
Back	Go back to the previous Wizard page.
Next	Go forward to the next Wizard page.

2.13.4.28 Options Tab for Configuring a Windows Application

Use the **Options (Windows)** tab to refine properties of the currently-selected application logon form for special configurations.

To display this tab, do one of the following:

1. Create a new Windows application logon.

or

1. In the left pane, click **Applications** and select a Windows application.

2. Click the **General** tab in the right pane.

3. Select a logon form from the list and click **Edit**.

4. Select the **Options** tab.

Control	Function
Attach to window's Message Queue	Select to hold on to the target window while sending credentials.
Preset Focus	Select to set the focus on a logon field before the Agent places data in the field.
System Logon	(Reserved)
Use WM_CHAR messages to fill controls	Some applications require that you enter passwords via a keyboard and not set text commands. Enabling this setting simulates keyboard entry in an alternate way by setting text within controls.
Adhere to Logon Loop Grace Period	Select to have the Agent ignore this application's logon form when the logon loop grace period (set on the application's **Miscellaneous** tab) is in effect.
Fall back to SendKeys if direct injection fails	Indicates whether to use SendKeys to enter credentials if direct injection using Control IDs fails. Default is Yes.

Control	Function
Auto-Recognize	Select to have the Agent recognize the application automatically. If this setting is checked or unchecked, it overrides the Global Agent Setting. If this setting is checked, the user can configure this setting from the Logon Manager. If this setting is unchecked, the user will not have access to this setting from the Logon Manager.
Auto-Submit	Select to have the Agent automatically select **OK** for this application logon after providing credentials.
Sort Order	Specify the order in which Logon Manager searches templates for window class titles containing regular expressions. By setting sort order, you increase the efficiency of your search without eliminating less precise matches.

If you do not assign a sort order to a template, Logon Manager checks templates in ascending order (lower values are checked first). Default is 1000. |
| Detection Delay | The time interval that the Agent should wait before detecting the application fields. |

2.13.4.28.1 Select Window [Class] The **Select Window** dialog lets you select the class name for an onscreen window. Use this dialog to specify a window class that the Agent should allow or that it should ignore.

The **Select Window** dialog displays when you select one of the following options in the **Options** tab for a Windows logon.

- **Allowable Class.** Select a logon or password-change window class that must be present in order for the Agent to execute a logon.

- **Ignore this Window Class.** Select a logon or password-change window class that should be ignored when detecting credential fields.

Controls

Control	Function
Window List	Displays the windows of currently applications. Click on the column heads to sort the list.
Show hidden window	Select to include hidden windows in the Window list.

2.13.5 Creating a New Web Application Template

The Web Form Wizard simplifies the process of creating a new Web application template. You can launch the Web Form Wizard using the Applications menu or the **Add Application** icon in the Administrative Console, or directly from the window of an open application.

2.13.5.1 Creating a Template Using the Administrative Console

To create a template using the Administrative Console:

1. In the left pane, right-click **Applications** then select **New Web App** from the shortcut menu. The **Add Application** dialog appears with the Web option selected.

2. Enter a Name for the new logon and click **OK**. The Web Form Wizard (for configuring new logon forms) launches.

or

1. Click the **Add Application** icon (below) on the Administrative Console toolbar.

2. Select a Web application from the **Select Window** screen. The Web Form Wizard (for configuring new logon forms) launches.

2.13.5.2 Creating a Template Using an Open Application

You can create a new template on-the-fly for a Web application while the application is running.

In order to perform this procedure, both the Administrative Console and the Logon Manager Agent must be running, and you must configure the Agent settings to display the Title Bar Button menu.

1. Open a browser and navigate to the URL for which you want to create a template.

2. Select **Create Template** from the browser's Title Bar Button menu.
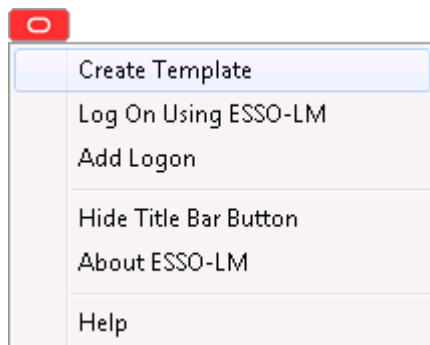
The Web Form Wizard (for configuring new logon forms) launches.

2.13.5.3 Web Form Wizard

The Web Form Wizard lets you browse the Web application itself to capture the identifiers for its logon or password-change windows, the individual fields, and the **Submit** (**OK)** button. To display the Web Form Wizard:

1. Create a New Web application.

2. In the **New Web Application** configuration dialog, click **Wizard**. The Web Form Wizard appears.

> **Note:** When using a workstation running at 800x600 resolution, buttons are missing from the bottom of the Web Form Wizard. The wizard is also extremely slow to start at this resolution. Oracle recommends that you set the resolution on your workstation to a higher resolution.

2.13.5.4 Configuring a Web Application Using the Wizard

To configure a Web Application with the Web Form Wizard:

1. In the first Wizard dialog that appears, select the type of application form you want to configure. The available options are:

- **Logon.** Configures a logon form.

- **Logon success.** Configures a form that detects a match during silent credential capture. In the presence of this form, the Agent delays credential capture until it verifies the user's entries and displays the **Logon Success** dialog. If this form is not present, the Agent captures credentials immediately after the user enters them and clicks **OK**.

- **Logon failure.** Configures a form that detects a non-match during silent credential capture. In the presence of this form, the Agent delays credential capture until it verifies the user's incorrect entries and displays the **Logon Failure** dialog. If this form is not present, the Agent immediately informs the user that the credentials are incorrect, displaying either the **New Logon** dialog or the **Retry Logon** dialog to allow the user to re-enter credentials.

- **Password change.** Configures a password change form.

- **Password confirmation.** Configures a form that verifies that the user's second password entry in a password change form is identical to the first password entry.

- **Password change success.** Configures a form that serves as a match for the target application's password change success message. Since this form does not inject credentials, the **Credentials** page of the Web Form Wizard is skipped. When the password change success message is detected, Logon Manager will automatically save the new credentials.

- **Password change failure.** Configures a form that serves as a match for the target application's password change failure message and reinjects credentials when the password change failure message is detected. If you select this option, you will be presented with the **Credentials** page of the Web Form Wizard in which you will configure the necessary fields.

  Refer to *Configuring and Diagnosing Logon Manager Application Templates* for a full discussion on using the forms above.

  Note: If you are editing an existing form, this dialog will not appear.

2. In the Web Form Wizard, enter the Web Address (URL) of the Web site and click **Go**. The top pane of the Wizard acts as a web browser window. You can resize the Wizard's window as needed.

3. In the top pane, navigate to the Web site's logon form. When the Wizard detects one or more forms in a web page, it lists the forms and their elements (fields and buttons) in the bottom pane.

4. Click the **Detect Fields** button. The Wizard attempts to detect and configure the credential fields and marks them accordingly:

- Username/ID
- Password
- Old Password (password change forms only)
- New Password (password change forms only)
- Submit button.

5. (Optional) Select **Use ordinals instead of names**. The **Credential Fields Screen** displays the fields, assigning Control IDs by location order instead of using native (dynamic) Control IDs.

6. (Optional) Select **Show non-input fields**. The Administrative Console detects fields that have input functionality but into which you cannot enter information, such as IMG tags that function as Submit buttons, and includes these fields in the Web Form Wizard fields list.

7. (Optional) Select **Allow multiple field designation**. The Administrative Console recognizes multiple fields that require the same credential, such as enter and confirm password fields, or a page with the same field on two forms.

8. Confirm that the Wizard has selected the correct fields. You can modify a selection, if necessary:

    a. If you are editing an existing template, you may change the form type using the **Form Type** drop-down at the lower right. Keep in mind that if you do so, you will need to reconfigure the template (reassign fields, and so on). Only fields relevant to a given form type are displayed when that form type is selected.

    b. Identify and select a field from the list in the bottom pane. (The Element and Type descriptions provide cues.) In the top pane, a blinking outline indicates the corresponding field or button you have selected.

    c. Confirm that you have selected the correct field, then right-click the selected item and choose from the shortcut menu (for example, UserID). An icon appears to the left of the item. To deselect an item, right-click the item and select **None** from the shortcut menu.

9. Confirm that the Wizard has selected the correct fields. You can modify a selection, if necessary:

    a. If you are editing an existing template, you may change the form type using the **Form Type** drop-down at the lower right. Keep in mind that if you do so, you will need to reconfigure the template (reassign fields, and so on). Only fields relevant to a given form type are displayed when that form type is selected.

    b. Identify and select a field from the list in the bottom pane. (The Element and Type descriptions provide cues.) In the top pane, a blinking outline indicates the corresponding field or button you have selected.

    c. Confirm that you have selected the correct field, then right-click the selected item and choose from the shortcut menu (for example, UserID). An icon appears to the left of the item. To deselect an item, right-click the item and select **None** from the shortcut menu.

10. Confirm that the Wizard has selected the correct fields. You can modify a selection, if necessary:

    a. If you are editing an existing template, you may change the form type using the **Form Type** drop-down at the lower right. Keep in mind that if you do so, you will need to reconfigure the template (reassign fields, and so on). Only fields relevant to a given form type are displayed when that form type is selected.

    b. Identify and select a field from the list in the bottom pane. (The Element and Type descriptions provide cues.) In the top pane, a blinking outline indicates the corresponding field or button you have selected.

    c. Confirm that you have selected the correct field, then right-click the selected item and choose from the shortcut menu (for example, UserID). An icon appears to the left of the item. To deselect an item, right-click the item and select **None** from the shortcut menu.

11. Repeat this process for each field required to complete the logon form. You can configure up to four fields in all.

12. Repeat the two previous steps for each field required to logon. You can configure up to four fields in all.

13. When you have completed your configuration click **OK** to save it and close the Web Form Wizard.

2.13.5.5 Web Form Wizard (for RSA SecurID Applications)

Use the Web Form Wizard to perform any of these tasks:

■ Configure new logons for RSA SecurID Windows applications

■ Add new forms to existing RSA SecurID logons

■ Create forms for automatic PIN changes

■ Create forms for automatic detection of PIN change success and failure

The Web Form Wizard lets you browse the Web application itself to capture the identifiers for its forms and windows, the individual fields, and the submit (OK) button. To display the Web Form Wizard:

1. Create a new Web application. Be sure to select the **RSA SecurID** check box in the **Add Application** dialog.

2. In the **New Web Application** configuration dialog, click **Wizard**. The Web Form Wizard appears.

> **Note:**   When using a workstation running at 800x600 resolution, buttons are missing from the bottom of the Web Form Wizard. The wizard is also extremely slow to start at this resolution. Oracle recommends that you set the resolution on your workstation to a higher resolution.

To configure a Web Application Using the RSA SecurID Wizard

1. In the dialog that appears, select the type of application form you want to configure. The available options are:

■ **SecurID Logon.** Configures a SecurID logon form.

■ **SecurID Logon success.** Configures a form that detects a match during silent credential capture. In the presence of this form, the Agent delays credential capture until it verifies the user's entries and displays the Logon Success dialog. If this form is not present, the Agent captures credentials immediately after the user enters them and clicks **OK**.

■ **SecurID Logon failure.** Configures a form that detects a non-match during silent credential capture. In the presence of this form, the Agent delays credential capture until it verifies the user's incorrect entries and displays the **Logon Failure** dialog. If this form is not present, the Agent immediately informs the user that the credentials are incorrect, displaying either the **New**

Logon dialog or the **Retry Logon** dialog to allow the user to re-enter credentials.

- **PIN change.** Configures a PIN change form.

- **PIN confirmation.** Configures a form that verifies that the user's second password entry in a password change form is identical to the first password entry.

- **PIN change success.** Configures a form that serves as a match for the target application's PIN change success message. Since this form does not inject credentials, the **Credentials** page of the Web Form Wizard is skipped. When the PIN change success message is detected, Logon Manager will automatically save the new credentials.

- **PIN change failure.** Configures a form that serves as a match for the target application's PIN change failure message and reinjects credentials when the PIN change failure message is detected. If you select this option, you will be presented with the **Credentials** page of the Web Form Wizard in which you will configure the necessary fields.

    Refer to *Configuring and Diagnosing Logon Manager Application Templates* for a full discussion on using the forms above.

    > **Note:** If you are editing an existing form, this dialog will not appear.

2. In the Web Form Wizard, enter the Web Address (URL) of the Web site and click **Go**. The top pane of the Wizard acts as a Web browser window. You can resize the Wizard's window as needed.

3. In the top pane, navigate to the Web site's logon form. When the Wizard detects one or more forms in a Web page, it lists the forms and their elements (fields and buttons) in the bottom pane.

4. Click the **Detect Fields** button. The Wizard attempts to detect and configure the credential fields and marks them accordingly:

   - SecurID Username

   - Passcode

   - Tokencode

   - Old PIN (PIN change and PIN change failure forms only)

   - New PIN (PIN change and PIN change failure forms only)

   - Submit button

5. (Optional) Select **Use ordinals instead of names**. The **Credential Fields Screen** displays the fields, assigning Control IDs by location order instead of using native (dynamic) Control IDs.

6. (Optional) **Select Show non-input fields**. The Administrative Console detects fields that have input functionality but into which you cannot enter information, such as IMG tags that function as Submit buttons, and includes these fields in the Web Form Wizard fields list.

7. (Optional) **Select Allow multiple field designation**. The Administrative Console recognizes multiple fields that require the same credential, such as enter and confirm password fields, or a page with the same field on two forms.

8. Confirm that the Wizard has selected the correct fields. You can modify a selection, if necessary:

   a. If you are editing an existing template, you may change the form type using the Form Type drop-down at the lower right. Keep in mind that if you do so, you will need to reconfigure the template (reassign fields, and so on). Only fields relevant to a given form type are displayed when that form type is selected.

   b. Identify and select a field from the list in the bottom pane. (The Element and Type descriptions provide cues.) In the top pane, a blinking outline indicates the corresponding field or button you have selected.

   c. Confirm that you have selected the correct field, then right-click the selected item and choose from the shortcut menu (for example, SecurID Username). An icon appears to the left of the item. To deselect an item, right-click the item and select **None** from the shortcut menu.

9. Repeat this process for each field required to complete the logon form. You can configure up to four fields in all.

10. Repeat the two previous steps for each field required to logon. You can configure up to four fields in all.

11. When you have completed your configuration click **OK** to save it and close the Web Form Wizard.

2.13.5.6 Identification Tab for Configuring a Web Application

Use the **Identification (Web)** tab to modify program and window information for a Web application logon configuration.

- You can configure a logon manually by adding, editing, or deleting entries in the Form name and URL fields.

  or

- You can use the Web Form Wizard to define URLs, forms, and fields by pointing and clicking.

To display this tab, do one of the following:

1. Create a new Web application logon.

or

1. In the left pane, click **Applications** and select a Web application.

2. Click the **General** tab in the right pane.

3. Select a form from the list and click **Edit**.

   The Web form-configuration window appears, displaying the **General** tab.

Control	Function
Form name	Enter an application name.
URL	One or more URLs of the logon or password-change form to configure. Click **Add** (or select a matching item and click **Edit**) to display the **URL** dialog. Click **Delete** to remove a URL.

2.13.5.7 Fields Tab for Configuring a Web Application

Use the **Fields (Web)** tab to define how the Agent interacts with the fields of the logon form. Select one of the following transfer methods for the currently-selected application form:

- Up to four logon fields (user ID, password, etc.), using Control IDs

- A series of keystrokes (with optional timings) that fill in and submit the logon form, using SendKeys or SendKeys using Journal Hook.

  If you want to switch from one transfer method to the other after creating a Web form, select the desired transfer method on this screen. The Administrative Console converts the fields for the transfer method you selected.

> **Note:** When you switch from Control IDs to SendKeys, all fields convert with a direct injection setting. You can change the injection method during the editing process. When you switch from SendKeys to Control IDs, any field that is not set to inject directly does not convert.

To display this tab, do one of the following:

1. Create a new Web application logon.

or

1. In the left pane, click **Applications** and select a Windows application.

2. Select the **General** tab in the right pane.

3. Select a logon form from the list and click **Edit**.

4. Select the **Fields** tab.

Control	Function
Transfer method (choose one)	Options: - **Control IDs.** Use standard Windows Control IDs to identify and transmit credentials to a field. Click **Add** to add a field and enter its Control ID or **Edit** to modify existing field settings. - **SendKeys.** Configure fields by transmitting a keystroke series to the form. Click **Edit** to enter or change the series. - **SendKeys using Journal Hook.** Configure fields by transmitting a keystroke series to the form using Journal Hook. Click **Edit** to enter or change the series.
Fields	One or more credential fields (including the Submit button) with transfer methods and their identifying information. You can: - Select a field and click **Edit** to modify Control ID or SendKeys settings. - Click **Add** to add a field (for Control ID only). - Click **Delete** to remove a field (for Control ID only). - Use the **Up** and **Down** arrows to reorder the fields.

2.13.5.8 Dynamic and Ordinal Control IDs

Certain applications change the Control ID for each field with every application launch. Logon Manager provides you with the option to assign ordinal ID numbers to

replace these dynamic Control IDs, thereby eliminating variations in Control IDs with each application launch.

> **Note:** Logon Manager assigns mandatory ordinal field IDs by default to .NET applications, which have no native support for Control IDs.

To configure Logon Manager to assign ordinal Control IDs:

1. Launch the Administrative Console.

2. Pause the Logon Manager Agent.

3. Launch an application to create a template.

4. Launch the template wizard.

5. Select **Logon**.

   The Control ID for each field appears in the **Credential Fields** screen. For applications with dynamic Control IDs, these ID numbers will vary with each launch. (This does not apply to .NET applications, which have no native Control IDs.)

6. Select **Use ordinals instead of Control IDs**.

   - The **Credential Fields Screen** displays the fields, assigning Control IDs by location order instead of using native (dynamic) Control IDs.

   - For applications with native Control ID Support, if **Use ordinals instead of Control IDs** is checked, the Control ID detection is done by enumerating controls on the application window. The ID column will be filled with field ordinals and the display refreshes.

   - If you opt not to use ordinal IDs, dynamic Control IDs will display as the default (except for .NET applications, for which the ordinals are already displayed).

   - If you select **Use 'Send Keys' for this form. Do not use Control ID**, the **Use ordinals instead of Control IDs** option is unavailable.

7. Select a numeric field value to determine which field is assigned to the ID. The field will be surrounded by a flashing border. Right-click the dropdown menu to select the field name (for instance, **Username** or **Password**).

2.13.5.9 Choose Control ID

Use the ConfigName wizard to select a logon window's text control to use as the initial name of the application logon. Use this feature to name a logon (when it is added to the Agent) with a variable text item (such as an account name) that appears in the logon window.

1. Select the window that contains the text control you want to use, then click **Next**.

2. Select the control that contains the text item to use as the logon's initial configuration name. Click **Finish**.

Control	Function
Window List	Displays the windows of the current applications. Click on the column heads to sort the list.

Control	Function
Show hidden window	Specifies to include hidden windows in the Window list.
Next	Advances to the next Wizard page.

Control	Function
Control List	Displays the controls of the currently-selected application window. Click on the headers (Class, ID, or Text) to sort the list.
Use ordinals instead of Control IDs	Indicates that the Agent should transmit data to this form as a series of numbered Control IDs assigned by Logon Manager, rather than addressing individual fields generated by native Control IDs.
Refresh	Updates the field list.
Back	Returns to the previous Wizard page.

2.13.5.10 SendKeys Settings for a Web Application

Use the controls on this screen to define SendKeys actions. If you convert the transfer method from Control IDs to SendKeys or SendKeys using Journal Hook, the Administrative Console automatically converts the ControlID settings to SendKeys actions, and specifies the Direct injection option. If you convert from either SendKeys transfer method to Control IDs, you must configure the settings to use direct injection or they will be lost.

To use the SendKeys editor:

1. On the **Fields** tab, select **SendKeys** as the transfer method. The Fields window changes to reflect conversion of the existing fields, whose names now include -> *direct injection*.

2. Click the **Edit** button to open the **SendKeys editor**. The **Current Actions** list contains the items that the editor has detected.

    The **New Actions** dialog contains a list of additional controls to add to the form. Depending on what you select in this list, the options vary.

    For example, if you select **Fields** from the **New Actions** list, the **Field Type** dialog appears, offering choices of a third and fourth field. If you select **Delay**, a menu in which you can specify a delay interval appears.

3. Select an item in the **Current Actions** list and click the **Edit** button below the list to change the settings for that field or action. Click the **Up** or **Down** arrows to reorder the list.

4. Use the **New Actions** section of the SendKeys editor to add fields and actions to the list. Refer to the following tables for information on configuring the various action choices.

    After you configure a New Action and insert it, it appears as part of the **Current Actions** list.

Current Actions	Function
Keys/Actions	Lists the keys and actions that the editor detected. If you converted this list from Control IDs to SendKeys, every action is configured for direct injection by default.
	Use the **Up** and **Down** arrows to reorder the items in this list.

New Action	Controls	Description
Fields	Field Type	Select a credential item from the list to add to the series. ■ Username/ID ■ Password ■ Third Field ■ Fourth Field
	Character to insert after field	Select a keystroke to insert automatically after the field is filled: ■ None (no keystroke) ■ Enter (to submit the form) ■ Tab (to advance the cursor) Also see Special Keys, below.
	Inject directly into control	Injects the credential directly into the control. Click the ellipsis ("…") button to open the Web Field dialog.
Web Field	Function	This box is pre-filled with the name of the field that you are editing and cannot be changed. 1. Click **Wizard** to launch the Web Form Wizard, which is pre-filled with the URL that you specified previously. 2. Select a field from the Web page in the wizard and click **OK** to close the wizard. You return to the Web Field dialog, which is populated with the parameters of the field that you selected. 3. Click **OK** to exit the **Web Field** dialog. The **Current Actions** list now includes the field or action that you just configured.
	Frame	Identifies the frame number in the Web page that contains the function you are configuring.
	Form	Identifies the type of form you are creating based on the function.
	Field identification	Identifies the field as specified in the Web page.
	Field type	Identifies the type of field: ■ Text ■ Password ■ Select-One ■ Select-Multiple
	Insert	Add the current selection to the series.

New Action	Controls	Description
Click	Click on a control	Click the ellipsis ("**…**") button to open the Web Element dialog, and click **Wizard** to launch the Web Form Wizard. This time, the wizard identifies only clickable fields.
		Select the field that you want to associate with a click, and select **OK**. The wizard closes and returns you to the **Web Element** dialog. Its fields are populated with the information that the wizard identified.
	Frame	Identifies the frame number in the Web page that contains the function you are configuring.
	Form	Identifies the type of form you are creating based on the function.
	Field identification	Identifies the field as specified in the Web page.
	Field type	Identifies the type of field: ■ Submit ■ Image ■ Button ■ Anchor ■ IMG ■ Image The Agent detects where the control is and simulates a click in the center of the control.
	Insert	Add the click selection to the series.

New Action	Controls	Description
Run Task	Command line to run	Enter a Command line to be executed. This feature allows you to run a program in the middle of entering keystrokes. ■ Window Handles can be appended to the command line to inform the script of the window handle currently being worked on: `$(HWND)` ■ Environment Variables can also be appended to the command line: `$(USERDOMAIN)\$(USERNAME)` Click the ellipsis ("**…**") button to open the **Choose File** dialog. **Note:** VirtualKeyCodes cannot be used within the command line (the initial backquote character will terminate the command line).
	Expected return code	Enter the expected return code. The rest of the SendKeys script is discarded if this value is not returned.

New Action	Controls	Description
	Time out (sec.)	Enter the number of milliseconds to wait for the task to complete. The rest of the SendKeys script is discarded if this timeout is reached. The maximum timeout period is five (5) seconds.
	Insert	Add the task to the series.

New Action	Controls	Description
Delay	Length of delay (in seconds)	Type or select a delay between keystrokes.
	Insert	Add the delay to the series.

New Action	Controls	Description
Set Focus	Set focus to control	Sets the focus to control. Click the ellipsis ("**…**") button to open the Web Element dialog and launch the Web Form Wizard. Select which of the available fields will receive focus. Click **OK**.
	Insert	Add the focus to the series.

New Action	Controls	Description
Text	Enter text to insert	Enter any literal text to add to the series.
	Insert	Add the text to the series.

New Action	Controls	Description
Special Keys	Category	Choose a keystroke category (for example, Movement keys) from the left list, then a specific key (for example, Backspace) from the right list.

New Action	Controls	Description
	Key List	Select the functionality of the key.
		■ **Key Press.** Insert the key as a single keystroke (default).
		■ **Key Down/Up.** Insert the key as a pair of actions: key-press and key-release. This option lets you insert other keystrokes between these actions to indicate one or more keys held down as another is typed, as for a "hot key" combination that moves the focus to a specific text box.
		For example, to insert the keystroke **Alt+P**, select the **Key Down/Up** option, then select **Modifier** for the Category and **Alt** for the Key, and click **Insert**. This inserts two actions: **[Down:Alt]** and **[Up:Alt]**.
		Select the **Text** tab and enter **P** in the text box. In the left pane, select **[Up:Alt]** and click **Insert**. The **P** is inserted between the two Alt-key actions, producing **Alt-P**.
		■ **Key Down.** Insert the key as a downward press only.
		■ **Key Up.** Insert the key as a release only.
	Insert	Add the keystroke to the series.

2.13.5.11 Matching Tab for Configuring a Web Application

Use the Web Matching tab to distinguish among logon, password-change, or password-confirmation forms (referred to here as target forms) within the same Web application, typically a multi-form portal page. The Agent uses the matching criteria you supply here to distinguish among similar forms.

This tab is typically used to refine the detection match criteria, that is, the set of HTML tags and values you use to identify a specific page. You can then create an offset match that uses a subset of the detection match to identify the desired logon or password-change form on the page.

To display this tab:

1. Create a new Web application logon.

or

1. In the left pane, select **Applications** and select a Web application.

2. Click the **General** tab in the right pane.

3. Select a form from the list and click **Edit**.

4. Select the **Matching** tab.

2.13.5.12 Creating or Modifying Detection-Matching Criteria

To create or modify detection-matching criteria:

1. In the **Detection Match** list, do one of the following:

■ Click **Add** to create a new matching criterion.

■ Select a match and click **Edit** to modify an existing match.

2. From the **Edit Match** dialog, enter or select the required information, then click **OK** to return to this dialog.

3. If necessary, adjust the match criteria order.

   a. Select a match to move.

   b. Click the **Up** or **Down** arrow.

4. Click **OK**.

2.13.5.13 Offset Matching

> **Note:** Offset matching should only be used with portal Web pages.

This type of matching is used with portal pages that have multiple windows that the user can rearrange, add, and remove. If the site you are matching on is not a portal, leave the offset matching section on this panel blank.

With regular match detection, the forms must always appear in the same order. With offset matching, you can rearrange the forms (which look like a window) and isolate a specific window from all the others. This only applies to portal pages because these pages are dynamic, and ordinal values are used to match instead of field names.

Use the **Offset Start** field to tell Logon Manager which match result's forms to use for the form offsets. The offset start value should be the number of the offset matches. For example, if there are three offset matches, the offset start value should be 3.

To create or modify Offset Matching criteria:

1. In the **Offset Match** list, do one of the following as needed:

   ■ Click **Copy from Detection** to copy defined Detection Match criteria.

   ■ Click **Add** to create a new matching criterion.

   ■ Select a match and click **Edit** to modify an existing match.

2. In the **Edit Match** dialog, enter or select the required information, then click **OK** to return to this dialog.

3. If necessary, adjust the match criteria order.

   a. Select a match to move.

   b. Click the **Up** or **Down** arrow.

   c. Select an **Offset Start**.

4. Click **OK**.

2.13.5.14 Edit Match Criteria for a Web Application

Use this dialog to create or modify matching criteria for the selected Web form.

Control	Function
Tag	Enter an HTML tag type; for example, <TD> for a table cell.
Match Tag Instance	Select to match a specific instance of the Tag and select the instance number; for example, 3 for the third table cell on the page.

Control	Function
Criteria	Select one criteria type: ■ **Text.** The plain-text (InnerText) content of the tag element (for example, Enter your password) ■ **HTML.** The rich-text (innerHTML) content of the tag element (for example, Enter your password). **Note:** Certain browsers' innerHTML properties tags can differ from the normal HTML. For instance, the tags might appear in a different letter case, or they might add or remove spacing between the tag and the enclosed text. In order to avoid matching problems, use alternate tags and wildcard characters to account for these differences. **Example:** Although you would expect the tag for a bold "OK" button to be: OK, the innerHTML tag might be: <B> OK </B>. To ensure that this match works, specify this regular expression as: <(b|B)>.*OK.*</(b|B)>. ■ **Attribute.** In the box, enter an HTML attribute of the tag element (for example, id=password).
Value	Enter the actual text to match. ■ **Match whole value.** Select to enforce strict matching of Value (that is, any additional text in the tag element will cause the match to fail). ■ **User regular expression.** Select to allow more flexible matching based on regular expressions.
Operation	Select the relationship of this match to any others: ■ **And.** This match is one of multiple matches required to identify the form. ■ **Or.** This match alone identifies the form. ■ **Not.** This match excludes the form. **Note:** The AND, OR, and NOT operators specify the conditions under which the Agent should respond to Web match combinations. If you assign a match value of AND to a match criterion, that criterion must be present for the Agent to respond to a page. So, when several fields are assigned an AND operator, all those criteria must be present. If you assign a match value of OR to several match criteria, the Agent responds if any one of the criteria is present. The NOT operator is used as an excluder when performing a match. The Agent responds to any criteria that are assigned the AND and OR operators, unless the conditions of the NOT criteria are present. The Agent excludes the instances specified by the NOT operator.

2.13.5.14.1 Offset Matching Example Following is a sample portal page that contains three windows. The goal is to log on to the Sales Database window. In order to do that, isolate that window from all the others windows on the page.
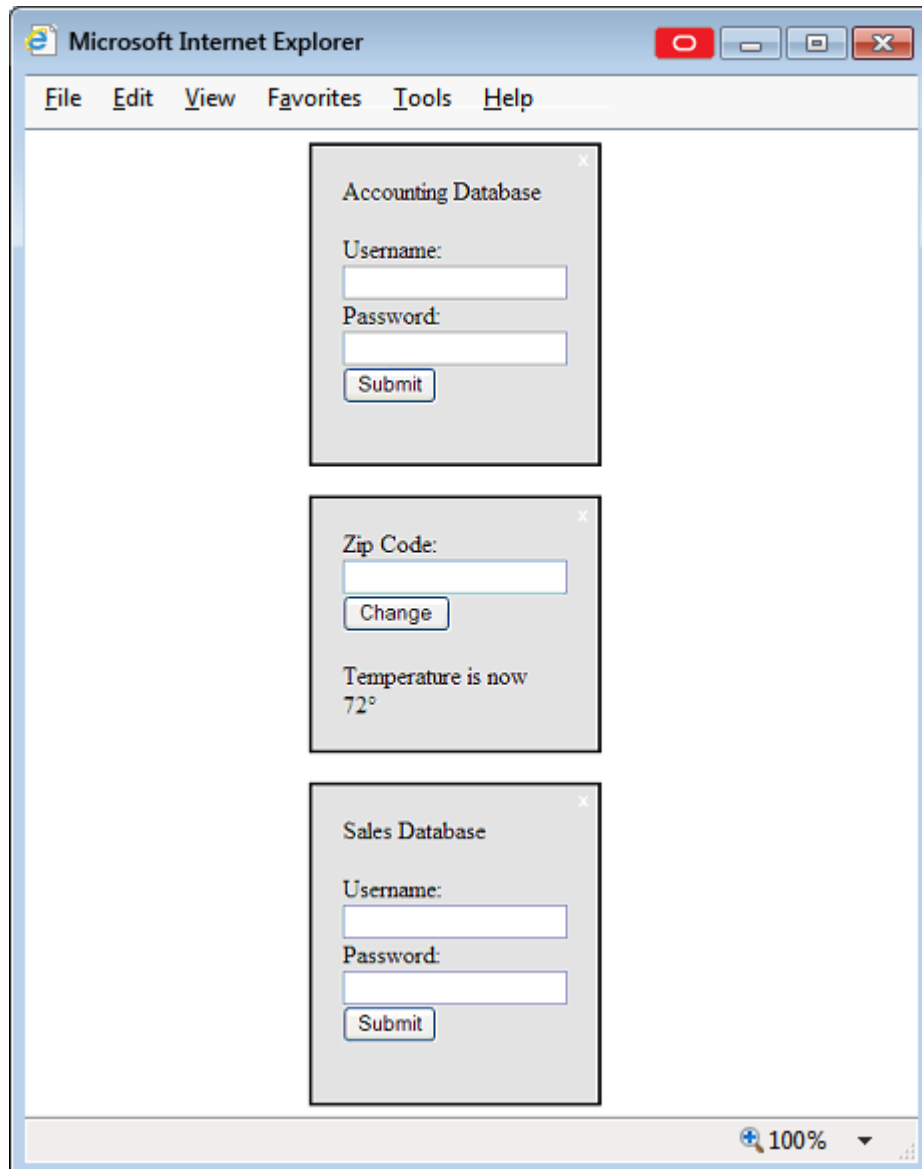
> **Note:** Like most portal sites, the windows can be rearranged and windows can be added or removed by the user so the order and the existence of windows can change. This can be done using both Detection Matching and Offset Matching (collectively referred to as Web Matching). This example describes Offset Matching.

Below is an HTML fragment that is shown when you click View > Source from the browser's toolbar (the HTML has been greatly simplified to illustrate the important elements):

```
<div name="portalLogon1">

p

Accounting Database

</p>
```

```
<form>

Username: <input type="text" name="username">

Password: <input type="password" name="password">

<input type="submit" >

</form>

</div>

<div name="weatherStation">

<form>

Zip Code: <input type="text" name="zipCode">

<input type="submit" >

</form>

<p>Temperature is now 72°</p>

</div>

<div name="portalLogon2">

<p>

Sales Database

</p>

<form>

Username: <input type="text" name="username">

Password: <input type="password" name="password">

<input type="submit" >

</form>

</div>
```

Each window is represented by a `<div>` tag and each `<div>` tag has a name attribute, which you use to filter out windows that are not pertinent to your task.

To do this, add an Offset Match to look for all `<div>` tags with the name attribute that contains the word `portalLogon`. Click **Add** to match this criterion.
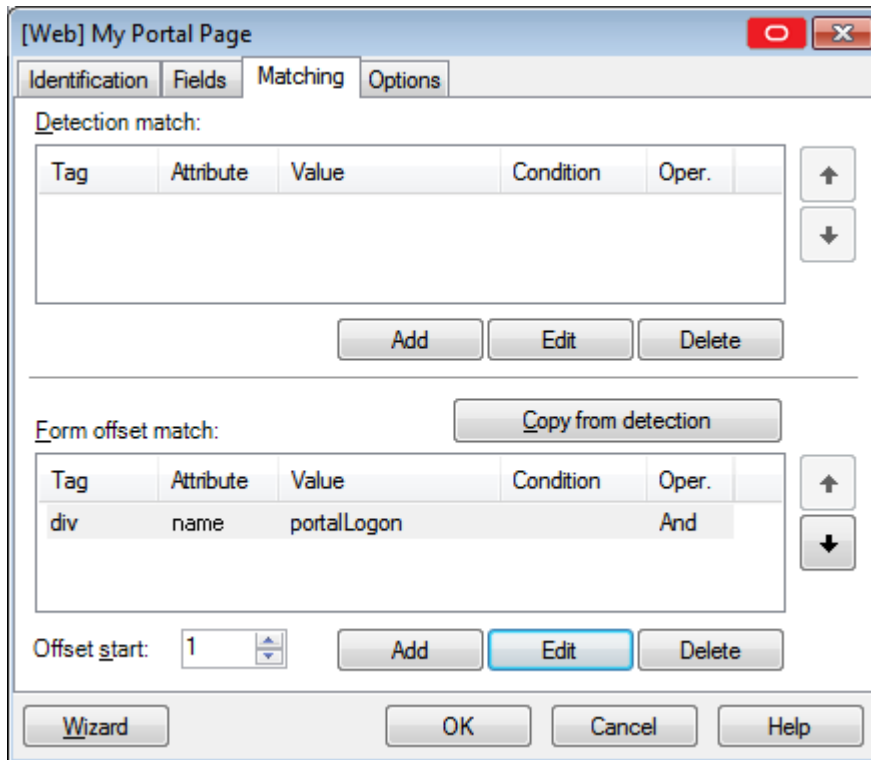
For this example, all the windows are now filtered out except the two portalLogon windows. The Agent now focuses only on the following windows:

```
<div name="portalLogon1">

…

</div>

<div name="portalLogon2">

…

</div>
```

To isolate the Sales Database window, you must add another offset match form. The HTML source indicates that the window to isolate contains a `<p>` tag that contains the text Sales Database. Click **Add** to match this criterion.
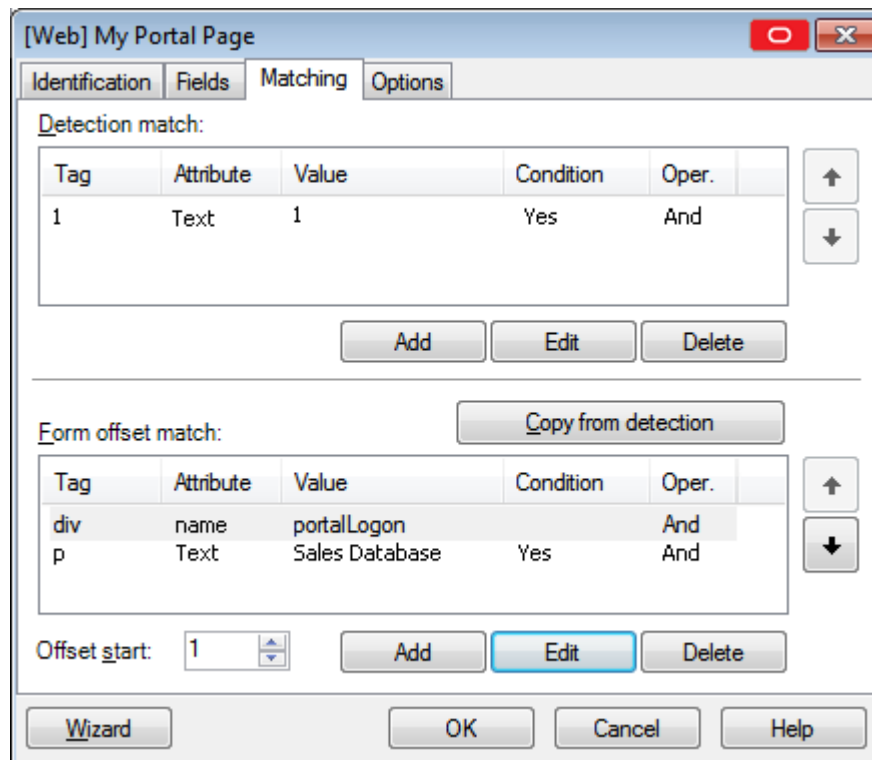
The Agent now sees only one window:

```
<div name="portalLogon2">
```

…

```
</div>
```

Because the targeted window is isolated, this is all the matching that you need to add.

The remaining task is to set the Offset Start values. To set this, determine at which match the form you want is visible. In this example, there are two matches.

The first matches the `<div>` tag, and the second match matches the `<p>` tag. In this match, the `<form>` tag is visible since it is contained in the `<div>` tag:

```
<div name="portalLogon2">
```

…

```
<form>
```

…

```
</form>
```

```
</div>
```

In the second match, the `<form>` tag cannot be seen since it is not contained in the `<p>` tag.

```
<p>
```

```
Sales Database
```

```
</p>
```

The Offset Match cannot be set to 2. It must be set to 1. This tells the Agent that the form offset for the fields is relative to the first match (the `<div>` match), as follows:

```
<div name="portalLogon2">

<p>

Sales Database

</p>

<form>

Username: <input type="text" name="username">

Password: <input type="password" name="password">

<input type="submit" >

</form>

</div>
```

All the form offsets and field offsets in the **Fields** list (found in the **General** tab) are relative to the above HTML.

2.13.5.15 Add/Edit URL

Use this prompt to specify the URL of the logon or password-change form to configure.

To specify a URL for matching

1. Select one of the following (see Matching Expressions).

   - Exact

   - Wildcard (does not apply to Kiosk Manager)

   - Regular Expression (does not apply to Kiosk Manager)

2. Enter (or edit) the URL or a matching expression.

3. Click **OK**.

2.13.5.16 Matching Expressions

For applications that have varying text in their URLs, you can use substrings or regular expressions to specify how to match the variable text.

Option	Function
Wildcards	- **?** (question mark) matches any single character.
	- ***** (asterisk) matches zero or more occurrences of any character.
	Note: This does not apply to Kiosk Manager.
Regular Expressions	You can also use the set of regular expressions to specify a string pattern that the Agent should recognize as a match.
	Note: This does not apply to Kiosk Manager.

2.13.5.17 Matching Environment Variables

For applications that include the user's name in the URL (as derived from the DOMAINUSER environment variable in the workstation operating system), select **Exact** as the matching criterion, and use one of the following substitution tokens in the match string:

Variable	Function
%DOMAINUSER%	User name exactly as derived from the environment variable
%UC%%DOMAINUSER%	User name converted to all upper case
%LC%%DOMAINUSER%	User name converted to all lower case

Example

This URL entry matches a password-change window title that includes the username:

```
Password Expired - %UC%%DOMAINUSER%
```

2.13.5.18 Adding and Editing Web Fields

Use this dialog to specify a credential field or Submit button on a Web form.

Option	Function	
Function	Select a credential type: ■ UserID ■ Password ■ Third Field ■ Fourth Field ■ New Password ■ Confirm New Password ■ Submit	
Frame	Type the target name of the browser frame in which the field appears (specified by the NAME attribute in a <frame> element in the target page's parent frameset).	
Form	Type the name of the form in which the field appears (specified by the NAME attribute in the <form> element in the target page).	
Field identification	Select the ellipsis ("**…**") button to launch the **Field Identification** dialog, where you can select which type of field you want to match.	
Field type	Select the field type (corresponding to the type attribute of the field's <input> element) or a hyperlink anchor or IMG tag (<A HREF=...>) used as a Submit button.	
	Credential Type	<INPUT TYPE=...> Options
	UserID	Text
	Password	Password
	Third Field	Select one
	Fourth Field	Select multiple
	New Password	
	Confirm New Password	
	Submit	Submit
		Image
		Button
		Anchor (<A HREF...> tag)
		IMG (<A HREF...> tag)

2.13.5.19 Field Identification Dialog

Use this screen to specify the type of field you want the Agent to recognize. Check the appropriate radio button from among the following:

- **Use field name.** Select for a Web site whose fields have consistent, named labels, such as "User" or "e-mail."

- **User ordinal number.** Select if you want to replace varying field numbers with ordinals for dynamic Web pages. See Dynamic and Ordinal Control IDs for more information.

- **Use matching.** Select for a Web site where the field index varies depending on the user. Choose from among the matching choices as explained in the following table.

Field	Function	
Tag	Enter an HTML tag type; for example, `<TD>` for a table cell.	
	Match Tag Instance	Select to match a specific instance of the Tag and select the instance number; for example, 3 for the third table cell on the page.
Criteria	Select one criteria type:	
	▪ **Text.** The plain-text (InnerText) content of the tag element (for example, Enter your password)	
	▪ **HTML.** The rich-text (InnerHTML) content of the tag element (for example, `<b>Enter your password</b>`).	
	▪ **Attribute.** In the box, enter an HTML attribute of the tag element (for example, `id =password`).	
	Note: Certain browsers' innerHTML properties tags can differ from the normal HTML. For instance, the tags might appear in a different letter case, or they might add or remove spacing between the tag and the enclosed text. In order to avoid matching problems, use alternate tags and wildcard characters to account for these differences.	
	Example: Although you would expect the tag for a bold "OK" button to be: `<b>OK</b>`, the innerHTML tag might be: `<B> OK </B>`. To ensure that this match works, specify this regular expression as: `<(b|B)>.*OK.*</(b|B)>`.	
Value	Enter the text of the Criteria to match.	
	Match Whole Value	Select to enforce strict matching of the Value you entered in the previous field (that is, any additional text in the tag element will cause the match to fail).
	Use regular expression	Select any legal expression to match the Value you entered in the previous field (you can use wildcards to create a broader matching range).
		Note: Do not use the colon (`:`) as part of your matching expression. Logon Manager uses this character as a delimiter when parsing the contents of the expression.

2.13.5.20 Options Tab for Configuring for a Web Application

Web pages occasionally include forms that require a short time to become enabled as the page loads. In such a case, Logon Manager might submit credentials too soon. To

avoid this occurrence, use the **Submit Delay** setting on the **Options** tab to allow time for all forms to become enabled.

Setting	Function
Dynamic Page	Check to indicate that the Web page for the template includes dynamic content.
Adheres to Logon Loop Grace Period	Select to have the Agent ignore this application's logon form when the logon loop grace period (set on the application's **Miscellaneous** tab) is in effect.
Auto-Recognize	Select to have the Agent recognize the application automatically. Specifying a status for this setting on the **Options** tab overrides the Global Agent Setting. If this setting is checked, the user can configure this setting from the Logon Manager. If this setting is unchecked, the user will not have access to this setting from the Logon Manager.
Auto Submit	Select to have the Agent automatically select **OK** for this application logon after providing credentials.
Preset Focus	Select to set the focus on a logon field before the Agent places data in the field.
Submit via Keyboard	Select to instruct the Agent to enter a programmatic **Submit** command for Web pages that have no **Submit** button.
Submit Delay (milliseconds)	Enter a time in milliseconds for the Agent to wait to submit credentials.

To display this tab:

- In the **General** tab in the right pane for a Web application, double-click or right-click on the **Web application**, and select the **Options** tab.

2.13.5.21 Proxy Tab for Configuring a Web Application

Use the **Proxy** tab to:

- Provide mock values for the single sign-on fields when the fields are first rendered to the Web page.

- Configure form masking to prevent the user from seeing or altering the injected credentials.

Setting	Function
Mock Fields	Contains the field values for the proxy connection.
Clear All	Deletes the entries in the **Mock Value** column.
Edit	Select a field from the list, and click to launch the **Update Mock Field** dialog.
Mask form	Enable/disable masking for the form
RED/GRN/BLUE	Set the numerical value for the red, green, and blue components of the desired mask color.
HEX	Enter the hexadecimal value for the desired mask color.
Select color	Opens the color picker, allowing you to pick the desired mask color visually.
Image	Relative path and filename of the desired mask image to be used instead of a solid color mask.
"Timeout	Number of seconds before the form mask is dismissed.

Setting	Function
Close button	Enable/disable the **Close** button on the form mask (allows user to remove the mask).
Opacity	Percentage opacity of the form mask.
Default	Reset all form mask options to default values.
Wizard	Click to launch the **Web Form Wizard**.
OK	Click to confirm your settings.
Cancel	Click to dismiss the dialog without saving changes.

2.13.5.21.1 Update Mock Field Dialog Use this dialog to edit the fields in the **Web Proxy** list.

The uneditable **You are updating** field displays the field you selected in the previous dialog. Enter the desired information in the **Mock value** field and click **Update** to save your changes. Click **Close** to dismiss the dialog without saving changes.

2.13.6 Creating a New Host/Mainframe Application

Use this dialog to configure a new logon for a host/mainframe application.

1. Start the target application.

2. In the left pane, right-click **Applications** then select **New Host App** from the shortcut menu.

3. The **Add Application** dialog appears with the Host/Mainframe option selected.

4. In the **Add Application** dialog, enter a **Name** for the new logon and click **OK**. The Host/Mainframe Form Wizard (for configuring new logon forms) appears.

See Adding Host/Mainframe Applications for more information.

2.13.6.1 Host/Mainframe Form Wizard

Use the Host/Mainframe Form Wizard to perform any of these tasks:

- Configure new logons for a host/mainframe emulator or Telnet (scrolling-screen) applications.

- Add new forms to existing logons.

- Create forms for automatic password changes.

- Create forms for detecting password change success and failure.

The Host/Mainframe Form Wizard lets you use the application itself to identify its logon/password-change windows and the individual username/ID, password, and other fields. The general steps for creating a logon are as follows:

1. Start the target emulator or Telnet application.

2. Select the **Form Type** and **Screen Type**.

3. Copy the text of the application's logon/password-change screen and paste it to the Administrative Console.

4. Indicate the text and position of onscreen captions that identifies the screen as a logon/password-change form.

5. Indicate the position (or, for Telnet applications, the sequence) of the individual username/ID, password, and other fields.

6. Review the configuration and make changes as needed, using the **Back** and **Next** buttons.

7. To modify a host/mainframe logon's settings manually, use the Identification Tab for Configuring a Host or Mainframe Application.

8. Before you begin this procedure, refer to the General Guidelines for Setting Up Applications for configuring applications. Also see Adding Host/Mainframe Applications for specific information about creating and configuring host/mainframe logons.

2.13.6.2 Configuring a Host/Mainframe Application

Start the target application in the host/mainframe emulator or Telnet.

1. In the Administrative Console, do one of the following:

    ■ Create a new host/mainframe application logon.

    ■ Select an existing host mainframe application, then in the **General** tab, click **Add**.

2. In the Host/Mainframe Wizard, select the form type. The available options are:

    ■ **Logon.** Configures a logon form.

    ■ **Logon success.** Configures a form that detects a match during silent credential capture. In the presence of this form, the Agent delays credential capture until it verifies the user's entries and displays the **Logon Success** dialog. If this form is not present, the Agent captures credentials immediately after the user enters them and clicks **OK**.

    ■ **Logon failure.** Configures a form that detects a non-match during silent credential capture. In the presence of this form, the Agent delays credential capture until it verifies the user's incorrect entries and displays the **Logon Failure** dialog. If this form is not present, the Agent immediately informs the user that the credentials are incorrect, displaying either the **New Logon** dialog or the **Retry Logon** dialog to allow the user to re-enter credentials.

    ■ **Password change.** Configures a password change form.

    ■ **Password confirmation.** Configures a form that verifies that the user's second password entry in a password change form is identical to the first password entry.

    ■ **Password change success.** Configures a form that serves as a match for the target application's password change success message. Since this form does not inject credentials, the **Credentials** page of the Host/Mainframe Wizard is skipped. When the password change success message is detected, Logon Manager will automatically save the new credentials.

    ■ **Password change failure.** Configures a form that serves as a match for the target application's password change failure message and reinjects credentials when the password change failure message is detected. If you select this option, you will be presented with the **Credentials** page of the Host/Mainframe in which you will configure the necessary fields.

    Refer to *Configuring and Diagnosing Logon Manager Application Templates* for a full discussion on using the forms above.

3. In the Screen Type wizard page, do one of the following:

    ■ Choose **Fixed Screen** for applications running on a host/mainframe emulator that presents logon forms as static text pages.

- ■ Choose **Scrolling Screen** for applications running on Telnet or other scrolling-screen consoles that request logon information as a series of prompts.

4. In the **Paste Screen Text** page that opens, in the target application, copy all of the onscreen text to the Windows Clipboard.

> **Note:** Some emulators provide a Copy command or button; others let you select **Ctrl+C** to copy. In Windows Telnet, select the text and press **Enter**.

5. In the Administrative Console's **Paste Screen Text** page, click **Paste Text** to paste the text into the wizard page, and click **Next**.

> **Note:** If the emulator screen does not use return or line-feed characters, adjust the **Characters per Line** to set proper text wrapping.

6. In the **Cursor Position** page, click or use the arrow keys to place the text cursor in the exact position that it appears in the Telnet application's window.

7. Click **Next** to display the next wizard page.

8. In the **Text to Match** wizard page, select a block of text that identifies the screen as a logon or password-change form. Right-click the selection, and click **Add as Text Match**. Repeat this step for additional text blocks.

9. When your selections are complete, click **Next** to display the next wizard page.

10. In the **Fields** wizard page, do one of the following:

    - ■ For a fixed-screen logon, place the text cursor at the starting position of a field. Right-click and select the field type (**Username/ID**, **Password**, **Third Field**, **Fourth Field**) from the shortcut menu. Repeat this step for each required field.

    - ■ For a scrolling screen, place the text cursor at the prompt-entry position. Click **Add**, then select the first field type requested. Repeat this step for each required prompt.

11. When your selections are complete, click **Next** to display the summary page.

12. Review the configuration. To make changes, use the **Back** and **Next** buttons to display a page.

13. When your configuration is complete, click **Finish**.

2.13.6.3 Host/Mainframe Form Wizard for RSA SecurID

Use the Host/Mainframe Form Wizard to perform any of these tasks:

- ■ Configure new logons for a host/mainframe emulator or Telnet (scrolling-screen) applications

- ■ Add new forms to existing logons

- ■ Create forms for automatic PIN changes

- ■ Create forms for detecting PIN change success and failure

The Host/Mainframe Form Wizard lets you use the application itself to identify its windows and fields. The general steps for creating a logon are as follows:

1. Start the target emulator or Telnet application.

2. Select the **Form Type** and **Screen Type**.

3. Copy the text from the form displayed by the application and paste it to the Administrative Console.

4. Indicate the text and position of onscreen captions that identifies the screen as a form of the selected type.

5. Indicate the position (or, for Telnet applications, the sequence) of the individual username/ID, PIN, and other fields.

6. Review the configuration and make changes as needed, using the Back and Next buttons.

To modify a host/mainframe logon's settings manually, use the Identification Tab for Configuring a Host or Mainframe Application.

Before you begin this procedure, refer to the General Guidelines for Setting Up Applications for configuring applications. Also see Adding Host/Mainframe Applications for specific information about creating and configuring host/mainframe logons.

2.13.6.4 Configuring a Host/Mainframe Application for RSA SecurID

Start the target application in the host/mainframe emulator or Telnet.

1. In the Administrative Console, do one of the following:

   - Create a new host/mainframe application logon. Be sure to select the **RSA SecurID** check box in the **Add Application** dialog.

   - Select an existing host mainframe application, then in the **General** tab, click **Add**.

2. In the Host/Mainframe Wizard, select the form type. The available options are:

   - **SecurID Logon.** Configures a logon form.

   - **SecurID Logon success.** Configures a form that detects a match during silent credential capture. In the presence of this form, the Agent delays credential capture until it verifies the user's entries and displays the **Logon Success** dialog. If this form is not present, the Agent captures credentials immediately after the user enters them and clicks **OK**.

   - **SecurID Logon failure.** Configures a form that detects a non-match during silent credential capture. In the presence of this form, the Agent delays credential capture until it verifies the user's incorrect entries and displays the **Logon Failure** dialog. If this form is not present, the Agent immediately informs the user that the credentials are incorrect, displaying either the **New Logon** dialog or the **Retry Logon** dialog to allow the user to re-enter credentials.

   - **PIN change.** Configures a PIN change form.

   - **PIN confirmation.** Configures a form that verifies that the user's second password entry in a password change form is identical to the first password entry.

   - **PIN change success.** Configures a form that serves as a match for the target application's PIN change success message. Since this form does not inject credentials, the **Credentials** page of the Host/Mainframe Wizard is skipped. When the PIN change success message is detected, Logon Manager will automatically save the new credentials.

- **PIN change failure.** Configures a form that serves as a match for the target application's PIN change failure message and reinjects credentials when the PIN change failure message is detected. If you select this option, you will be presented with the Credentials page of the Host/Mainframe Wizard in which you will configure the necessary fields.

  Refer to *Configuring and Diagnosing Logon Manager Application Templates* for a full discussion on using the forms above.

3. In the Screen Type wizard page, do one of the following:

   - Choose **Fixed Screen** for applications running on a host/mainframe emulator that presents logon forms as static text pages.

   - Choose **Scrolling Screen** for applications running on Telnet or other scrolling-screen consoles that request logon information as a series of prompts.

4. In the **Paste Screen Text** page that opens, in the target application, copy all of the onscreen text to the Windows clipboard.

   Note: Some emulators provide a **Copy** command or button; others let you select **Ctrl+C** to copy. In Windows Telnet, select the text and select Enter.
   ---

5. In the Administrative Console's **Paste Screen Text** page, click **Paste Text** to paste the text into the wizard page, and click **Next**.

   Note: If the emulator screen does not use return or line-feed characters, adjust the **Characters per Line** to set proper text wrapping.
   ---

6. In the **Cursor Position** page, click or use the arrow keys to place the text cursor in the exact position that it appears in the Telnet application's window.

7. Click **Next** to display the next wizard page.

8. In the **Text to Match** wizard page, select a block of text that identifies the screen as a logon or password-change form. Right-click the selection, and click **Add as Text Match**. Repeat this step for additional text blocks.

9. When your selections are complete, click **Next** to display the next wizard page.

10. In the **Fields** wizard page, do one of the following:

    - For a fixed-screen logon, place the text cursor at the starting position of a field. Right-click and select the field type (**Username/ID**, **Password**, **Third Field**, **Fourth Field**) from the shortcut menu. Repeat this step for each required field.

    - For a scrolling screen, place the text cursor at the prompt-entry position. Click **Add**, then select the first field type requested. Repeat this step for each required prompt.

11. When your selections are complete, click **Next** to display the summary page.

12. Review the configuration. To make changes, use the **Back** and **Next** buttons to display a page.

13. When your configuration is complete, click **Finish**.

2.13.6.5 Identification Tab for Configuring a Host or Mainframe Application

Use the **Identification** tab to modify information about a Host/Mainframe application logon form.

Note: See Adding Telnet Applications for information about configuring logons for Telnet applications.

To display this tab, do one of the following:

1. Create a new host/mainframe application logon.

or

1. In the left pane, select **Applications** and select a host/mainframe application.

2. Click the **General** tab in the right pane.

3. Select a logon form from the list and click **Edit**.

The Host/Mainframe form-configuration dialog appears, displaying the **General** tab.

Control	Function
Form Name	The name of the application logon form. You can edit the name.
Window Titles	Because some emulators do not have unique characteristics within their screens to differentiate one from another, you have the option of selecting the window title from a list of open emulator applications. ■ Click **Add** to open the Window Title dialog and enter a window title name manually. or ■ Click **Choose** to open the Select Window screen and select an application from the open emulator list.
Text Matching	Displays the literal text string that the Agent uses to identify this form: the screen coordinates (Row and Column numbers) of the first character of the string. Click **Add** to specify a new text identifier or **Edit** to modify an existing one.
Fields	Displays the series of keystrokes that Logon Manager transfers to the host application's logon form. To add or modify a keystroke series, click **Edit** to display the Edit SendKeys Fields and Actions for a Host/Mainframe Application dialog.
Wizard	Start the Host/Mainframe Form Wizard for configuring an application visually.

2.13.6.6 Text Matching (on a Host/Mainframe Logon Form)

Use the **Text Matching** dialog to specify the text and position of an onscreen caption that identifies the screen as a logon or password-change form.

You must also specify the location (row and column number) of the first character of the text. Use the cursor-position indicator in the status bar at the bottom of the session window to find the row and column numbers of the text.

Note: For Telnet applications, use row coordinates relative to the cursor position. See Adding Telnet Applications for an example. You can also use an asterisk (*) for wildcard matching of a row, column or both.

When you have completed your entries for a match, click **OK**.

Control	Function
Row	Enter the **row number** (vertical screen coordinate) of the first character of the Text.
	For Telnet applications (with supported host emulators), this value is relative to the cursor position and can be negative (to indicate a row above the cursor) or an asterisk (*) to indicate any row onscreen.
Column	Enter the **column number** (horizontal screen coordinate) of the first character of the Text. For Telnet applications (with supported host emulators), this setting can be an asterisk (*****) to indicate any row onscreen.
Text	Enter the string of text to match.

To display this dialog, click the **Add** button under **Text Matching** on the Identification Tab for Configuring a Host or Mainframe Application.

2.13.6.7 Edit SendKeys Fields and Actions for a Host/Mainframe Application

Use the **Edit Fields/Actions** dialog to specify a series of keystrokes for Logon Manager to transfer to the host application's logon form.

The tabs in the right pane of the **Edit Fields/Actions** dialog provide the keystroke options. Select or enter the options you need on each tab. Click the **Insert** button to add the key or action to the series.

Your selections appear in the list in the left pane. To change the order of the series, select an item and click the **Up** or **Down** arrows to move it. To modify an item, select it, and click **Edit** to display the **Fields** dialog. To delete an item, select it, and click **Delete**.

Tab	Command	Action
Fields tab	Select fields to insert	Select a credential item from the list to add to the series:
		■ UserID
		■ Password
		■ Third Field
		■ Fourth Field
		■ New Password
		■ Confirm New Password
		Use the **Up** and **Down** arrows for correct navigation through the form.
	Insert this character after field	Select a keystroke to insert automatically after the field is filled:
		■ None (no keystroke)
		■ Tab (to advance the cursor)
		■ Enter (to submit the form)
		Also see Special Keys, below.

Tab	Command	Action
	Position	Enter the row and column coordinates of the first character of the text-entry field.
		If the column number is variable, (for example, most Unix systems include the affected username as part of the **New Password** and **Confirm Password** field labels when changing passwords), you can use a regular expression to wildcard the variable portion of the field label so that Logon Manager always injects credentials in the correct spot.
	Insert	Add the current selection to the series.
Delay tab	Length of delay (in seconds)	Enter or select a delay between keystrokes.
Text tab	Enter text to insert	Enter any literal text to add to the series.
	Insert	Add the text to the series.
Special Keys tab	Category/Key	Select a keystroke category (for example, Movement keys) from the left list, then a specific key (for example, Page Down) from the right list.
	Insert	Add the keystroke to the series.

To display this dialog:

1. Do one of the following:

   a. Create a new Host/Mainframe application logon.

      or

   a. In the left pane, select **Applications** and select a host application.

   b. Click the **General** tab in the right pane.

   c. Do one of the following:

      Select a logon form from the list and click **Edit**.

      or

      Click **Add** to configure a new form.

      The **Host/Mainframe** form-configuration dialog appears, displaying the **General** tab.

2. Under the **Fields** list box, click **Edit**.

2.13.6.8 Fields Tab for Configuring a Host or Mainframe Application

Use the **Fields** tab to define how the Agent interacts with the fields of a form.

You must also specify the location (row and column number) of the first character of the field. Use the cursor-position indicator in the status bar at the bottom of the session window to find the starting row and column numbers of the text. When you have completed your entries, click **OK**.

See Adding Host/Mainframe Applications for more information.

Field/Actions	Function
Fields/Actions	Select the field type: ■ UserID ■ Password/OldPassword ■ Third Field ■ Fourth Field ■ New Password ■ Confirm New Password Use the **Up** and **Down** arrows to reorder the fields for correct navigation through the form. Click **Edit** to specify the way the Agent navigates the form.

2.13.6.9 Matching Tab for Configuring a Host or Mainframe Application

Use the **Matching** tab to specify the text that identifies the screen as a logon or password-change form.

Field	Function
Row	Enter the **row number** (vertical screen coordinate) of the first character of the text. For Telnet applications (with supported host emulators), this value is relative to the cursor position and can be negative (to indicate a row above the cursor) or an asterisk (*) to indicate any row onscreen.
Column	Enter the **column number** (horizontal screen coordinate) of the first character of the text. For Telnet applications (with supported host emulators), this setting can be an asterisk (*****) to indicate any row onscreen
Text to Match	Displays the literal Text string that the Agent uses to identify this form: the screen coordinates (Row and Column numbers) of the first character of the string. Click **Add** to specify a new text identifier or **Edit** to modify an existing one.

2.13.6.10 Options Tab for Configuring a Host or Mainframe Application

Use the **Options** tab to configure behaviors for a host or mainframe application.

To display this tab, do one of the following:

1. Create a new host/mainframe application logon.

or

1. In the left pane, click **Applications** and select a host/mainframe application.

2. Click the **General** tab in the right pane.

3. Select a logon form from the list and click **Edit**.

4. In the **Host/Mainframe** form-configuration dialog, select the **Options** tab.

Control	Function
Field Delay	Enter a time in milliseconds for the Agent to wait to submit credentials.
Screen type	Specify whether the application has a fixed or scrolling screen.

Control	Function
Column position of cursor	Specify the column where the cursor should be placed before starting to enter credentials.
	Enter the starting column number of the text cursor when logon or password change begins. If this position varies (for example, most Unix systems include the affected username as part of the **New Password** and **Confirm Password** field labels when changing passwords), you can use a wildcard for the variable portion of the field label so that Logon Manager always injects credentials in the correct spot.
Adhere to logon loop grace period	Select to have the Agent ignore this application's logon form when the logon loop grace period (set on the application's **Miscellaneous** tab) is in effect.
Auto-Recognize	Select to have the Agent recognize the application automatically. If this setting is checked or unchecked, it overrides the Global Agent Setting. If this setting is checked, the user can configure this setting from Logon Manager. If this setting is unchecked, the user will not have access to this setting from Logon Manager.
Auto-Submit	Select to have the Agent automatically select **OK** for this application logon after providing credentials.

2.14 Configuring a Specific Application

The application list represents all configured application in Logon Manager. Use the tabs in the right pane to view or modify an application's properties.

To select an application for viewing or editing:

1. Click **Applications** in the left pane, then click the **Applications List** tab in the right pane.

2. Select an application from the list, then click **Edit**.

or

1. In the left pane, click the plus sign (**+**) next to the **Applications** icon (or double-click **Applications**) to display the configured logons.

2. Do one of the following:

   ■ Click a logon icon to select it. The **General** tab appears in the right pane.

      or

   ■ Right-click a logon icon to display a shortcut menu with the following options:

Option	Function
New Form	Add a new form for the selected application logon. Displays the corresponding configuration dialog for the selected application type.
Delete	Delete the selected logon.
Make copy	Duplicate the selected logon.
Rename	Rename the selected logon.
Publish…	Select to launch the **Publish to Repository** dialog, from which you can select among all publishable items and the repository to which you want to publish them.
Publish To	Select to specify a repository to which you want to publish a specific item.

2.14.1 General Tab (for a Selected Application

Use the **General** tab to add or modify form or field configurations for the selected application.

Option	Function
Description	A meaningful description of the application for the user.
Reference	An internal reference describing the version/variant of the application template. **Note:** This field is read-only on the client side.
Category	Enter the category under which the application will appear; for example, "Finance," "Development," and so on.
Icon Image URL	The URL to the icon image that will appear next to the application entry.
Logo Image URL	The URL to the full-size application logo image.
Vendor	The vendor of the application.
Administrator	Contact information for the application's administrator within your organization.
Forms	A list of all forms associated with this application.
Add	Add a new form for the selected application. The corresponding configuration dialog for the selected application type appears.
Edit	Modify an existing logon form. Select a form from the **Forms** window, then click **Edit**. The corresponding configuration dialog for the selected application type appears.
Delete	Remove a form. Select a form from the **Forms** window, then click **Delete**. If only one form is listed, deleting it will remove the application entirely.
Add Notes	Type or modify optional comments or documentation.
Deny response	Check this button to prevent the Agent from responding to this form. **Note:** Disabling any form in a template disables the entire template.

To display this tab:

1. Do one of the following:

   - Select an application.

     or

   - Configure a new application.

2. Click the **General** tab in the right pane.

2.14.2 Bulk Add Tab (for a Selected Application)

Use the **Bulk-Add** tab for special configurations of the currently-selected application. Also see Bulk-Adding Applications for First-Time Use for more information.

Control	Function
Enable Bulk-Add capability for this application	Select to enable this application to be included in a bulk-add.
Confirm UserID during Bulk-Add	Select to require the user to confirm username in order to perform a bulk-add.

Control	Function
Confirm Password during Bulk-Add	Select to require the user to confirm password in order to perform a bulk-add.
Confirm Third Field during Bulk-Add	Select to require the user to confirm a third field's information in order to perform a bulk-add.
Confirm Fourth Field during Bulk-Add	Select to require the user to confirm a fourth field's information in order to perform a bulk-add.

To display this tab:

1. Do one of the following:

    ■   Select an application.

        or

    ■   Configure a new application.

2. Click the **Bulk-Add** tab in the right pane.

2.14.3 Authentication Tab (for a Selected Application)

Use the **Authentication** tab to set the minimum authentication grade for the selected application.

The Primary Logon Method used must have an Authentication Grade equal to or higher than this value in order for Logon Manager to log on to the selected application.

If the end-user's Primary Logon Method has an authentication grade lower than the minimum set for this application, when the user requests access to the application, Logon Manager prompts the user to authenticate at a higher grade. The user will only gain access after successfully logging on at the required grade.

To set the authenticator grade for primary logon methods using the Authentication Grade setting.

Control	Function
Minimum Authentication Grade	Select or type the numeric value of the lowest Authentication Grade the end user's Primary Logon Method must have. The default is 1.

To display this tab:

1. Do one of the following:

    ■   Select an application.

        or

    ■   Configure a new application.

2. Click the **Authentication** tab in the right pane.

2.14.4 Error Loop Tab (for a Selected Application)

Use the **Error Loop** tab (under a selected application) to control the appearance and behavior of the **Logon Error** dialog for individual applications.

Control	Function
Logon timeout (sec.) [TimeOut]*	Maximum time in seconds between successive logon attempts before Logon Error dialog appears. Default is 30. **Note:** If the logon timeout is set to zero (0), a logon error (for example, entering the wrong credentials) does not cause the **Logon Error** dialog to display.
Max. retries [MaxRetry]*	Maximum number of retries (after first try) allowed before the **Logon Error** dialog appears. Default is 0.
Hide "Confirm Password" [HideConfirmPW]*	Whether to suppress the **Confirm Password** dialog after the user enters a password. Default is No.
*(Global registry equivalents shown in brackets.)	

To display this tab:

1. Do one of the following:

   ■ Select an application.

      or

   ■ Configure a new application.

2. Click the **Error Loop** tab in the right pane.

2.14.5 Password Change Tab (for a Selected Application)

Use the **Password Change** tab to set or modify options that control how the Agent manages password changes.

The Agent distinguishes between logon and password change fields that appear on the same screen or on different tabs of a dialog. In the instance of this type of screen, the Agent prompts the user, through the **Action Chooser** dialog, to select a password change or logon. You can configure a period of time for which the user will not need to change passwords, and hence will not receive the **Action Chooser**.

Setting Group	Control	Function
Password Change	Password Change Dialog Behavior	Controls how the Agent responds when an application prompts the end user to change passwords. The options are: ■ **Prompt User.** Prompts the user with the Password Change Wizard. ■ **Manual.** Prompts the user to select a new password; does not let the Password Change Wizard automatically generate a password. ■ **Manual w/Auto Option.** Prompts user to select a new password, but lets the Password Change Wizard offer to generate a password automatically. ■ **Auto w/Manual Option.** Generates a new password automatically, but first allows the user to select a new password. ■ **Quietly Generate and Submit Password.** Generates and submits password without prompting the user.

Setting Group	Control	Function
	Prevent Ability to Cancel	When enabled, disables the **Cancel** button in the password change dialog, prohibiting the user from canceling the password change process.
	Enable Password verify pop-up dialog	Check this box if you want to display the password change verification pop-up dialog, which provides an additional confirmation that the password has been changed.
	Lock focus to password change dialog	When enabled, locks desktop focus to the password change dialog, preventing interaction with the target application until the user completes or dismisses the dialog.
	Allow to finish with unsaved changes after successful submit	Check this box to allow the user to finish the password change process after a successful submission, even if he has unfinished updates. Logon Manager displays a warning message, alerting the user that he has unsaved changes.
	Password Generation Policy	Select a password generation policy. To subscribe multiple applications to a policy, see Managing Policy Subscribers. Also see Creating Password Generation Policies.
	Credential Sharing Group	Select a credential sharing group. To assign multiple applications to a password group, see Working with Credential Sharing Groups.

Setting Group	Control	Function
Password Expiration	Enable Password Expiration	Select this check box to require users to change passwords after a specified period.
	Number of days until password expires	Enter or select the number of days for which a user's password is valid.
	Run this command when the password expires	Type the full path and command (or click **Browse** to locate the executable file) that should be invoked when the user attempts to log on after the Number of days setting has elapsed.(Example: `C:\Program Files\PassChange\passchange.exe`.)

Setting Group	Control	Function
Logon Chooser	Bypass Logon Chooser	Controls whether the **Logon Chooser** appears when a password change is initiated. When enabled, the password change dialog will be displayed immediately if the selected condition is met. The available conditions are listed below.
		Options:
		■ When the most recent logon was to the same application instance.
		■ When the most recent logon for the same application occurred within:
		If you select the second condition, specify the length of the timeout in seconds. Valid range is 1-999999 seconds.

Setting Group	Control	Function
	Bypass Logon Chooser for This setting is new as of 11.1.1.5.0.	If you select to bypass the Logon Chooser by either means above, specify the forms that you want the Agent to bypass. Options: ■ Password Change and Logon forms. ■ Password Change form only.

Setting Group	Control	Function
Action Chooser Grace Period	Days	Enter the length of the grace period (in days) for which the Agent will not display the **Action Chooser** dialog.
	Automatically proceed with password change	When enabled, the Action Chooser is bypassed when the grace period expires and password change initiates automatically. **Note:** This option is only available after the grace period has been specified.

To display this tab:

1. Do one of the following:

    ■ Select an application.

      or

    ■ Configure a new application.

2. Click the **Password Change** tab in the right pane.

2.14.6 Events Tab (for a Selected Application)

Use this tab to add a logon event and configure the environment surrounding it.

Setting Group	Control	Function
Add Logon Event	Run this command when a logon for this application is added	This setting allows you to define a process (such as exe, web, script, etc.) to be run immediately after the Add Logon Wizard is completed for an application. For example, this setting could be used to launch a password change application right after credentials are entered into the Agent, thus allowing the Agent to change the application password immediately. Click the **Browse** button to locate a command to be entered.

Setting Group	Control	Function
Pre Logon Event	Run this command before a logon for this application is used	This setting allows you to define a pre-logon task that occurs prior to each logon instance, transmitting information from this process about the current logon attempt. The information in the resulting exit code cues Logon Manager whether to continue credential submission or abort the logon process.
		For example, you might want to run a script to call an API, perform a task to ensure that an application is in the state required for logon, or check usernames against a list of permitted or prohibited applications.
		Click the **Browse** button to locate a command to be entered.
	Failure Return Code	The Agent will ignore a logon returning a number of errors equal to or higher than the number set in this field. A higher setting allows the application to return multiple error codes. The default for this setting is 1.
	Time out	Specifies the time, in milliseconds, for the Agent to wait for the task to complete. This setting is incremental from 1.000 to 5.000 milliseconds (default). If the task has not completed within the specified time, the task terminates and logon does not occur.

Note: It is recommended that you specify a full path to the application to run, and surround it with double quotes. For example, `"C:\Program Files\My Tools\checktool.exe"`

2.14.7 Miscellaneous Tab (for a Selected Application)

Use this tab for special configurations of the currently-selected application.

Setting Group	Control	Function
Miscellaneous	Allow Masked Fields to Be Revealed	Select to enable the **Reveal** button for masked fields in Wizards and property pages.
	Force Reauthentication	Select to require the user to reauthenticate before providing credentials to this application.
	Auto Submit	Select to have the Agent automatically select **OK** for this application logon after providing credentials.
	Service Logon	Select to let the Agent detect an application that runs as a Windows service (that is, in the System space, rather than the User space).
	Auto-Recognize	Select to have the Agent recognize applications and Web sites and log users on automatically. If this setting is checked or unchecked, it overrides the Global Agent Setting.
		If this setting is checked, the user can configure this setting from the Logon Manager. If this setting is unchecked, the user will not have access to this setting from the Logon Manager.
		If this setting has a green box instead of a check, this means that the user can configure this setting from Logon Manager.

Setting Group	Control	Function
	Mask Third Field	Select to mask the third field of an application logon. This affects the third field appearance on the following pages: New Logon property, Error Loop dialog, Logon Properties, and FTU Entry. By default, this box is checked (third field is masked).
	Mask Fourth Field	Select to mask the fourth field of an application logon. This affects the fourth field appearance on the following pages: New Logon property, Error Loop dialog, Logon Properties, and FTU Entry. By default, this box is checked (fourth field is masked).
	Prohibit disabling the addition of new logons	Specifies whether the **Disable** button in the New Logon dialog is active for this application. When enabled, the **Disable** button is deactivated and the user is prohibited from adding new logons for this application when auto-prompted by the Agent. When disabled, clicking the **Disable** button adds this application is to the **Exclusions** list in the Agent settings dialog. Options: ■ Yes ■ No (default)
	Prohibit canceling the addition of new logons	Specifies whether the **Cancel** button in the New Logon dialog is active for this application. When enabled, the **Cancel** button is deactivated and the user is prohibited from canceling a logon addition in progress for this application after being auto-prompted by the Agent. When disabled, clicking the **Cancel** button defers the logon addition until the next time this application is detected. Options: ■ Yes ■ No (default)
	Allow creation of multiple accounts during credential capture	Specifies whether to enable the checkbox that allows the user to add another set of credentials in the **New Logon** dialog. For any template, this setting overrides the Global Agent Setting of the same name.
	File extension (for Icon)	Enter a Windows file extension associated with a logon. Instructs the Agent to map an icon to the configuration.
	ConfigName	Click **Choose** to select the windows and control that contains the text to use to create the new logon's initial configuration name (Windows applications only).
	UserID Field Label	Type a text label to be used by the Agent for the username/ID field.
	Password Field Label	Type a text label to be used by the Agent for the password field.
	3rd Field Label	Type a text label for the Agent to use when displaying a third logon field.
	4th Field Label	Type a text label for the Agent to use when displaying a fourth logon field.

Setting Group	Control	Function
Logon Chooser	Logon chooser columns	Select **Choose** to open the **Logon Chooser Columns** window, which contains a list of possible columns to display in the **Logon Chooser** dialog.
		Note: Third and Fourth field selection is available only if you do not choose to mask them in the setting above.

Setting Group	Control	Function
SendKeys Settings	Delay Char	Use this setting to add a delay, in milliseconds, between every press in SendKeys, slowing credential submission. This setting is useful for applications that require additional time to recognize credential input.

Setting Group	Control	Function
Logon Loop Grace Period	None	The user is logged on automatically after initial logon. There is no grace period between logon prompts. (Default)
	Prompt	If the logon grace period has not expired, the user receives a prompt asking if he wants to log back on to an application.
	Silent	The Agent ignores the application for the duration of the grace period and does not inject credentials until the grace period expires.
	Minutes	Set the length of the grace period in minutes.
	Reset for each process	When enabled, the grace period is reset for each new process that is launched. This will cause Logon Manager to log the user on to an application when the application is closed and restarted, even if the grace period has not expired.
		When disabled, the grace period is not reset for each new process. Logon Manager does not attempt to log the user on to an application that has been restarted until the grace period has expired. (When this is disabled and the grace period has not expired, the user will be prompted to log on again if the Prompt/Silent option is set to Prompt.)

Setting Group	Control	Function
Credential Capture Mode		Configures credential capture behavior by using one of the modes below.
		Note: Silent credential capture mode is not compatible with applications that require SendKeys. For this reason, you cannot use this mode for host/mainframe applications, nor for any Web or Windows application for which you use SendKeys.
		You should not use silent credential capture for applications where the username and password are obfuscated.
	Default to global agent setting	Specifies that this application should use the same value as that in the global agent setting.
		Selecting any of the following settings overrides the global agent setting.

Configuring a Specific Application

Setting Group	Control	Function
	Do not capture silently	Presents the **New Logon** dialog in which the user enters credentials manually.
	Capture, but do not inform user	The Agent captures the credentials as the user enters them, and does not inform the user of the process.
	Capture, and inform user with balloon tip	The Agent captures the credentials as the user enters them, and displays a balloon tip near the system tray to inform the user during the process.
	Capture, and present New Logon dialog	The Agent captures the credentials as the user enters them, and displays a balloon tip near the system tray to inform the user during the process. After capturing the credentials, the Agent displays the **New Logon** dialog with the user's entries pre-filled. The user can accept, change, cancel, or disable.
	Silent capture timeout	The time (in milliseconds) that the Agent should wait to create an account after the user submits credentials. If this timeout expires before the Agent can determine if the logon succeeded or failed, it dismisses the credentials it captured.

To display this tab:

1. Do one of the following:

   ■ Select an application.

   or

   ■ Configure a new application.

2. Click the **Miscellaneous** tab in the right pane.

2.14.8 Security Tab-Role/Group Support (for a Selected Application)

Use this tab to set the access rights for the currently selected configuration item. You can assign access rights to these items:

■ Application logons (including associated credential sharing groups)

■ Password generation policies

■ Global Agent settings

■ Passphrase question sets

■ Exclusion lists

> **Note:** For increased security on Active Directory domains, right-click the domain administrator's name and select **DENY**. This action will ensure that application templates are not automatically sent to domain administrators.

Control	Function
Directory	Select the target directory server.
Access information:	
Name	Lists the groups or users who currently have access to this item.

2-140 Oracle Fusion Middleware Administering Oracle Enterprise Single Sign-On Suite

Control	Function
ID	The user account name.
Access	Indicates whether the user or group has read/write or read-only access rights to the currently selected item. To change a user or group's access rights, right-click the user or group and select **Read** or **Read/Write** from the shortcut menu.
Actions:	
Copy Permissions To…	Displays the Select Application screen. Select an application to add; use **Ctrl+Click** or **Shift+Click** to select multiple entries. Click **OK** to confirm your selection.
Add	Displays the **Add User or Group** dialog (for LDAP or Active Directory) to select the users or groups who should have access to the currently selected item. Click **OK** to confirm your selection.
Remove	Removes selected user(s) or group(s) from the list. Select a user or group to remove; use **Ctrl+Click** or **Shift+Click** to select multiple entries. Click **OK** to confirm your selection.

2.14.9 Provisioning Tab-Role/Group Support (for a Selected Application)

To access this tab, expand **Applications** and double click any application. Click the **Provisioning** tab.

From this tab, you can add and remove permissions. You can also select the level of access rights (for example, add/modify/delete applications) for those permissions.

Control	Function
Directory	Select the target directory server.
Access information:	
Name	Lists the groups or users who currently have access to this item.
ID	Lists the user account name.
Access	Indicates the permissions that have been granted to the user or group (Add, Modify or Delete Logon). To change a user or group's access rights, right-click the user or group and select **Add Logon**, **Modify Logon** or **Delete Logon** from the shortcut menu.
Actions:	
Copy Permissions To…	Use this button to easily apply the provisioning rights for the current application to multiple applications. Clicking this button displays a dialog listing all the applications. Selects the applications that you want these provisioning rights to be copied to. Use **Ctrl+Click** or **Shift+Click** to select multiple entries. Click **OK** to confirm your selection.
Add	Displays the **Add User or Group** dialog (for LDAP or Active Directory) to select the users or groups who should have access to the currently selected item.
Remove	Removes selected user(s) or group(s) from the list. Select a user or group to remove; use **Ctrl+Click** or **Shift+Click** to select multiple entries.

2.14.9.1 Add User or Group Dialog

The Select User or Group dialog varies based on the directory server being used:

- LDAP
- Active Directory

■   AD LDS (ADAM)

2.14.9.1.1 LDAP Use this dialog to select the individual users or user groups that you want to add to the access list for the current configuration item (Add Logon, Modify Logon, or Delete Logon).

Control	Function
Search Base	The base (highest-level) directory to begin searching for user/group accounts. All subdirectories of the base directory are searched. Enter a location or click **Change** to browse the directory tree.
Change	Displays the **Select Search Base** dialog to browse for a base directory for the search. Use this dialog to browse to and select the base (highest-level) directory to search for user/group names. Click **OK** when finished.
Search	Begin searching the base directory for users and groups.
Users or Groups	Lists the search results. Select the names to be added to the access list for the current configuration item. Use **Ctrl+Click** or **Shift+Click** to select multiple entries. Click **OK** when finished to copy your selections to the access list.

2.14.9.1.2 Active Directory and AD LDS (ADAM) Use this dialog to select the individual users or user groups that you want to add to the access list for the current configuration item (Add Logon, Modify Logon, or Delete Logon).

Control	Function
List Names From	Select an Active Directory domain or server.
Names	Lists the names of users and groups for the selected domain or server. Select one or more names to add to the access list.
Add	Copies user(s) and group(s) selected in the Names list to the **Add Names** list. Use **Ctrl+Click** or **Shift+Click** to select multiple entries.
Members	When a group is selected in the **Names** list, displays the Global Group Membership dialog, which lists the members of the selected group.
Search	Displays the **Find Account** dialog for searching one or more domains for a specific user or group.
Add Names	Display the names of the user(s) or group(s) that have been added. Click **OK** to add these names to the access list for the current configuration item. **Note:** You can type or edit user names in this list. However, entries are checked for invalid account names, and duplicate account selections are automatically removed when you click **OK**.

2.14.10 Privileged Accounts Tab (for a Selected Application)

Use this tab to specify whether the account for this template is privileged. Check the box to identify this template as belonging to a privileged account.

See Privileged Accounts Settings for more information about configuring a privileged account.

2.14.11 Delegated Credentials Tab (for a Selected Application)

Use this tab to specify whether a user can delegate credentials for this application to another user, and the terms of the delegation. This feature is useful in scenarios where one user (the delegator) temporarily assigns some responsibilities to another user (the delegatee), but where the delegatee will not be performing the delegator's duties permanently.

The delegator is required to authenticate when revoking a delegated credential. To complete the revocation, the delegatee must also authenticate. This causes a repository synchronization that reverts the credentials back to their undelegated state.

Only the delegator can revoke delegated credentials. If for any reason you need to revoke credentials from the delegatee in the delegator's absence, you can lock the delegatee's account and force a password reset.

Delegated credentials are installed during installation of the Logon Manager Client as one of the selections in the Advanced installation setup mode.

Control	Function
Allow users to delegate credentials for this application	Check the box if you want to allow a user to delegate credentials to another user. After the box is checked, the following configuration options become available.
	Default is Disabled.
Allow reveal password	Specify whether to allow the delegatee to see the delegator's password.
	Default is Disabled.
Maximum number of delegation days	Specify the maximum number of days that the delegatees has the delegator's credentials for this application.
	Default is 15.
Permitted usage	Specify the day(s), and time interval for each day, that the delegatee can access the application.

> **Note:** You must also specify the path to the provisioning service and the encryption algorithm in the Global Agent Provisioning Settings.

2.14.11.1 Setting Up Delegated Credentials with Oracle Repositories

You have the option of using Oracle Internet Directory (OID), Oracle Unified Directory (OUD), or Oracle Virtual Directory (OVD) for your repository. Perform the following configuration steps to use delegated credentials with any of these Oracle repositories.

1. Navigate to the Provisioning Gateway Service folder (typically, `%PG_SERVER%\Service`).

2. Open the web.config file in a text editor. Near the end of the file there are two lines:

   - `<add key="LDAP_Username" value="" />`

   - `<add key="LDAP_Password" value="" />`

3. Set the value attribute of these lines to the username and password of a directory account with permissions to do the following (this account does not have to be an administrator account):

   - Read the objects in the Locator container

- ■ Read the objects in the CO container

- ■ Read and write objects in the People container and its sub-containers

4. Encrypt the `web.config` file where you are storing these credentials:

   a. From the command prompt, go to the directory:
   `%Windows%\Microsoft.NET\Framework\v2.0.50727`.

   b. Enter the following command: `aspnet_regiis -pef "appSettings"`
   `"C:\Program Files\Passlogix\v-GO PM\Service"` (assuming you installed
   the Provisioning Gateway server in the folder: `C:\Program Files`).

   c. Open the `web.config` file to make sure the `appSettings` section has been
   encrypted.

2.14.11.2 Export to INI File

An `entlist.ini` file is a store of selected application, all password policies, and
groups. To export selected items to an `INI` file:

1. Do one of the following:

   - ■ Select applications to export (use **Ctrl+Click** or **Shift+Click** to select multiple
   entries), then click **OK**.

     or

   - ■ Click **Export All** to export all listed applications.

2. If any of the applications you have selected is enabled for Bulk-Add, you can
   select Create First-Time-Use file to generate a bulk-add (`ftulist.ini`) file.

3. Click **OK**. The **Export EntList file** dialog appears.

4. Locate and open the folder for the file, name the file, and click **Save**.

5. If you chose to create a First-Time Use file, the Export First-Time Use dialog
   appears. Locate and open the folder for the file (rename the file if desired), and
   click **Save**.

To display the **Export EntList file** dialog:

- ■ Right-click **Applications** and select **Export** from the shortcut menu.

  or

- ■ Choose **Export** from the **File** menu.

2.14.11.3 Export EntList File

Save an exported application configuration file (`enlist.ini`) to disk. The Export
EntList file dialog displays when you export application logon information using the
Export to `INI` dialog.

1. Locate and open the folder for the file, name the file, and click **Save**.

2. If you chose to create a First-Time Use file, the **Export First-Time Use** dialog
   opens. Locate and open the folder for the file (rename the file if desired), and click
   Save.

2.14.11.4 Export First-Time Use

Save a first-time-use file (`ftulist.ini`) to disk. The **Export First-Time Use** dialog
opens when you create a First-Time Use file while exporting application logon
information to an `enlist.ini` file.

1. Locate and open the folder for the file (rename the file if desired).

2. Click **Save**.

2.14.11.5 Import Merge Conflict

The **Import/Merge Conflict** dialog appears if the merged file contains items with the same names as those in the current configuration.

■   Select the items to import and click **OK**.

   The items you select overwrite the current like-named items.

2.14.11.6 Override Settings Tab (Edit Template Dialog)

Use this tab to select the settings that the template updates in all logons that are based on it. You can choose global overrides that apply to all of the forms in the application logon configuration, and you can also select specific overrides for individual forms.

The left pane displays the hierarchy of the application and its component forms:

■   The global override settings for applications correspond to the general configuration settings for each application-type.

■   The form-specific settings correspond to the configuration controls for individual logons.

Both Setting types are listed in the right pane with a category that corresponds to the application-configuration dialog in which you make the setting. Refer to the dialog or tab for information on each setting.

Control	Function
Applications	■ General
	■ Error Loops
	■ Password Change
	■ Miscellaneous
Windows forms	■ General
	■ Fields
	■ Matching
	■ Miscellaneous
Web forms	■ General
	■ Matching
Mainframe/Host forms	■ General
	■ Options

To display this tab:

1. Choose **Manage Templates** from the **Tools** menu.

2. Do one of the following:

   ■   Add a new template.

      or

   ■   Select an existing template and click **Edit**.

3. In the **Edit Templates** dialog, select the **Overriding Settings** tab.

2.14.11.7 Supply Info Tab (Edit Template Dialog)

Use this tab to specify what information an administrator must provide in order to complete an application logon based on this template. You can choose all items or choose individual items by selecting checkboxes.

2.14.11.8 Update Applications (from Template)

Use this dialog to update application logons based on a template that has been modified since the logons were created. Only logons whose templates have been modified appear in the list. Select the applications to update (use **Ctrl+Click** or **Shift+Click** for multiple applications), then click **Update**.

2.14.11.9 Launch Tab (for a Selected Application)

Use this tab to specify the location of the target application.

Control	Function
Launch URIs	The list of URI(s) that will be accessed when the user launches the application. Click **Add** or **Edit** to open the **Manage Launch URI** dialog, where you configure these URIs.
Login Failure URI	The URI that should be accessed if the user's logon fails.
Add	Allows you to add a URI to the list by opening the **Manage Launch URI** dialog.
Edit	Allows you to change settings for a selected Launch URI by opening the **Manage Launch URI** dialog.
Delete	Deletes the selected Launch URI.

2.14.12 Launch Tab (for a Selected Application)

Use this tab to specify the application launch URI, as follows:

1. In the **Launch** tab, click **Add**.

2. In the **Manage Launch URI** dialog's **Type** dropdown:

   ■ Select **Web** for a client application that supports launching a Web application directly.

   ■ Select **WebProxy**, for a client application that does not support launching a Web application directly.

3. Enter the URI or (its proxy version, depending on your selection in the previous step) of the target Web application. This URI will be accessed when the user launches the application. Obtain this URI from your application administrator.

4. Click **Update** to save your changes.

Control	Function
Launch URIs	The list of URI(s) that will be accessed when the user launches the application. Click **Add** or **Edit** to open the **Manage Launch URI** dialog, where you configure these URIs.
Login Failure URI	The URI that should be accessed if the user's logon fails.
Add	Allows you to add a URI to the list by opening the **Manage Launch URI** dialog.
Edit	Allows you to change settings for a selected Launch URI by opening the **Manage Launch URI** dialog.

Control	Function
Delete	Deletes the selected Launch URI.

2.14.12.1 Manage Launch URI

Use this tab to specify the location (the target) that will be accessed when the user launches the application.

Control	Function
Type	Select the type of URI that this will be: ■ Web ■ WebProxy
URI	Enter the URI or its proxy version of the target Web application.
Update	Click to save the new configuration and close the **Manage Launch URI** dialog.
Close	Click to close the **Manage Launch URI** dialog without saving changes.

2.14.13 Testing Templates

The Administrative Console Template Test Manager provides a simple way to validate templates that you have created, before publishing them. It engages the Agent directly, bypassing the repository and synchronization. The manager guides you through the test, prompting you to take action at various points, and asking questions about the results. Your answers to these questions are the cue to the manager's next steps.

Using the Template Test Manager requires the following:

■ The Administrative Console

■ The Logon Manager Agent

■ Application templates that you want to test added to the Administrative Console

■ Applications whose templates you have added to the Administrative Console

> **Note:** The Template Test Manager supports Windows applications only.

To use the Template Test Manager:

1. Launch the Administrative Console.

2. Right-click on a template under the **Applications** menu, and select **Test** to launch the Template Test Manager. During testing, the Administrative Console application window minimizes and the Template Test Manager receives focus.

3. Observe the three sections of the manager window:

   ■ The **Forms to be validated** section contains the name of the template (and all its forms) that you have selected to test. A status icon appears next to each name to indicate its status:

   Processing
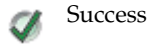
Success

Failure

- The **Status Messages** section apprises you of the test status.

- The **Interactions** section prompts you to take the actions required to proceed with the test. Watch the status messages and follow the interactions prompts and proceed accordingly.

4. The manager asks if the Agent detected the template. If the test was successful, click **Yes**, and then click **Finish**. If the test is not successful, click the button that best describes why detection was unsuccessful:

- Yes, but also responds to other windows that should be ignored.

- No (any other reason).

5. Click **Next** to receive suggestions to correct the errors in the template.

6. Continue the process until the Agent responds correctly to the template.

7. Select **Close** to shut down the Template Test Manager and return to the Administrative Console.

Example

1. In the Administrative Console, you have selected an application template, right-clicked it, and selected **Test**. The Template Test Manager launches, and the template's forms appear in the "Forms to be validated" section, but the Agent is not running. The **Status Messages** section reads, "Waiting for the Logon Manager Agent…" This indicates that the Agent is not active and that you must launch it to begin the test. So, the **Interactions** section displays the action request, "Launch the Logon Manager Agent."

2. You launch the Agent, and the status message indicates that the Template Test Manager is publishing the template to the Agent. The "Actions" message prompts you to launch the application for the template you are testing.

3. After you launch the application, the Agent should detect it and respond (in accordance with your configuration for initial credential capture).

4. The **Interactions** section informs you that you are at the "Detection" stage and presents the question, "Does the Agent detect the window?" Select the appropriate response:

- Yes

- Yes, but also responds to other windows that should be ignored

- No

5. Click **Next**.

6. If you responded Yes, the Interactions section in the next screen informs you that the test was completed successfully. A check icon appears next to the template name.

7. If you responded with either of the other answers, click **Next** and the manager prompts you through a series of troubleshooting tests, offering suggestions based on your input.

8. Continue the process until you have modified the template to achieve successful results.

9. Click **Close** when done.

2.15 SSO Applications Node

The **SSO Applications** node allows you to add Federated and SSO-Protected applications to Logon Manager.

To add an application:

1. Do one of the following:

   - Right-click on the **SSO Applications** node and select the application type from the context menu.

   - Right-click in the empty area under **Applications List** and select the application type from the context menu.

   - Select the **SSO Applications** node and click the **Add** button at the bottom right.

2. In the **Add SSO Application** dialog, select an application type if it is not already selected, enter a name for this application, and click **OK**.

The application appears under the **SSO Applications** node. When you select it, two tabs display to the right:

- **General**

  Use this tab to define field configurations for the selected application.

Option	Function
Description	A meaningful description of the application for the user.
Reference	An internal reference describing the version/variant of the application template.
	Note: This field is read-only on the client side.
Category	Enter the category under which the application will appear; for example, "Finance," "Development," and so on.
Icon Image URL	The URL to the icon image that will appear next to the application entry.
Logo Image URL	The URL to the full-size application logo image.
Vendor	The vendor of the application.
Administrator	Contact information for the application's administrator within your organization.

- **Launch**

  Use this tab to specify the location of the target application.

Control	Function
Launch URIs	The list of URI(s) that will be accessed when the user launches the application. Click **Add** or **Edit** to open the **Manage Launch URI** dialog, where you configure these URIs.
Login Failure URI	The URI that should be accessed if the user's logon fails.
Add	Allows you to add a URI to the list by opening the **Manage Launch URI** dialog.

Control	Function
Edit	Allows you to change settings for a selected Launch URI by opening the **Manage Launch URI** dialog.
Delete	Deletes the selected Launch URI.

Manage Launch URI

Use this tab to specify the location (the target) that will be accessed when the user launches the application.

Control	Function
Type	Select the type of URI that this will be: ■ Web ■ WebProxy
URI	Enter the URI or its proxy version of the target Web application.
Update	Click to save the new configuration and close the **Manage Launch URI** dialog.
Close	Click to close the **Manage Launch URI** dialog without saving changes.

2.16 Configuring Logon Manager for Specific Environments

These topics describe how to configure Logon Manager to support specific environments.

■ Configuring the Agent for Windows Authentication

■ Configuring the Agent for Directory Server Synchronization

■ Configuring the Agent for Database Synchronization

■ Configuring the Agent for File System Synchronization

■ Configuring the Agent in a Citrix Environment

2.16.1 Configuring the Agent for Windows Authentication

Logon Manager supports Windows Authentication v2 as the Primary Logon Method (Authenticator), creating a true single sign-on user experience. The Agent can use the Windows logon credentials as its authentication. In order for Logon Manager to support this, the administrator needs to be aware of two issues:

■ The OS must have 128-bit encryption installed.

■ The administrator must enable user-level profiles.

2.16.1.1 Confirming 128-bit Encryption

To check the encryption strength of the OS, launch Microsoft Internet Explorer, and select **Help>About**. Confirm that Cipher Strength is 128-bit.

If the OS is not 128-bit, download the update from Microsoft:

http://www.microsoft.com/windows/ie/ie6/downloads/recommended/128bit/default.mspx.

2.16.2 Configuring the Agent for Directory Server Synchronization

This topic describes the settings needed to configure Logon Manager to use a directory server as a repository. The configuration is similar for all supported directory servers, with explanations of any differences.

■ See Using Role/Group Support with Directory-Server Synchronization for more information about how Logon Manager makes use of directory server resources.

■ See Configuring the Agent with Global Agent Settings for detailed descriptions of the associated registry entries.

> **Note:** Where the LDAP AUI and LDAP Directory Server extension are both installed, values must exist in both `AUI\LDAP` and `Extensions\SyncManager\Syncs\%LDAP%`.

1. Point Logon Manager to the server or servers.

2. Do one of the following:

    ■ From Global Agent Settings in the left pane, select an existing set of registry entries.

    ■ Import a saved set of settings (**File>Registry>Import**).

    ■ Create a new set of registry settings (**Insert>Global Agent Settings**).

3. In the left pane of the Administrative Console, select and open the set of settings, select and open **Synchronization** (add the appropriate extension if needed), select and open the appropriate extension, then select and open **Servers**.

4. In the right pane, select **Servers**, select the ellipsis ("**…**") button, enter the server names, or IP addresses, and click **OK**.

    For Microsoft Active Directory Server (other than AD LDS (ADAM)):

    ■ If no Servers are entered for the Active Directory extension, and the user account is in an Active Directory domain, then Logon Manager uses Active Directory domain resources to discover the server. If one or more servers are specified in the Global Agent Settings, then Logon Manager uses the Servers list to locate the server.

    ■ Unless otherwise configured, Logon Manager queries the domain name server (DNS) for the name of the preferred domain controller assigned to the local subnet.

    ■ In Active Directory networks with multiple servers, be sure to enable replication in order to include the Logon Manager schema extension and related objects. This assures that Logon Manager will always find SSO information on every server it connects with.

    ■ If one or more servers are provided for Microsoft Active Directory Server, use server names, rather than IP addresses.

    For Microsoft AD LDS (ADAM):

    ■ At least one server must be specified for AD LDS (ADAM) services.

    ■ Use the port parameter (for example myserver.com:9890) to specify particular instances of AD LDS (ADAM) running on a single server.

    ■ Applications templates must reside in a specific OU and not at the root of the AD LDS (ADAM) instance.

5. Point Logon Manager to the **User path**.

6. In the left pane, select the appropriate extension. Then do one of the following:

   ▪ For an LDAP extension, select **Required**.

   ▪ For an Active Directory extension, select **Advanced**.

7. In the right pane, select **User Paths**, then select the ellipsis ("**…**") button, enter the user path(s), and click **OK**.

8. Enable or disable SSL.

9. In the left pane, select the appropriate extension.

10. In the right pane, select SSL options as follows:

11. If using SSL, select SSL (for LDAP or Active Directory) and select Connect via SSL (defaults to port #636).

    > **Note:** SSL is not enabled by default; the non-secure default port is #389.
    >
    > To set non-standard ports, use the Servers setting (for LDAP or Active Directory).

12. If using SSL, select **When SSL Fails** (for LDAP or Active Directory) appropriately.

    For Novell eDirectory: There are two major caveats for Novell eDirectory and some other environments. If the domain name for a user is in the form of:

    ```
    cn=%UserName%,ou=people,dc=Oracle,dc=com
    ```

    instead of the form:

    ```
    namingattribute=%UserName%,ou=people,dc=Oracle,dc=com
    ```

    where *namingattribute* can be any string, do the following:

    a. In the left pane, select the appropriate extension, then select **Advanced**.

    b. Select **Naming Attribute string** and set it to **CN**.

    c. Select **Alternate User ID location** and set it to:

    ```
    uid=%user%,path
    ```

    where *path* is the rest of the path to the object; for example:

    ```
    uid=johnd,ou=people,dc=Company,dc=com
    ```

2.16.2.1 Using Role/Group Support with Directory-Server Synchronization

In directory-server synchronization installations, Logon Manager provides support for role/group access control for individual configurations, including application logons, password-change policies, Global Agent Settings, and passphrase question sets. When this feature is enabled, you can assign access-control lists, similar to those used in Windows security to the individual logons, policies, settings, and question sets.

Role/group support-enabled configurations are exported to a synchronizer container object just like the standard Logon Manager configuration objects (EntList, FTUlist, and AdminOverride). When role/group support is enabled and these access-controlled objects are present in the container, they override the standard objects. Follow these steps to configure role/group support:

1. Configure these Global Agent Settings to enable role/group security support and update the Agent:

Setting Location	Setting Name	Function
Synchronization	Enable role/group security support	Enables role/group support for application logons, password policies, Global Agent Settings, and passphrase question sets. Options: ■ Do not use role/group security (default). ■ Use role group security.
Synchronization > selected sync > Advanced	Configuration Objects Base Locations (LDAP, Active Directory, AD LDS (ADAM))	Specifies where to begin the search for role/group-enabled configuration objects. The search is from the specified locations or locations downward, (away from the root). If there are no entries for this setting, the search is from the root.

2. Specify the access rights for each configuration:

   Use the **Security** tab for each configuration (application logons, password policies, Global Agent Settings, and passphrase question sets) to specify the users and groups that should have access to it.

3. Export the configurations to a synchronizer container.

4. Connect to the synchronizer directory.

5. In the right pane, right-click a container object and choose Publish to Repository from the shortcut menu to display this window.

6. Choose **Administrative Console** as the Data Source.

7. Choose and complete the Wizard procedure to export the configuration objects as individual, access-controlled objects.

> **Note:** For best performance and highest security, Oracle recommends the following practices:
>
> ■ Unless your organization explicitly requires role/group support, make certain that Enable role/group security support is set to **Do not use…**.
>
> ■ For best security, make certain that there are no user-writable areas anywhere down the directory tree from the location specified by Configuration Objects Base Locations (LDAP, Active Directory, AD LDS (ADAM)).
>
> ■ For best performance, always specify at least one location for Configuration Objects Base Locations. This ensures that the entire server is not searched.
>
> ■ To minimize the search load and length, be sure to store as little unnecessary data as possible down the directory tree from the location specified by Configuration Objects Base Locations.

2.16.3 Configuring the Agent for Database Synchronization

You can distribute the configuration settings described below to the client workstations either as part of the general deployment of the Agent software (by

modifying the MSI installer file) or, after Agent deployment, by distributing a registry entries (.REG) file to merge with the client workstation's registry.

- See Considerations Before Deploying Logon Manager for topics about Logon Manager Agent rollout.

- See Database Synchronization Support for more information about how Logon Manager makes use of database server resources.

- See Configuring the Agent with Global Agent Settings for detailed descriptions of the associated registry entries.

1. Point Logon Manager to the database server.

2. Do one of the following:

    - Import a saved set of settings (from the **File** menu, choose **Registry**, then **Import**).

    Note: The Console produces a .REG file compatible only with 32-bit systems. If you are merging the .REG file on a 64-bit system, you must run the following command to move the merged registry data to the correct location within the registry (otherwise, Universal Authentication Manager will not function):

    ```
    reg.exe COPY HKLM\Software\Passlogix
    HKLM\Software\Wow6432Node\Passlogix /s
    ```

    - Create a new set of registry settings (from the **Insert** menu, choose **Global Agent Settings**).

3. In the left pane, select and open the set of registry settings, select and open **Synchronization**, add the appropriate extension (if needed), select and open the appropriate extension, then select and open **Servers**.

4. In the right pane, select **Servers**, click the ellipsis ("**…**") button, enter the database server name(s) and click **OK**.

5. Export the settings to the Agent by selecting a method for initial distribution to client workstations:

    - Customize the MSI package that installs the Logon Manager Agent to include these settings.

    - Distribute a .REG file that you export from the Administrative Console. The .REG file can be merged with the client workstation's registry locally by double-clicking the file icon.

    Note: The Console produces a .REG file compatible only with 32-bit systems. If you are merging the .REG file on a 64-bit system, you must run the following command to move the merged registry data to the correct location within the registry (otherwise, Universal Authentication Manager will not function):

    ```
    reg.exe COPY HKLM\Software\Passlogix
    HKLM\Software\Wow6432Node\Passlogix /s
    ```

2.16.4 Configuring the Agent for File System Synchronization

This topic describes the settings needed to initially configure the Logon Manager Agent to synchronize application logons, global agent settings, and user credentials with a network file share.

The configuration settings described below can be distributed to the client workstations either as part of the general deployment of the Agent software (by modifying the MSI installer file), or after Agent deployment, by distributing a registry-entries (.REG) file that can be merged with the client workstation's registry.

- See Considerations Before Deploying Logon Manager for topics about Logon Manager Agent rollout.

- See File System Synchronization Support for more information about how Logon Manager makes use of file system resources.

- See Overriding Settings for detailed descriptions of the associated registry entries.

1. Point the Logon Manager Agent to the server.

2. Do one of the following:

   - Import a saved set of settings (choose **Registry**, then **Import** from the **File** menu).

   - Create a new set of registry settings (from the **Insert** menu, choose **Global Agent Settings**).

   - Select an existing set of registry entries (by selecting it in the left pane under **Global Agent Setting**s).

3. In the left pane, select and open the set of registry settings, select and open **Synchronization**, add the appropriate extension (if needed), select and open the appropriate extension, then select **Required**.

4. In the right pane, select **Server**, enter the server names or IP address, and click **OK**.

5. Export the settings to the Agent.

6. Select a method for initially distributing the global agent settings to client workstations:

   a. Customize the MSI package that installs the Logon Manager Agent to include these settings.

   b. Distribute a .REG file that you export from the Administrative Console. The .REG file can be merged with the client workstation's registry locally by double-clicking the file icon.

   > **Note:** The Console produces a .REG file compatible only with 32-bit systems. If you are merging the .REG file on a 64-bit system, you must run the following command to move the merged registry data to the correct location within the registry (otherwise, Universal Authentication Manager will not function):
   >
   > ```
   > reg.exe COPY HKLM\Software\Passlogix
   > HKLM\Software\Wow6432Node\Passlogix /s
   > ```

2.16.5 Configuring the Agent in a Citrix Environment

The Logon Manager default installation process automatically detects and installs the components necessary for Logon Manager in a Citrix environment. The installation process enables Logon Manager support for every application published on that Citrix server.

2.16.5.1 Installing Logon Manager on Citrix Server

To install Logon Manager on Citrix Server:

1. Log on to the Terminal server as an administrator and close all applications.

2. Click **Start** and then click **Run**.

3. In the **Run Dialog** window, enter cmd and press **Enter**.

4. In the **Command Prompt** window, enter change user/install and press **Enter**.

5. Install Logon Manager with the appropriate installation options for your environment.

6. At the command prompt, enter change user/execute when installation is complete.

2.16.5.2 Controlling Logon Manager for Specific Applications in Citrix

The following section explains how to change the default installation of Logon Manager and enable it for only specific applications in a Citrix environment. There are two steps in this process:

- Remove global Logon Manager support.

- Specify applications to be SSO-enabled through their published application configurations.

2.16.5.2.1 Removing Global Logon Manager Support To remove global Logon Manager support:

1. Click **Start** and then click **Run**.

2. In the **Run Dialog** window, enter Regedit and press **Enter**.

3. Go to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon.

4. From the right pane, right-click the string value **AppSetup** and select **Modify**.

5. Delete the value data in this entry that refers to SSOLauncher. (C:\Program Files\Passlogix\v-GO SSO\wts\ssolauncher.exe /nossoshutdown)

6. If you are using Windows Authentication v1, add the CheckForParentProcess key to the Passlogix registry hive. This ensures authentication event handoff to Logon Manager.

   HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix\AUI\WinAuth\

   DWORD:

   CheckForParentProcess

   Value=0

Removing ssolauncher.exe from AppSetup configures Logon Manager not to function with any applications on this Citrix server unless specified in your published applications configuration.

2.16.5.2.2 Specifying Which Applications Are SSO-Enabled Through the Published Application Configuration (SSOLauncher) Since Logon Manager support is now globally disabled, you must specify which applications you wish to be published with Logon Manager support by including the `SSOLauncher.exe` command in the published application properties.

1. Open Citrix Management Console.

2. Publish/Locate the application you would like to enable for Logon Manager.

3. Right-click on the published application and select **Properties**.

4. On the **Application Location** tab, add to the front of the Command Line the following syntax:

   ```
   C:\Program Files\Passlogix\v-GO SSO\wts\SSOLauncher.exe/application
   ```

The command for `SSOLauncher.exe` is added to your published application's command line; it does not replace it.

Following is an example of the Command Line syntax for the application ACT:

```
C:\Program Files\Passlogix\v-GO SSO\wts\SSOLauncher.exe" /application
C:\Program Files\ACT\act.exe
```

> **Note:** This example is based on the assumption that Logon Manager and ACT are both installed on the C:\ drive of the Citrix Server.

See SSOLauncher for Citrix Servers for more information.

2.16.5.2.3 Enabling Citrix Server Monitoring To enable Logon Manager to be monitored by Citrix Server, so that Logon Manager will not keep otherwise-ended sessions alive, go to the following registry tree:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\ Wfshell\TWI
```

If an entry named `LogoffCheckSysModules` exists, append to it the following items:

- `ssosehell.exe`
- `ssocredcap64.exe`
- `ssocredcap.exe`
- `ssobho.exe`
- `ssox64ho.exe`
- `ssowebho.exe`
- `ssomho.exe`
- `ssosapho.exe`
- `idcontext.exe`
- `ssoauth.exe`

For example, change:

```
app1.exe,app2.exe
```

to:

```
app1.exe,app2.exe,ssoshell.exe,ssocredcap64.exe
```

and so forth.

If the current `LogoffCheckSysModules` includes `ssomozho.exe`, remove this executable.

If the entry does not exist, create `LogoffCheckSysModules` as type `STRING` and set to include the executables above.

Also see the reference topic, Best Practices for Deploying the Agent in a Citrix Environment.

2.16.5.3 SSOLauncher for Citrix Servers

This utility lets you control the delivery Logon Manager with published applications in a Citrix Server environment.

To use the `ssolauncher` utility:

1. Copy the `ssolauncher` utility in the `WINNT\system32` folder. Otherwise you must include the full path to where ssolauncher resides.

2. You can now manage the applications you that you want Logon Manager to run by utilizing the ssolauncher utility. By accessing the Citrix Published Application Management console and applying the ssolauncher command through the Application Definition command line, you can make Logon Manager run on an application-by-application basis.

> **Note:** The `ssolauncher` command is applied in front of the command line. For example:
>
> ```
> ssolauncher.exe /application "C:Program Files\Internet
> Explorer\IEXPLORE.EXE"
> ```

The following are the commands for ssolauncher:

Command	Function
/application	The full path of the application to execute. This is required.
/command	Used to supply command parameters to an application. This is optional.
/directory	Used to supply working to an application. This is optional.
/wait	The number of milliseconds to wait for an application to shut down. This is optional. If not specified ssolauncher will wait forever for the application to terminate.
/verbose	This supplies dialogs for error message if ssolauncher has any failures.
/nossoshutdown	Prevents shutting down SSO when application completes.
/SSOCOMMAND LOGON	Used to initiate a command to the "Log On Using Logon Manager" trigger, located in the Logon Manager system tray icon.

For example, the following command line launches AIM:

```
ssolauncher.exe /verbose /application "C:\Program Files\AIM95\aim.exe"
/directory "C:\Program Files\AIM95"
```

> **Note:** The command should begin and end with quotation marks if it contains backslash (\) characters.

2.17 Configuring the Agent with Global Agent Settings

This section discusses the ways in which an administrator can configure the Agent's behavior. It begins with a discussion of the differences between using Global Agent Settings and administrative overrides: the best practices for the use of each, and which is preferable to use for different functions.

Following the best practice discussion is a complete list of Global Agent Settings, including all setting options, registry paths, and default values.

2.17.1 Global Agent Settings vs. Administrative Overrides

Logon Manager's behavior, including its interaction with the directory, is governed by settings configured and deployed to the end-user machine by the Logon Manager administrator using the Administrative Console. The settings fall into one of the following categories:

■   Global Agent settings are the "local policy" for the Agent; they are stored in the Windows registry on the end-user machine and are included in the Logon Manager `MSI` package to provide the Agent with an initial configuration during deployment.

Global Agent settings are stored in `HKEY_LOCAL_MACHINE\Software\Passlogix` (32-bit systems) or `HKEY_LOCAL_MACHINE\Wow6432Node\Software\Passlogix` (64-bit systems).

> **Note:**   Users able to modify the `HKLM` hive can alter their Global Agent Settings and thus change the behavior of the Agent from the one originally intended. To ensure that a setting will not be changed by the end-user, deploy it through an administrative override.

■   Administrative overrides take precedence over the Global Agent Settings stored in the Windows registry and constitute the "domain" policy for the Agent. Overrides are downloaded from the central repository by the Agent during synchronization and stored in the Agent's encrypted and tamper-proof local cache, which makes them immune to end-user alterations. When role/group security is enabled, administrative overrides can be applied on a per-user or per-group basis; they can also be applied enterprise-wide to enforce configuration consistency for all users.

> **Note:**   Be conservative when planning your administrative overrides. Fewer overrides mean less data to store and transfer, and thus more efficient synchronization with the central repository. Reducing the number of overrides also simplifies troubleshooting by eliminating unknowns, as administrative overrides cannot be viewed on the end-user machine.

Global Agent settings together with administrative overrides constitute the complete configuration policy for the Agent. The rest of this section describes the recommended optimal configuration.

Following is a typical view of the Administrative Console:
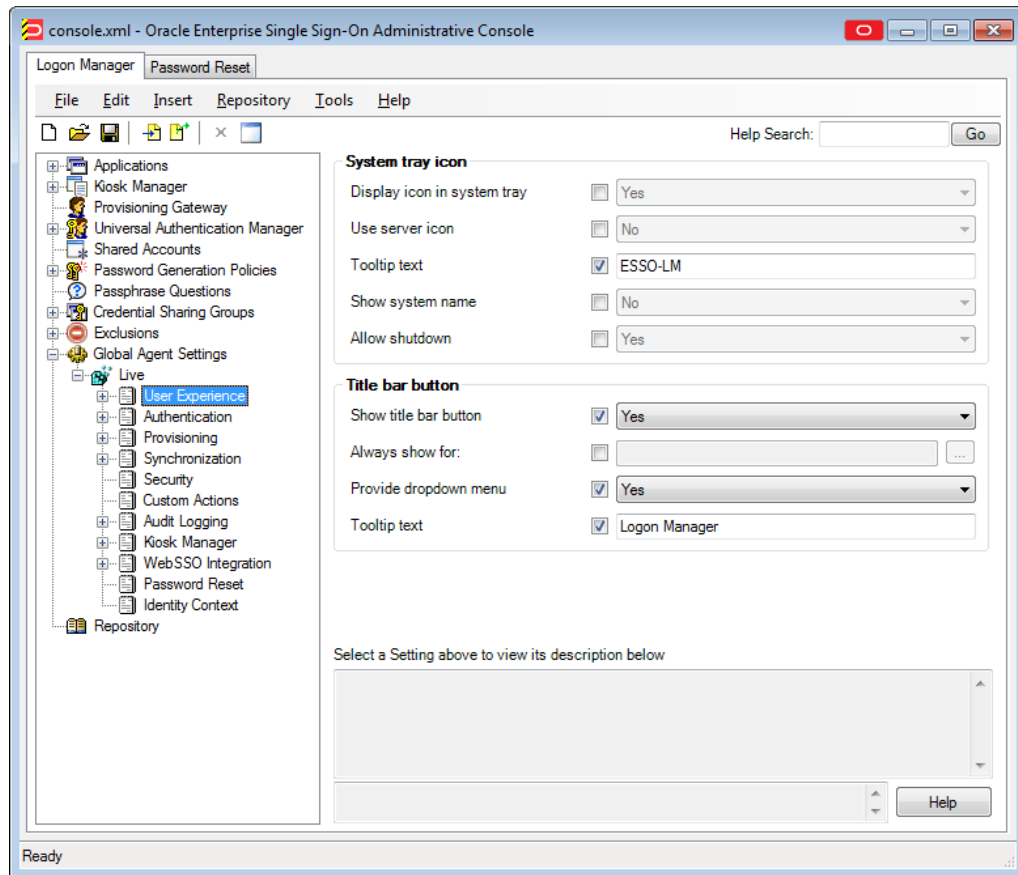
Note: In a development or staging environment, disable the option **Check for publisher's certificate revocation in Internet Explorer** to eliminate a delay when the Administrative Console launches and your machine is not connected to the Internet. (The delay is caused by Internet Explorer's attempting to look up the server's certificate and timing out when a certificate authority cannot be reached.) Do not disable this option on production machines.

A Note on Default Values

The best practice for settings not described in this and other Logon Manager guides is to leave them at their default values, unless your environment dictates otherwise. The default value is automatically in effect whenever the check box for the setting in the Administrative Console is left blank. The value is visible in the inactive field next to the check box.

2.17.1.1 Recommended Global Agent Settings

This section lists Oracle-recommended best-practice Global Agent Settings. Configure the settings as described below and include them in the customized Logon Manager `MSI` package.

2.17.1.1.1 Allow User to Exclude Accounts from Credential Sharing Groups Credential sharing groups allow you to share a single credential among a group of applications; the credential is managed at the group level, and the changes propagate instantly to all applications in the group. When an application is part of a credential sharing group

and the user has more than one set of credentials for the application, all but the shared credentials must be excluded from the group. This feature gives users the ability to exclude logons from assigned credential sharing groups.

Located in: Global Agent Settings > Live > User Experience > Password Change
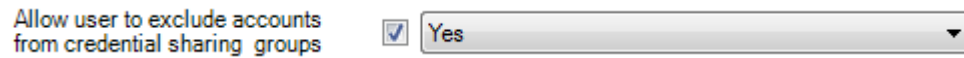
To enable: Select the check box, then select **Allow** from the drop-down list.

When this option is enabled, users can exclude a logon as follows:

1. In the "Logon Manager" window, select the logon you want to exclude from the assigned group.

2. Click **Properties**.

3. In the dialog that appears, select the **Exclude from password sharing group** check box.

4. Click **OK**.

5. Click **Refresh** to synchronize the changes with the central repository.

2.17.1.1.2   Restrict Disconnected Operation As a best practice, the Agent should run even if it cannot reach the central repository so that users can receive the benefits of single sign-on when not on the corporate network. Before working offline, the user must have done the following:

■   Completed the First Time Use (FTU) wizard while connected to the repository to generate encryption keys that protect the user's credentials. The keys are stored in the repository and in the Agent's local cache.

■   Synchronized with the repository at least once to obtain templates, policies, and any pre-provisioned credentials. These items are stored in the Agent's local cache for offline use.

If the user has successfully synchronized on one machine and completes the FTU on a secondary machine (such as a laptop) that has never been used with Logon Manager and is not connected to the repository, the keys generated on the secondary machine will not match the keys already stored in the repository. The secondary machine will not be able to synchronize with the repository due to this mismatch.

In order to avoid this problem and still allow users to work offline, do the following:

1. In your custom `MSI` package, configure the Agent not to run when disconnected from the repository, as shown below:

    Located in: Global Agent Settings > Live > Synchronization

    To set: Select the check box, then select **No** from the drop-down list.

2. After deployment, push an administrative override that lifts this restriction, as described in Allow the Agent to Run when Disconnected from the Repository. (The override will be in effect after first successful synchronization.)

2.17.1.1.3   Select the Primary Authenticator for End-Users Oracle highly recommends that you select and configure the primary authenticator in the following scenarios:

- If you want to disable the First-Time Use (FTU) wizard, as described in Do Not Show the First-Time Use Wizard.

- If you want users to authenticate only via the selected primary authenticator.

For information on configuring specific authenticators, see the Authentication section of the Global Agent Settings.

> **Note:** If this setting is left blank and the FTU wizard is disabled, the first installed logon method (in descending alphabetical order) is automatically selected by default. To view the list of installed authenticators, temporarily enable the setting and examine its drop-down list.

Located in: Global Agent Settings > Live > User Experience > Setup Wizard

| Selected authenticator | ☑ | Windows v2 ▼ |

To set: Select the check box, then select the desired logon method from the drop-down list.

2.17.1.1.4 Do Not Show the First-Time Use Wizard When Logon Manager starts for the first time, the FTU wizard appears and prompts the user to:

- Restore credentials and settings from a backup file (if a backup exists).

- Select the primary logon method.

- Authenticate to Logon Manager using the selected primary logon method.

- Provide credentials for default applications.

As a best practice, avoid burdening end-users with setting up Logon Manager manually. Instead, disable the FTU wizard, select the primary authenticator as described in the previous section, and provision the required applications beforehand; at that point, the only thing users will need to provide on the first launch of Logon Manager is their Windows password.

Located in: Global Agent Settings > Live > User Experience > Setup Wizard

| Show first-time-use (FTU) wizard | ☑ | No ▼ |

To disable: Select the check box, then select **No** from the drop-down list.
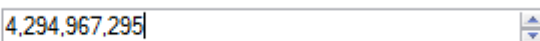
2.17.1.1.5 Disable the Reauthentication Timer Disable the reauthentication timer so that users are not interrupted by unexpected reauthentication prompts. (The user is prompted at the next secure operation that occurs after the timer expires.)

> **Note:** This is not an inactivity timer; this function is best served by the secure screensaver included in the operating system.

Located in: Global Agent Settings > Live > Security

| Reauthentication timer | ☑ | 4,294,967,295 |

To disable: Select the check box, then enter 4,294,967,295 in the field; this value disables the timer.

2.17.1.1.6   Use the Default Encryption Algorithm Do not change the default encryption algorithm (AES MS CAPI) that Logon Manager uses to encrypt application credentials to retain compatibility with all supported operating systems. Not all algorithms supported by Logon Manager function with all operating systems. (The operating systems supported by a given algorithm are listed next to the algorithm's name in the drop-down list.)

> **Note:**   Oracle strongly advises you to use MS CAPI algorithms to retain FIPS compliance across your enterprise.

Located in: Global Agent Settings > Live > Security

To set: Select the check box, then select the desired encryption method from the drop-down list.

Oracle recommends that you leave this setting at the default value shown above.

2.17.1.2 Recommended Administrative Overrides

This section lists recommended best-practice administrative overrides. Configure the overrides as described below and push them to the central repository. The overrides will be applied to end-user machines during the next synchronization event.

2.17.1.2.1   Configure Silent Credential Capture Logon Manager provides the ability to automatically (silently) capture credentials when a user logs into a supported application for the first time instead of displaying the interactive wizard. To simplify the user experience, Oracle recommends that you take advantage of this feature, but configure it so that users are aware that Logon Manager is capturing their credentials; fully silent capture (without user notification) may lead to trust issues (most users prefer to have a choice whether their credentials are captured or not) and increase incoming helpdesk calls as a direct result.

- For most applications, set the **Credential capture mode** option to **Capture and inform the user with balloon tip**.

- For applications that do not support silent credential capture (such as applications that require Logon Manager to use the SendKeys response method), set the **Credential capture mode** option to **Do not capture silently**.

Located in: Global Agent Settings > Live > Use Experience > Application Response > Initial Credential Capture

To set: Select the check box, then select the desired value from the drop-down list.

2.17.1.2.2   Make the Logon Manager Agent Wait for Synchronization on Startup To ensure that users always have the most recent credentials, application templates, password policies, and administrative overrides, configure the Agent to wait for synchronization

on startup. When this option is enabled, the Agent checks whether the directory is online when initializing and does one of the following:

- If the directory is online, the Agent does not respond to application logon requests until it successfully synchronizes with the directory.

- If the directory is offline, the Agent does not attempt to synchronize and starts immediately.

Located in: Global Agent Settings > Live > Synchronization

Use the default value shown above unless your environment requires otherwise.

2.17.1.2.3 Use Optimized Synchronization Optimized synchronization instructs the Logon Manager Agent to synchronize only credentials that have changed since the last synchronization. Do one of the following, depending on your environment:

- Enable this option to improve synchronization performance on deployments with more than five credentials per user.

- Disable this option to improve synchronization performance on deployments with fewer than five credentials per user and large number of downloaded templates per user.

Located in: Global Agent Settings >Live > Synchronization

Use the default value shown above unless your environment requires otherwise.

2.17.1.2.4 Allow the Agent to Run when Disconnected from the Repository This override is required to lift the restriction placed on the Agent in its initial configuration as described in Restrict Disconnected Operation. When this override is applied, users will benefit from single sign-on capability while not on the corporate network.

Located in: Global Agent Settings > Live > Synchronization

To allow: Select the check box, then select **Yes** from the drop-down list.

> **Note:**   This override must be applied in tandem with the restriction described in Restrict Disconnected Operation.

2.17.1.2.5 Set the Optimal URL Matching Precision for Web Applications URL matching precision determines how many levels within a URL are considered when matching the URL of an application to that defined in the template. If the URL matching precision is set too low, Logon Manager might mistake one intranet application for another and respond with incorrect credentials. If URL matching precision is set too high, an application served through a distributed infrastructure with unique host names may be erroneously recognized as separate applications due to the varying host name.

Follow these guidelines when determining the optimal URL matching precision for your environment:

- Typically, set URL matching precision to 5 (the maximum value). This will ensure that Logon Manager only responds when the URL of the application requesting logon exactly matches the URL stored in the template. The auto-recognize feature will have limited functionality.

- If you want to get the maximum benefit from the Logon Manager auto-recognize feature for Web applications, leave URL matching precision at its default value of 2. However, response to intranet applications might be impaired.

Located in: Global Agent Settings > Live > User Experience >Application Response > Web Applications

URL matching precision	☑	5	▲▼

To set: Select the check box, then enter the desired value in the field.

2.17.1.2.6 Limit Users to Predefined Applications Logon Manager allows you to prevent users from storing credentials for applications for which templates do not exist in the repository. To simplify the user experience while maintaining a degree of flexibility, Oracle recommends that you do the following, based on the type of application:

- **Windows applications.** Determine and provision the required applications before users begin working with Logon Manager. Instruct Logon Manager to store credentials only for applications for which templates already exist in the repository. Since users will not be prompted to store credentials for unprovisioned Windows applications, you retain full control of the single sign-on process for your enterprise applications.

   Located in: Global Agent Settings > Live > User Experience > Application Response >Initial Credential Capture

Windows applications	☑	Predefined applications only ▼

   To set: Select the check box, then select **Predefined applications only** from the drop-down list.

- **Web applications.** To provide the maximum value of single sign-on, you should allow users to store credentials for Web applications of their choice (by using this option's default value of Unlimited). Note, however, that users will be prompted to store credentials for each unprovisioned Web application every time they access it, until credentials are successfully stored. For this reason, Oracle recommends that you set this option to **Predefined applications only** rather than **Unlimited**. In the end, your decision will depend on the needs of your organization.

   Located in: Global Agent Settings > Live > User Experience > Application Response > Initial Credential Capture

Web applications	☑	Predefined applications only ▼

   To set: Select the check box, then select **Unlimited** from the drop-down list.

> **Note:** The individual options shown above take precedence over the All applications option.

2.17.1.2.7   Create and Set the Company Password Change Policy By default, Logon Manager ships with an inadequate default password change policy that must be replaced with a new policy which meets the security requirements of your organization. Include the name of your organization in the policy name to indicate that it is not a built-in policy. You must create this policy before setting this option; for instructions on creating a password change policy, see Adding a Password Policy.

Located in: Global Agent Settings > Live > User Experience > Password Change

To set: Select the check box, then select the desired policy from the drop-down list.

> **Note:**   The policy set as the default password change policy is in effect enterprise-wide.

2.17.1.2.8   Force Reauthentication when Revealing Masked Fields To prevent unauthorized access to stored application passwords, configure Logon Manager to prompt the user to authenticate when the "reveal masked fields" feature is invoked within the Agent. Configuring this policy as an administrative override will also prevent a rogue administrator from manually adding the setting to the local machine's registry and gaining unauthorized access to the local user's passwords if the setting is left unconfigured during initial deployment.

Located in: Global Agent Settings > Security

To set: Select the check box, then select **Yes** from the drop-down list.

2.17.1.2.9   Select an Audit Logging Method Configure and use audit logging to make troubleshooting your installation efficient. The audit method you choose will depend on the needs of your organization; a quick summary of the available methods is provided below.

- Syslog and Windows Event Logging Server are the methods of choice for most organizations.

- Databases are also supported (a valid ODBC connection string to the database is required).

- If you want to implement a custom event logging system, Logon Manager offers the "XML File" option which exposes raw log data that can be directly parsed by an external application. (Be aware that the raw log data are not self-cleaning and will grow indefinitely unless cleaned up externally.)

For more information on the available audit methods, see Audit Logging Settings.

2.17.1.2.10   Select Event Types to Log If you are using an audit logging method other than the Reporting Server, you must select the types of events that should be logged. Oracle highly recommends logging all event types for maximum benefit during troubleshooting.

> **Note:** You must select the **Event Types: Info** item in addition to the desired event types. This item is the parent to all event types and is required for data capture.

Located in: Global Agent Settings > Audit Logging > Selected Audit Logging Method>

Events to log ☑ [   ] [...]

To set: Select the check box, then select the desired event types in the dialog that appears. When you are finished, click **OK** to dismiss the dialog.

2.17.2 Working with a Set of Global Agent Settings

Global Agent Settings contain defaults, switches, and other configuration information that modify the behavior of Logon Manager on the desktop. Double-click items in the list in the right pane to view or modify the individual settings. Click **Add Notes** to enter notes about this set of settings.

To view a set of Global Agent Settings:

1. Do one of the following:

   - Click **Global Agent Settings** in the left pane, then double-click a set of settings from the right pane.

     or

   - In the left pane, click the plus sign (**+**) next to the Global Agent Settings icon (or double-click **Global Agent Settings**) to display the sets of settings.

2. Do one of the following:

   - Select a **Global Agent Settings** icon. The list of individual settings appears in the right pane.

     or

   - Right-click a **Global Agent Settings** icon to display a shortcut menu with these options:

Control	Function
Export	Save the selected set of settings to a registry file or administrative override object.
Write to Live HKLM	Export the current Agent configuration to the local-machine registry (HKLM).
Test	Launch the Logon Manager Configuration Test Manager, which tests your connections and adjusts settings, if necessary.
Manage Synchronizers	Add, delete, and reprioritize synchronizers.
Delete	Delete the selected set of settings.
Make copy	Duplicate the selected set of settings.
Rename	Rename the selected set of settings.
Publish	Opens the **Publish to Repository** dialog, from which you can select the Global Agent Settings and other objects you want to publish.

Control	Function
Publish To	Allows you to select a location to which to publish the selected set of Global Agent Settings.

2.17.2.1 Creating and Importing Global Agent Settings

The Global Agent Settings contain Agent configuration information and provide access to stored sets of Global Agent Settings. To create or import a set of Global Agent Settings:

1. Click **Global Agent Settings** in the left pane to display a list of sets of Global Agent Settings in the right pane.

2. Right-click **Global Agent Settings** in the left pane to display a shortcut menu with these options:

Control	Function		
New Settings	Create a new set of Global Agent Settings. Displays the **Settings** dialog.		
Import	Import a set of Global Agent Settings from an external source:		
		From File	Import a set of settings from an administrative override object (INI) file or a registration-entries (REG) file. Navigate to the file and click **Open**.
		From Live HKLM	Import the current Agent configuration from the local-machine registry (HKLM) as a set of settings named **Live**.
Publish	Opens the **Publish to Repository** dialog, from which you can select the Global Agent Settings and other objects you want to publish.		

> **Note:** If the imported settings have the same name as an existing set in the current configuration, the imported set is named "Copy of" existing settings.
>
> If this version of the Administrative Console is installed on a foreign operating system (any operating system other than English), do not use the **New Settings** option. Rather, use the **Import** option. If you use the New Settings option, the path for the synchronization extension points to an invalid location, which results in a synchronization failure.

2.17.2.2 Adding a Set of Global Agent Settings

Use this dialog to add and name a new set of Global Agent Settings.

■ Enter the Set of Settings Name and click **OK**.

To display this dialog:

■ Right-click **Global Agent Settings** and choose **New Settings** from the shortcut menu.

or

■ Choose **Global Agent Settings** from the **Insert** menu.

2.17.2.3 Exporting a Set of Global Agent Settings

To export a set of Global Agent Settings:

1. (Optional) Select **Unicode format** for the `.REG` file, if desired. See Export Format for options for this menu.

2. Click an option.

3. In the **File Save** dialog, locate and open the folder for each file, name the file, and click **Save**.

To display this dialog:

- Right-click the **Global Agent Settings** icon in the left pane and select **Export** from the shortcut menu.

2.17.2.4 Export Format

Use this dialog to select an output format for the selected set of settings.

Control	Function
Administrative Override Object	Export the settings as an administrative override object (`INI`) file.
HKLM Registry	Export the settings as a registration-entries (`REG`) file.
Both	Export both file types.
Unicode encoding (`.REG` format only)	Export the `.REG` file in Unicode format.

> **Note:** The Console produces a `.REG` file compatible only with 32-bit systems. If you are merging the `.REG` file on a 64-bit system, you must run the following command to move the merged registry data to the correct location within the registry (otherwise, Universal Authentication Manager will not function):
>
> ```
> reg.exe COPY HKLM\Software\Passlogix
> HKLM\Software\Wow6432Node\Passlogix /s
> ```

2.17.3 Global Agent Settings in Depth

This section provides detailed information about each Global Agent Setting. The settings are listed in the order in which they appear in the Administrative Console. Each listing includes the setting's registry path, description, setting options (if applicable), default (if applicable), whether the setting is overrideable, and the registry and data types.

2.17.3.1 User Experience

The User Experience settings control the Agent as a Windows application, including its interactions with the end user and with other programs.

2.17.3.1.1 System tray icon

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Display icon in system tray `Shell:ShowTrayIcon`	Specifies whether to show the Logon Manager icon in the system tray.	0: No 1: Yes (Default)	Yes	dword/Ø
Use server icon `Shell:TrayIcon UseRemote`	Specifies whether to use the alternative server icon, as opposed to the standard system tray icon.	0: No (Default) 1: Yes	Yes	dword/Ø

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Tooltip text `Shell:TrayIconName`	Specifies the text to display when the mouse hovers over the system tray icon. (Recommended use: Label each Citrix Server/Terminal Services/Remote server)	63 characters maximum (Default: Oracle Enterprise Single Sign-On Logon Manager)	Yes	string/Ø
Show system name `Shell:TrayIcon DisplaySysName`	Specifies whether to append the computer name to the tooltip text, separated by a space-dash-space.	0: No (Default) 1: Yes	Yes	dword/Ø
Allow shutdown `Shell:Allow Shutdown`	Specifies whether the "Shut Down" option is enabled on the system tray icon menu for the end user.	0: No 1: Yes (Default)	Yes	dword/Ø
Pause behavior `Shell:PauseBehavior`	Specifies the behavior of the Pause option in the context menu of the Logon Manager tray icon.	0: Pause indefinitely (Default) 1: Do not allow pause 2: Self un-pause after pause timeout	Yes	dword/Ø
Pause timeout `Shell:PauseTimeout`	Specifies the length of time the pause will last, in milliseconds when Pause behavior is set to Self un-pause after a pause timeout; has no effect otherwise.	Minimum: 0ms Maximum: 1800000ms Default: 60000ms	Yes	dword/int

2.17.3.1.2   Title bar button

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Show title bar button `Shell:ShowAccessBtn`	Specifies whether to show the Logon Manager button on all window title bars. This button can be configured for single-click application recognition and response, or it can provide a menu similar to the system tray menu, by changing the "Provide Dropdown Menu" setting.	0: No (Default) 1: Yes	Yes	dword/Ø
Always show for `Shell:ShowTitleIconAl waysForModuleN`	Identifies a list of applications (by executable filename, such as "notepad.exe") for which the title bar button should always be displayed. This setting overrides the "Show title bar button" setting. Click the ellipsis button ("...") button to enter the application names. Separate application names with a carriage return.		Yes	string/Ø
Provide dropdown menu `Shell:ShowAccessBtnMe nu`	Specifies whether to show the menu from the title bar button. If turned off, the title bar button acts as a single-click button for application recognition and response.	0: No (Default) 1: Yes	Yes	dword/Ø
Tooltip text `Shell:TitleIconName`	Specifies the text to display when the mouse hovers over the title bar button.	Default: Oracle Enterprise Single Sign-On Logon Manager	Yes	string/Ø

2.17.3.2 Application Response

The Application Response settings control the behavior of the Agent when the end user provides credentials for new logons and when detecting applications requiring logons.

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType DataType
Log on to waiting applications upon Agent startup `Shell:LogonOnStartup`	Enables the Agent, at startup, to submit credentials to a Windows or Java application that has already presented its logon form before the Agent was initialized and ready. **Note:** Web and host/mainframe application logons are not affected by this setting.	0: No (Default) 1: Yes	Yes	dword/(

SendKeys event interval
 	
`Extensions\`
`AccessManager:`
`SendkeysEventInterval`
	Specifies the minimum time to allow between SendKeys key events. This is especially useful for eastern languages where keystrokes are sometimes lost.
	
	Note: Logon Manager does not support credential submission using Journal Hook SendKeys.
		0: Best speed (Default)
		60: Typical for eastern languages
		80: Use for slow system
		120: Use for very slow system
			Yes	dword/(

Respond to hidden and minimized windows
 	
`Shell:StrictWindow`
`Detect`
	Specifies whether the Agent will respond to hidden and minimized windows.
	
	Note: This setting must be disabled when using Kiosk Manager.
		0: Yes (Default)
		1: No
			Yes	dword/(

Applications that hooks should ignore
 	
`Shell:HookIgnorePaths`
`Contain`
	Specifies applications that are incompatible with hooks, and which Logon Manager should therefore ignore. Click the ellipsis "**…**" button and enter the list of paths to exclude, separating items with semi-colons. This list can include full paths or sub-strings of paths.
	
	Example:
	
	To exclude all applications from all folders whose paths contain "C:\Program Files\Java," and all folders whose paths contain "Administrative Console," enter the following:
	
	`C:\Program Files\Java;Administrative`
	`Console.`
	
	Note: This setting is specifically for applications that might cause loss of functionality for compatibility reasons. Such applications might be discovered only in a production environment.
	
	Do not use this setting for applications that are compatible with Logon Manager functionality; for these applications, use the exclude/ignore settings on the appropriate application-type settings pages.
	
	You cannot use this setting as an administrative override.
			Yes	string/
				string

2.17.3.3 Initial Credential Capture

The Initial Credential Capture settings control the behavior of the Agent when it first encounters an application.

2.17.3.3.1 User interface

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Credential capture mode
 	
`Shell:CaptureType`
	Specifies how the Agent should respond when it encounters a new application requiring credentials, and the level of involvement on the user's part.
	
	Silent credential capture mode is not compatible with applications that require SendKeys. For this reason, you cannot use this mode for host/mainframe applications, nor for any Web or Windows application for which you use SendKeys.
	
	You should not use silent credential capture for applications where the username and password are obfuscated.
	
	Silent Credential Capture for on-the-fly Web applications requires a "Submit" element with one of the following tags:
	
	`<input type=submit>`
	
	`<button type=submit>`
	
	`<input type=image>`
	
	You must create a template for a Web application if the "Submit" element has an underlying tag of <img> or <a>.
		0: Do not capture silently. Presents the New Logon dialog in which the user enters credentials manually.
		
		1: Capture, but do not inform user. The Agent captures the credentials as the user enters them, and does not inform the user of the process.
		
		2: Capture, and inform user with balloon tip (Default) The Agent captures the credentials as the user enters them, and displays a balloon tip near the system tray to inform the user during the process.
		
		3: Capture, and present New Logon dialog. The Agent captures the credentials as the user enters them, and displays a balloon tip near the system tray to inform the user during the process. After capturing the credentials, the Agent displays the New Logon dialog with the user's entries pre-filled. The user can accept, change, cancel, or disable.
			Yes	dword/Ø

Enable Auto-Prompt `Shell:UseAutoSense`	Specifies whether to automatically prompt the user to add a logon when a new application is detected.	0: No 1: Yes (Default)	Yes	dword/Ø

Enable Auto-Enter
 	
`Extensions\`
`AccessManager:`
`LogonAfterConfig`
	Specifies whether to log on to an application after configuring it (adding its credentials).
	
	Note: The end-user can override this setting by deselecting it in the Logon Manager "Response" tab.
		0: No
		
		1: Yes (Default)
			Yes	dword/Ø

Enable Auto-Recognize `Shell:UseActiveLogin`	Specifies whether to automatically provide credentials to applications. **Note:** The application configuration-specific setting overrides the global setting.	0: No 1: Yes (Default)	Yes	dword/Ø

Allow creating multiple accounts during credential capture
 	
`Extensions\`
`AccessManager:`
`ShowAddAdditional`
`Logon`
	Specifies whether to enable the checkbox in the New Logon dialog that allows the user to add another set of credentials.	0: No (Default)
		
		1: Yes
			Yes	dword/Ø

Prohibit canceling the addition of new accounts
 	
`Extensions\`
`AccessManager:`
`EnableCancelButton`
	Specifies whether the user has the option to click the **Cancel** button or close the "New Logon" dialog to defer entering credentials. This permits current access to an application and re-prompts the user to enter credentials at the next appropriate instance.	0: Yes
		
		1: No (Default)
			Yes	dword/Ø

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Prohibit disabling the addition of new accounts Extensions\ AccessManager\ EnableNeverButton	Specifies whether the Disable button is available in the New Logon dialog, allowing the user to reject adding credentials for applications permanently. **Note:** Disabling an application adds it to the Exclusions list in Agent settings.	0: Yes 1: No (Default)	Yes	dword/Ø
Prohibit excluding accounts from credential sharing groups Extensions\ AccessManager: DisableAllowExclude PWSG	Specifies whether to disable the checkbox in the New Logon dialog that allows an account to be excluded from credential sharing groups. This checkbox will be available for the "Account Properties" dialog.	0: No (Default) 1: Yes	Yes	dword/Ø

2.17.3.3.2 Limit response to predefined applications for…

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
All application types Extensions\ AccessManager: AllowUnknown	Sets the following options: ■ Whether the Agent should auto respond to an application; ■ Whether the user should be allowed to create logons for applications that the Administrator has not predefined. The "Predefined applications only" setting prohibits both options. The 'Unlimited' setting permits both options.	0: Predefined applications only 1: Unlimited (Default)	Yes	dword/Ø
Windows applications Extensions\ AccessManager: AllowUnknownApp	Specifies whether the users is allowed to add credentials for Windows applications that are not predefined by the administrator.	0: Predefined applications only 1: Unlimited (Default)	Yes	dword/Ø
Web applications Extensions\ AccessManager: AllowUnknownWeb	Sets the following options: ■ Whether the Agent should respond to a Web application automatically. ■ Whether the user should be allowed to create logons for applications that the administrator has not predefined. The "Predefined applications only" setting prohibits both options. The "Unlimited" setting permits both options. The "Manually add undefined" setting prohibits the first option and permits the second option.	0: Predefined applications only 1: Unlimited (Default) 2: Manually add undefined	Yes	dword/Ø
Allowed Web pages Extensions\ AccessManager\ BHOAllowedWebPages: WebPageN	Use this setting to list the Web pages that the Agent should allow. Click the ellipsis "**…**" button to add the allowed Web pages and enter the regular expressions that match the URLs. (There is no default for this setting.) **Note:** Use this setting only when you select "All application types" or "Web applications" for "Predefined applications only."		Yes	string/Ø

2.17.3.4 Web Application Response

The Web Applications Response settings control the behavior of the Agent with Web applications.

Because some Web applications contain content that changes with each visit, you can configure a Web template to re-scan dynamic Web pages, detect changes, and respond appropriately.

2.17.3.4.1   Credential field identification

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Show border
 	
`Extensions\`
`AccessManager\`
`BHO:ShowBorder`
	Specifies whether to display a highlighted border around the credential fields of a Web form during logon.	0: No
		1: Yes (Default)
			Yes	dword/Ø

Border appearance
 	
`Extensions\`
`AccessManager\`
`BHO:FeedbackColor`
	Default border color/size/style for highlighting detected web page fields.
	
	See Border Values for Web Logon Credential Fields for more information.
		Default: red 6px solid	Yes	string/ string

2.17.3.4.2   Behavior

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

URL matching precision
 	
`Extensions\`
`AccessManager:`
`DNLevelsToMatch`
	Number of levels of the host portion of the URL used for application detection and response.
	
	For example, for the URL http://mail.company.co.uk:
	
	2=match to `*.co.uk`
	
	3=match to `*.company.co.uk`
	
	4=match to `*.mail.company.co.uk`
	
	Note: Values less than 2 are treated as 2.
		Minimum: 2 (Default)
		Maximum: 5
			Yes	dword/int

Scroll into view
 	
`Extensions\`
`AccessManager\`
`BHO:ScrollIntoView`
	Enables or disables scrolling the browser window to bring the logon fields into view.
	
	This setting disables scrolling when the user has not yet stored credentials for a Web application. The Agent always scrolls when injecting credentials into the logon fields for an account that already exists.
		0: No (Default)
		1: Yes
			Yes	dword/Ø

Activate tab
 	
`Extensions\`
`AccessManager\`
`BHO:ActivateTab`
	Enables or disables activating the tab that identifies the logon fields.	0: No
		1: Yes (Default)
			Yes	dword/Ø

Respond to IE modal dialogs
 	
`Extensions\`
`AccessManager\BHO:`
`RespondToIEModal`
`Dialogs`
	Enables Agent response to a Web page that displays as a modal dialog or HTML application.	0: No (Default)
		1: Yes
			Yes	dword/Ø

2.17.3.4.3   Response control

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Applications to ignore
 	
`Extensions\`
`AccessManager:`
`BHOIgnoredApps`
	Enter a comma-delimited list of applications (without path or extension) that the Browser Helper Object (BHO) should not attach to when searching for logons. Used when the BHO causes conflicts with certain applications.
	
	Example: `ws_ftp, customapp1`
			Yes	string/Ø

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Web pages to ignore Extensions\ AccessManager\ BHOIgnoredWebPages: WebPageN	Use this setting to list the Web pages that the Agent should ignore. Used when the BHO causes conflicts with specific web applications or sites. Click the ellipsis ("**…**") button to enter the regular expressions that match the URLs to be ignored (one per line). Examples: .*http://login\.company\.com/.* .*http://.*\.company\.com/.*		Yes	string/Ø
Allowed dynamic Web pages Extensions\ AccessManager\ BHOAllowed DynamicWebPages: DynamicWebPageN	Use this setting to list the dynamic (DHTML) Web pages allowed by the Agent. By default, the BHO does not detect changes made to a dynamic page after the initial presentation of the page. Click the ellipsis ("**…**") button to enter the regular expressions that match the URLs. Examples: .*http://logon\.company\.com/.* .*http://.*\.company\.com/.*		Yes	string/Ø

2.17.3.5 Windows Application Response

The Windows Applications Response setting controls the behavior of the Agent with Windows applications.

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Allow fallback from Control IDs to SendKeys Extensions\ AccessManager:Allow SendKeysFallback	Allows fallback to SendKeys when direct injection of credentials using Control IDs fails.	0: No 1: Yes (Default)	Yes	dword/Ø
Supported Window Classes for Applications Extensions\AccessMan ager:AppClasses	Specifies the list of window class names that the Agent recognizes as applications. This setting is provided to improve performance by restricting the Agent to this list. To enable support for dynamic window classes, delete the default settings to set this value to null.	#32770;Dialog;Thunder RT5 FormDC; ThunderRT6FormDC (Default)	Yes	string/ string
Ignored Window Classes for Applications Extensions\AccessMan ager:AppIgnoreClasse s	Specifies the list of window class names that the Agent does not recognize as applications. This setting allows you to direct the Agent to ignore a specific window class globally.	No default	Yes	string/ string

2.17.3.6 Java Application Response

The Java Application Response settings control the behavior of the Agent with Java applications.

2.17.3.6.1 Exclusions

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Excluded Java versions Extensions\ AccessManager\ JHO:JhoExclude JavaVersionN	Specifies Java versions to exclude, listed as regular expressions. Enter one expression per line.		No	string/Ø

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Excluded Java vendors Extensions\ AccessManager\ JHO:JhoExclude JavaVendorN	Specifies Java vendors to exclude, listed as regular expressions. Enter one expression per line. This setting is new as of Logon Manager version 11.1.1.5.0.		No	string/Ø

2.17.3.6.2 Response delays

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Time allowed for Java applets to load Extensions\ AccessManager: MaxAppletLoadTime	Specifies the maximum time (in seconds) that the Agent waits for a Java applet to be fully loaded in the browser.	(Default: 6)	Yes	dword/int
Delay after Java runtime startup Extensions\ AccessManager: JHOAttachDelay	Specifies the length of time (in milliseconds) the JHO should wait before listening to window events at Java startup. Adding a delay can resolve timing conflicts during Java runtime initialization.	(Default: 0)	Yes	dword/int
Delay between retries Extensions\ AccessManager: JhoRetryTimeout	Specifies the length of time (in milliseconds) the JHO should wait between retries of credential injection into a form control.	(Default: 500)	Yes	dword/int

2.17.3.6.3 Retry behavior

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Maximum times to retry credential injection Extensions\ AccessManager: JhoRetryMaxAttempts	Specifies the number of times to retry credential injection.	(Default: 0)	Yes	dword/ int

2.17.3.6.4 Java events to respond to

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Hierarchy events Extensions\ AccessManager: JhoHierarchy EventProcessing	Specifies which Java hierarchy events are recognized. Set the flag using the following syntax: HIERARCHY_EVENT_CHANGED = 0x1 This instructs the JHO to recognize all hierarchy events.	(Default: 0)	Yes	dword/int

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Window events `Extensions\ AccessManager: JhoWindow EventProcessing`	Specifies which Java window events are recognized.	A combination of the following values: ■ `WINDOW_EVENT_ OPENED = 0x1` ■ `WINDOW_EVENT_ CLOSED = 0x2` ■ `WINDOW_EVENT_ ACTIVATED = 0x4` ■ `WINDOW_EVENT_ DEACTIVATED = 0x8` ■ `WINDOW_EVENT_ CLOSING = 0x10` ■ `WINDOW_EVENT_ ICONIFIED = 0x20` ■ `WINDOW_EVENT_ DEICONIFIED = 0x40` (Default: 255-All window events are recognized.) The recommended setting for new installations of Logon Manager is 3.	Yes	dword/int
Component events `Extensions\ AccessManager: JhoComponent EventProcessing`	Specifies which Java component events are recognized.	A combination of the following values: ■ `COMPONENT_EVENT_ SHOWN = 0x1` ■ `COMPONENT_EVENT_ HIDDEN = 0x2` ■ `COMPONENT_EVENT_ ADDED = 0x4` ■ `COMPONENT_EVENT_ REMOVED = 0x8` (Default: 15-All component events are recognized.) The recommended setting for new installations of Logon Manager is 0xB (11).	Yes	dword/int

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Injection type
 	
`Extensions\`
`AccessManager:`
`JhoInjectType`
	Specifies the injection type that the JHO uses to submit data to the controls.	One of the following values:
		
		■ `INJECT_TYPE_`
		`DEFAULT = 0`
		`(Default)`
		
		The default causes the JHO to attempt injection using each of the following methods in the order shown until injection is successful:
		
		■ `INJECT_TYPE_`
		`METHOD = 1` (if an appropriate set method has been found for the control)
		
		■ `INJECT_TYPE_`
		`ACCESSIBLE = 2` (if the control supports accessibility)
		
		■ `INJECT_TYPE_`
		`NONACCESSIBLE =`
		`3`
		
		■ `INJECT_TYPE_`
		`ROBOT = 4`
		
		Note: For combo and list boxes, the JHO always uses `INJECT_`
		`TYPE_METHOD`.
			Yes	dword/int

2.17.3.7 Host/Mainframe Application Response

The Host/Mainframe Response settings control the behavior of the Agent with host/mainframe applications.

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

16-bit screen capture attempts
 	
`Extensions\`
`AccessManager\`
`MHO\ConXP:`
`16BitTimeouts_`
`ToFallback`
	Specifies the number of times to attempt the 16-bit screen capture. If an attempt is unsuccessful after the allotted number of tries, the Agent reverts to the 32-bit method.	(Default: 5)	Yes	dword/
				int

Credential request delay interval
 	
`Extensions\`
`AccessManager\`
`MHO:NotNowDelay`
	Specifies the interval (in milliseconds) between prompts to create a logon for a mainframe session.
	
	When a user logs on to a mainframe session that matches a configured application for which there is no stored password, the Agent prompts the user: "Would you like Logon Manager to remember your logon information for this application?"
	
	If the user selects **Not Now**, the next time the user presses any key on the mainframe screen, the Agent prompts the user again. This delay setting is the amount of time the Agent should wait before displaying the question again.
		(Default: 60000)	Yes	dword/int

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Polling interval
 	
`Extensions\`
`AccessManager\`
`MHO:CycleInterval`
	Specifies the interval (in milliseconds) between instances when the Agent checks the host emulator for changes. Lower values can use more CPU time; higher values can increase the time between when a screen appears and when the Agent provides credentials.	(Default: 700)	Yes	dword/int

2.17.3.8 Password Change

The Password Change settings control the Agent behavior and policies for password generation and credential maintenance.

2.17.3.8.1 Password change behavior

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Default password policy
 	
`Extensions\`
`AccessManager:`
`DefaultPolicy`
	Name of the Password Generation Policy that application templates will use when no policy is defined in the application template. To define this setting, ensure that you currently have a defined/named policy loaded in the console, so the dropdown allows you to select the policy.
	
	Note: If no policy is defined here or in the template, a default policy of exactly eight alpha-only characters applies. For this reason, it is important to define a more appropriate policy.
			Yes	string/Ø

Allow user to exclude accounts from credential sharing groups
 	
`Extensions\`
`AccessManager:`
`AllowExcludePWSG`
	Allows end user to exclude application logons from an assigned credential sharing group.
	
	Enabling this option causes a check box to appear on the **New Logon** and **Properties** dialogs, giving the user the choice to omit accounts from credential sharing groups.
		0: No (Default)
		1: Yes
			Yes	dword/Ø

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Change passwords automatically `Extensions\AccessMana ger: QuietGenerator`	Specifies the level of control given to the user in the password change process.	▪ No. (Default) The user has full control; Logon Manager does not automatically change passwords. The user must initiate password change. (default) ▪ Yes, with user confirmation. The user has partial control; Logon Manager automatically initiates password change and prompts the user to either accept the auto-generated password, request to generate another, or enter one manually. ▪ Yes, without user confirmation. The user has no control; Logon Manager automatically initiates password change, generates a password, and submits it to the application without permitting user interaction.	Yes	dword/Ø

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Manual password change behavior
 	
`Extensions\`
`AccessManager:CPWFlag`
	Specifies the behavior of the Password Change Wizard when a user encounters a password-change request.	■ Prompt. (Default) Prompts user with the Password Change Wizard.
		
		■ Manual, offer auto. Prompts user to select a new password, but also allows the Password Change Wizard to offer to generate the password automatically.
		
		■ Auto, offer manual. Generates the new password automatically, but also allows the user to select the new password.
		
		■ Manual only. Prompts user to select a new password; does not allow Password Change Wizard to automatically generate the password.
			Yes	dword/Ø

Pop-up dialog text after submission
 	
`Extensions\`
`AccessManager:`
`CPVerifyMessage`
	To change the default text, select the checkbox and highlight the current text, then type in new text. To restore default text, unselect the checkbox.	Default: After closing this message, verify that the application accepted the password. Select OK if it was accepted. If it was rejected, please try again.	Yes	string/Ø

2.17.3.8.2 Allowed character sets

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Lowercase characters
 	
`Extensions\`
`AccessManager:`
`LowerAlphaChars`
	Specifies the list of lowercase alphabet characters to allow in passwords.	Any lowercase characters
		
		(Default: All lowercase characters)
			Yes	string/Ø

Uppercase characters
 	
`Extensions\`
`AccessManager:`
`UpperAlphaChars`
	Specifies the list of uppercase alphabet characters to allow in passwords.	Any uppercase characters
		
		(Default: All uppercase characters)
			Yes	string/Ø

Numeric characters
 	
`Extensions\`
`AccessManager:`
`NumericChars`
	Specifies the list of numeric characters to allow in passwords.	Any numeric characters
		
		(Default: All numeric characters)
			Yes	string/Ø

Special characters
 	
`Extensions\`
`AccessManager:`
`SpecialChars`
	Specifies the list of non-alphanumeric (special) characters to allow in passwords	!@#$%^&*()_-+=[]|,?
		(Default)
			Yes	string/Ø

2.17.3.9 User Interface

The User Interface settings control the appearance of the Agent when performing a logon and of the information presented in the Logon Manager and "Logon Chooser" dialog.

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Language `[Root]:Language`	Specifies the language in which to present the user interface. **Note:** Other values may be acceptable based on localized versions. The display font should support the desired characters in the specified language.	English (Default) Chinese (Simplified) Chinese (Traditional) Czech Danish Dutch Finnish French German Greek Hungarian Italian Japanese Korean Norwegian Polish Portuguese (Brazil) Portuguese (Portugal) Romanian Russian Slovak Spanish Swedish Thai Turkish	Yes	string/Ø
Allow refresh in My Accounts `Extensions\ AccessManager: AllowRefresh`	Enables/disables the SSO Manager Refresh button.	0: No 1: Yes (Default)	Yes	dword/Ø
Columns in "Details" view of My Accounts `Extensions\ AccessManager\ LogonManager:Columns`	Click the ellipsis "…" button to display the **Edit Columns** dialog. Choose the appearance and order of columns in the Logon Manager.	1: Application Name 2: URL/Module 3: Username/ID 4: Password 5: Modified 6: Last Used 7: Description 8: Reference 9: Group 10: Third Field 11: Fourth Field (Default: 1,2,3,4,5,6,7,8,9)	Yes	string/Ø

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Columns in Logon Chooser `Extensions\ AccessManager\ LogonChooser:Columns`	Click the ellipsis "**…**" button to display the Edit Columns dialog. Choose the appearance and order of columns in the Agent's "Logon Chooser" dialog.	1: Username/ID 2: Application Name 3: Description (Default: 1,2,3)	Yes	string/Ø
Logon animation's duration `Shell:AutoLogon AnimationTime`	Specifies the duration (in milliseconds) that the animated spinner appears (pausing response). A value of 0 (the default) disables the spinner.	(Default: 0)	Yes	dword/int

2.17.3.9.1 Edit Columns Use the **Edit Columns** dialog to select and order the logon details that appear as columns in the Agent's **Logon Manager** and **Logon Chooser** dialogs.

- To add detail columns, select the columns in the **Available** list, then click **>>** to move your selections to the **Selected** list.

- To remove detail columns, select the columns in the **Selected** list, then click **<<** to move your selections to the **Available** list.

- To change the order of the columns, select a column in the **Available** list and click **Up** or **Down**.

2.17.3.10 Setup Wizard

The Setup Wizard settings control the behavior of the First-Time-Use Wizard, which launches when you start Logon Manager for the first time. See First-Time-Use Scenarios for more information.

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Show first-time-use (FTU) wizard `Extensions\ SetUpManager: HideWizard`	Controls whether the Setup Wizard displays when first-time-use is invoked. **Note:** If more than one authenticator (primary logon method) is installed, then the first authenticator in the list is automatically selected as the end user's primary logon method. You must have the FTU Wizard enabled in order to use the Bulk-Add feature.	0: Yes (Default) 1: No	Yes	dword/Ø

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Selected authenticator `AUI:FTUShowOnly`	Enables the selected logon method as the primary logon method and hides all other installed logon methods. **Note:** To hide the primary logon method selection menu, use the "Show first-time-use (FTU) wizard" setting. If the primary logon method selection page is hidden, and this setting is blank, then the first installed logon method in the list is automatically selected.	None (Default: End-users select their own primary logon method) MSauth: Windows v2 WinAuth: Windows LDAPauth: LDAP v2 LDAP: LDAP SCauth: Smart Card ROSCAuth: Read-Only Smart Card ProxcardAuth: Proximity Card SecureIDAuth: RSA SecurID Entrust: Entrust MultiAuth: Authentication Manager UAMAuth: Universal Authentication Manager	Yes	string/Ø
Skip selection page if only one authenticator is installed `AUI:HideSingle Selection`	Hides the Select Primary Logon Method step in the Setup Wizard if only one authenticator (primary logon method) is installed.	0: No (Default) 1: Yes	Yes	dword/Ø

2.17.3.11 Authentication

Use the Global Agent Authentication Settings to configure the overall authentication environment and individual authenticator settings. Select a topic below to learn more about authentication options.

- **Authentication Manager.** This pane and its sub-panes contain settings that apply to your overall authentication configuration.

  - Enrollment

  - Grade

  - Order

- **Authenticator Panes.** Each pane contains settings applicable to a specific authenticator.

  - Windows v2

  - Windows v2 Passphrase

  - Windows (deprecated)

  - LDAP v2

  - LDAP v2 Special Purpose

  - LDAP

  - LDAP Special Purpose

  - Smart Card

  - Read-Only Smart Card

     –   Proximity Card

■ **Secure Data Storage.** Refer to this section for information about configuring storage for use with strong authenticators.

■ **Strong Authentication.** Refer to this section for information about advanced configuration of strong authenticators, such as cards and tokens.

2.17.3.12 Authentication Manager

The Authentication Manager setting controls the number of authenticators and their priority.

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Allowed number of authenticators `AUI\MultiAuth: MaxPreferred`	Specifies the maximum number of logon methods that the Agent offers the user to select. If the user receives and skips this number of logon methods, a "Choose Logon" dialog appears. **Note:** This setting is only used for the Multi-Authenticator primary logons.	(Default: 1)	Yes	dword/int

2.17.3.12.1 Enrollment Settings The Authentication Manager Enrollment settings specify the primary logon methods (authenticators) that can be used by the Multi-Authenticator primary logon.

The settings on this page will determine whether a user will be required to set up a specific logon method during the First Time Use Wizard, if Authentication Manager is chosen as the primary logon method. Use these settings for Multi-Authenticators only.

For each primary logon method, select one of the following:

■ **Disabled.** The logon method will not be presented to the user during the FTU Wizard.

■ **Optional.** Logon Manager will have the option to configure this logon or to skip it. If the user defers the logon request, Logon Manager will not ask again. (Default)

■ **Required.** The user will be required to configure this logon. If this logon is not configured, the user will not be able to complete enrollment.

■ **Incremental.** Logon Manager will have the option to configure this logon or to skip it. If the user defers the logon request, Logon Manager will ask for credentials each time the application starts.

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Windows v2 `AUI\MSauth:AuthState`	Specifies whether a user will be required to set up Windows v2 as a primary logon method during the First Time Use Wizard, if Authentication Manager is chosen as the primary logon method.	0: Disabled 1: Optional (Default) 2: Required 3: Incremental	Yes	dword/Ø
Windows `AUI\WinAuth:AuthState`	Specifies whether a user will be required to set up Windows as a primary logon method during the First Time Use Wizard, if Authentication Manager is chosen as the primary logon method. **Note:** Windows Authenticator is deprecated as of version 11.1.2 and is listed for upgrade scenarios only. Do not use this authenticator for new configurations.	0: Disabled 1: Optional (Default) 2: Required 3: Incremental	Yes	dword/Ø

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
LDAP v2 AUI\LDAPauth: AuthState	Specifies whether a user will be required to set up LDAP v2 as a primary logon method during the First Time Use Wizard, if Authentication Manager is chosen as the primary logon method.	0: Disabled 1: Optional (Default) 2: Required 3: Incremental	Yes	dword/Ø
LDAP AUI\LDAP:AuthState	Specifies whether a user will be required to set up LDAP as a primary logon method during the First Time Use Wizard, if Authentication Manager is chosen as the primary logon method.	0: Disabled 1: Optional (Default) 2: Required 3: Incremental	Yes	dword/Ø
Smart card AUI\SCauth:AuthState	Specifies whether a user will be required to set up smart card as a primary logon method during the First Time Use Wizard, if Authentication Manager is chosen as the primary logon method.	0: Disabled 1: Optional (Default) 2: Required 3: Incremental	Yes	dword/Ø
Read-only smart card AUI\ROSCauth: AuthState	This setting determines whether a user will be required to set up read-only smart card as a primary logon method during the First Time Use Wizard, if Authentication Manager is chosen as the primary logon method.	0: Disabled 1: Optional (Default) 2: Required 3: Incremental	Yes	dword/Ø
Proximity card AUI\ProxCardAuth: AuthState	Specifies whether a user will be required to set up proximity card as a primary logon method during the First Time Use Wizard, if Authentication Manager is chosen as the primary logon method.	0: Disabled 1: Optional (Default) 2: Required 3: Incremental	Yes	dword/Ø
RSA SecurID AUI\SecureIDAuth: AuthState	Specifies whether a user will be required to set up RSA SecurID as a primary logon method during the First Time Use Wizard, if Authentication Manager is chosen as the primary logon method.	0: Disabled 1: Optional (Default) 2: Required 3: Incremental	Yes	dword/Ø
Entrust AUI\Entrust:AuthState	Specifies whether a user will be required to set up Entrust as a primary logon method during the First Time Use Wizard, if Authentication Manager is chosen as the primary logon method.	0: Disabled 1: Optional (Default) 2: Required 3: Incremental	Yes	dword/Ø
Universal Authentication Manager AUI\UAMAuth:AuthState	Determines whether a user will be required to set up Universal Authentication Manager as a primary logon method during the First Time Use Wizard, if Authentication Manager is chosen as the primary logon method. This setting is only used for Multi-Authenticator primary logons.	0: Disabled 1: Optional (Default) 2: Required 3: Incremental	Yes	dword/Ø
ESSO-UAM: Windows Password AUI\UAMAuth-{0C29417D -8A20-48B7-8CC4-D948D 384E9B2}:AuthState	Determines whether a user will be required to set up Universal Authentication Manager: Windows Password as a primary logon method during the First Time Use Wizard, if Authentication Manager is chosen as the primary logon method. This setting is only used for Multi-Authenticator primary logons.	0: Disabled 1: Optional (Default) 2: Required 3: Incremental	Yes	dword/Ø
ESSO-UAM: Fingerprint AUI\UAMAuth-{16627EE1 -FAE3-43B5-B884-D3661 649B97D}:AuthState	Determines whether a user will be required to set up Universal Authentication Manager: Fingerprint as a primary logon method during the First Time Use Wizard, if Authentication Manager is chosen as the primary logon method. This setting is only used for Multi-Authenticator primary logons	0: Disabled 1: Optional (Default) 2: Required 3: Incremental	Yes	dword/Ø

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
ESSO-UAM: Smart Card `AUI\UAMAuth-{A1B34553 -8D40-42A9-8ED5-F70E3 497E138}:AuthState`	Determines whether a user will be required to set up Universal Authentication Manager: Smart Card as a primary logon method during the First Time Use Wizard, if Authentication Manager is chosen as the primary logon method. This setting is only used for Multi-Authenticator primary logons.	0: Disabled 1: Optional (Default) 2: Required 3: Incremental	Yes	dword/Ø
ESSO-UAM: Proximity Card `AUI\UAMAuth-{4A8F93E4 -2328-44CA-8DBE-FBFA4 E5FD334}:AuthState`	Determines whether a user will be required to set up Universal Authentication Manager: Proximity Card as a primary logon method during the First Time Use Wizard, if Authentication Manager is chosen as the primary logon method. This setting is only used for Multi-Authenticator primary logons.	0: Disabled 1: Optional (Default) 2: Required 3: Incremental	Yes	dword/Ø
ESSO-UAM: Challenge Questions `AUI\UAMAuth-{393D4B53 -EC46-4A38-9E9E-3D6B5 141DD34}:AuthState`	Determines whether a user will be required to set up Universal Authentication Manager: Challenge Questions as a primary logon method during the First Time Use Wizard, if Authentication Manager is chosen as the primary logon method. This setting is only used for Multi-Authenticator primary logons.	0: Disabled 1: Optional (Default) 2: Required 3: Incremental	Yes	dword/Ø

2.17.3.12.2 Grade Settings The Authentication Manager Grade settings specify an authentication grade for each primary logon method.

Authentication Grades are numeric values:

- An authentication grade automatically defaults to grade level 1 if authentication grading is turned on and no grade level is specified.

- The higher the grade level specified, the stronger the authentication level that is being requested.

- The grading scale can be arbitrarily configured. For example, an expected normal scenario would be a scale of 1-3, but you have the flexibility to make this 1-5 or 1-n, as required. Any grade less than 1 will be converted to 1.

The Multi-Authenticator logon supports the authentication grades by mapping the grades to the authentication methods used, if you choose Authentication Manager as the primary logon method.

If a user tries to access credentials with a grade level that is too low, he will be asked to authenticate at a higher grade and only gain access if successful.

Lockouts occur as per normal Logon Manager authentication lockout policy. Since graded authentication uses the core SSO authentication process, this will happen naturally.

Set a number grade value (≥1) for each logon method. Use these settings for Multi-Authenticators only.

Display Name/ Registry Path	Description Text	Options/Default	Overridable	RegType/ DataType
Windows v2 `AUI\MSauth:AuthGrade`	Assigns an authentication grade to Windows v2. Set a number grade value (≥1). The higher the grade level specified, the stronger the authentication level that is being requested.	(Default: 1)	Yes	dword/Ø

Display Name/ Registry Path	Description Text	Options/Default	Overridable	RegType/ DataType
Windows AUI\WinAuth:AuthGrade	Assigns an authentication grade to Windows. Set a number grade value (≥1). **Note:** Windows Authenticator is deprecated as of version 11.1.2 and is listed for upgrade scenarios only. Do not use this authenticator for new configurations.	(Default: 1)	Yes	dword/Ø
LDAP v2 AUI\LDAPauth: AuthGrade	Assigns an authentication grade to LDAP v2. Set a number grade value (≥1).	(Default: 1)	Yes	dword/Ø
LDAP AUI\LDAP:AuthGrade	Assigns an authentication grade to LDAP. Set a number grade value (≥1).	(Default: 1)	Yes	dword/Ø
Smart card AUI\SCauth:AuthGrade	Assigns an authentication grade to Smart card. Set a number grade value (≥1).	(Default: 1)	Yes	dword/Ø
Read-only smart card AUI\ROSCauth: AuthGrade	Assigns an authentication grade to read-only smart card. Set a number grade value (≥1).	(Default: 1)	Yes	dword/Ø
Proximity card AUI\ProxCardAuth: AuthGrade	Assigns an authentication grade to Proximity card. Set a number grade value (≥1).	(Default: 1)	Yes	dword/Ø
RSA SecurID AUI\SecureIDAuth: AuthGrade	Assigns an authentication grade to RSA SecurID. Set a number grade value (≥1).	(Default: 1)	Yes	dword/Ø
Entrust AUI\Entrust:AuthGrade	Assigns an authentication grade to Entrust. Set a number grade value (≥1).	(Default: 1)	Yes	dword/Ø
Universal Authentication Manager AUI\UAMAuth:AuthGrade	Assigns an authentication grade to Universal Authentication Manager. Set a number grade value (>=1). This setting is only used for Multi-Authenticator primary logons.	(Default: 1)	Yes	dword/Ø
ESSO-UAM: Windows Password AUI\UAMAuth-{0C29417D-8A20-48B7-8CC4-D948D384E9B2}:AuthGrade	Assigns an authentication grade to Universal Authentication Manager: Windows Password. Set a number grade value (>=1). This setting is only used for Multi-Authenticator primary logons.	(Default: 1)	Yes	dword/Ø
ESSO-UAM: Fingerprint AUI\UAMAuth-{16627EE1-FAE3-43B5-B884-D3661649B97D}:AuthGrade	Assigns an authentication grade to Universal Authentication Manager: Fingerprint. Set a number grade value (>=1). This setting is only used for Multi-Authenticator primary logons	(Default: 1)	Yes	dword/Ø
ESSO-UAM: Smart Card AUI\UAMAuth-{A1B34553-8D40-42A9-8ED5-F70E3497E138}:AuthGrade	Assigns an authentication grade to Universal Authentication Manager: Smart Card. Set a number grade value (>=1). This setting is only used for Multi-Authenticator primary logons.	(Default: 1)	Yes	dword/Ø
ESSO-UAM: Proximity Card AUI\UAMAuth-{4A8F93E4-2328-44CA-8DBE-FBFA4E5FD334}:AuthGrade	Assigns an authentication grade to Universal Authentication Manager: Proximity Card. Set a number grade value (>=1). This setting is only used for Multi-Authenticator primary logons.	(Default: 1)	Yes	dword/Ø
ESSO-UAM: Challenge Questions AUI\UAMAuth-{393D4B53-EC46-4A38-9E9E-3D6B5141DD34}:AuthGrade	Assigns an authentication grade to Universal Authentication Manager: Challenge Questions. This setting is only used for Multi-Authenticator primary logons.	(Default: 1)	Yes	dword/Ø

2.17.3.12.3 Order Settings The Authentication Manager Order settings specify the sequence in which the installed logon methods will be presented to the end user during reauthentication scenarios, if Authentication Manager is chosen as the primary logon method.

For each primary logon method, select or enter a number to indicate the logon method's position in the FTU/logon order. Use these settings for Multi-Authenticators only.

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Windows v2 `AUI\MSauth:AuthOrder`	Sets the ordered position for Windows v2. This will be the order that Windows v2 will be presented to the end user during reauthentication scenarios.	(Default: 2)	Yes	dword/int
Windows `AUI\WinAuth:AuthOrder`	Sets the ordered position for Windows. This will be the order that Windows will be presented to the end user during reauthentication scenarios. **Note:** Windows Authenticator is deprecated as of version 11.1.2 and is listed for upgrade scenarios only. Do not use this authenticator for new configurations.	(Default: 2)	Yes	dword/int
LDAP v2 `AUI\LDAPauth: AuthOrder`	Sets the ordered position for LDAP v2. This will be the order that Windows will be presented to the end user during reauthentication scenarios.	(Default: 3)	Yes	dword/int
LDAP `AUI\LDAP:AuthOrder`	Sets the ordered position for LDAP. This will be the order that Windows will be presented to the end user during reauthentication scenarios.	(Default: 3)	Yes	dword/int
Smart card `AUI\SCauth:AuthOrder`	Sets the ordered position for smart card. This will be the order that Windows will be presented to the end user during reauthentication scenarios.	(Default: 1)	Yes	dword/int
Read-only smart card `AUI\ROSCauth: AuthOrder`	Sets the ordered position for read-only smart card. This will be the order that Windows will be presented to the end user during reauthentication scenarios.	(Default: 1)	Yes	dword/int
Proximity card `AUI\ProxCardAuth: AuthOrder`	Sets the ordered position for proximity card. This will be the order that Windows will be presented to the end user during reauthentication scenarios.	(Default: 6)	Yes	dword/int
RSA SecurID `AUI\SecureIDAuth: AuthOrder`	Sets the ordered position for RSA SecurID. This will be the order that Windows will be presented to the end user during reauthentication scenarios.	(Default: 6)	Yes	dword/int
Entrust `AUI\Entrust:AuthOrder`	Sets the ordered position for Entrust. This will be the order that Windows will be presented to the end user during reauthentication scenarios.	(Default: 4)	Yes	dword/int
Universal Authentication Manager `AUI\UAMAuth:AuthOrder`	Sets the ordered position for Universal Authentication Manager. This will be the order that Universal Authentication Manager will be presented to the end user during reauthentication scenarios. This setting is only used for Multi-Authenticator logons.	(Default: 10)	Yes	dword/int
ESSO-UAM: Windows Password `AUI\UAMAuth-{0C29417D -8A20-48B7-8CC4-D948D 384E9B2}:AuthOrder`	Sets the ordered position for Universal Authentication Manager: Windows Password. This will be the order that the method will be presented to the end user during reauthentication scenarios. This setting is only used for Multi-Authenticator logons.	(Default: 11)	Yes	dword/int

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
ESSO-UAM: Fingerprint `AUI\UAMAuth-{16627EE1 -FAE3-43B5-B884-D3661 649B97D}:AuthOrder`	Sets the ordered position for Universal Authentication Manager: Fingerprint. This will be the order that the method will be presented to the end user during reauthentication scenarios This setting is only used for Multi-Authenticator logons	(Default: 12)	Yes	dword/int
ESSO-UAM: Smart Card `AUI\UAMAuth-{A1B34553 -8D40-42A9-8ED5-F70E3 497E138}:AuthOrder`	Sets the ordered position for Universal Authentication Manager: Smart Card. This will be the order that the method will be presented to the end user during reauthentication scenarios. This setting is only used for Multi-Authenticator logons.	(Default: 13)	Yes	dword/int
ESSO-UAM: Proximity Card `AUI\UAMAuth-{4A8F93E4 -2328-44CA-8DBE-FBFA4 E5FD334}:AuthOrder`	Sets the ordered position for Universal Authentication Manager: Proximity Card. This will be the order that the method will be presented to the end user during reauthentication scenarios. This setting is only used for Multi-Authenticator logons.	(Default: 14)	Yes	dword/int
ESSO-UAM: Challenge Questions `AUI\UAMAuth-{393D4B53 -EC46-4A38-9E9E-3D6B5 141DD34}:AuthOrder`	Sets the ordered position for Universal Authentication Manager: Challenge Questions. This will be the order that the method will be presented to the end user during reauthentication scenarios. This setting is only used for Multi-Authenticator logons.	(Default: 15)	Yes	dword/int

2.17.3.13 Windows v2 Authenticator Settings

The Windows v2 authenticator settings are the primary controls for the Windows Authenticator version 2.

> **Note:** Windows Authenticator version 2 is the preferred authenticator for Logon Manager and is installed by default. For more information about this authenticator, see Section 7.2.7, "Configuring Windows Authenticator Version 2".

2.17.3.13.1 Recovery

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Recovery method `AUI\MSauth\ ResetMethods: ResetMethodGUID`	Specifies the reset method to use when the user's password changes.	4ED42DB8-B8F1-4AE6-B13A-272F74B48FE7: User passphrase (Default) B623C4E7-A383-4194-A 719-7B17D074A70F: Passphrase suppression using user's SID 7B4235FF-5098-435c-9A 05-052426D96AA8: Passphrase suppression using secure key	Yes	string/Ø

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Use Windows Data Protection (DPAPI) AUI\MSauth:UseDPAPI	Set to Yes to use a DPAPI key to protect the Kiosk Manager encryption key, instead of the traditional two-key system of User Password and Recovery Key. **Note:** Consult Microsoft and Oracle DPAPI best practices to ensure your Active Directory and desktop infrastructure is capable and configured to use DPAPI.	0: No (Default) 1: Yes	Yes	dword/Ø

2.17.3.13.2 User interface

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Window title AUI\MSauth: WindowTitle	Use this setting to customize the window title name for this authenticator. Check the box and enter the desired name. **Note:** This entry is not required.		Yes	string/ string
Window subtitle AUI\MSauth: WindowSubTitle	Use this setting to customize the window subtitle name for this authenticator. Check the box and enter the desired name. **Note:** This entry is not required.		Yes	string/ string
Custom image for authentication prompt AUI\MSauth:ImagePath	Enter the fully-qualified path, including the file name, to the image, or click the ellipsis ("**…**") button and browse to the image file. **Note:** The image file must be in bitmap (.bmp) format. The dimensions set for this image are 300 pixels wide by 100 pixels tall. You cannot change these dimensions. If the image is smaller it will be centered in this area; if it is larger, it will be cropped equally on all sides.		No	string/ filename
Reauthentication dialog AUI\MSauth: AuthOptions	Select which method to use when Logon Manager requires the end-user to re-authenticate. **Note:** While the setting is called "Use GINA," it also applies to the Credential Provider mechanism in Windows Vista and newer operating systems.	0: Use SSO dialog. (Default) The user is presented with an authentication dialog whenever reauthentication is needed, and at initial enrollment. 1: Use GINA. The Windows desktop is locked, and the user must reauthenticate to the operating system (using whatever GINA or Credential Provider is installed) before Logon Manager is unlocked.	Yes	dword/Ø
Domains AUI\MSauth:DomainN	Specifies the domain(s) whose member users are permitted to authenticate. Enter one or more desired NetBIOS domain names separated by commas.		No	string/Ø
Prefill username/ID on FTU AUI\MSauth:PrefillUserTextOnFTU	Select whether to have Logon Manager populate the Windows Authenticator V2 authentication dialog with the current user's username/ID. **Note:** This setting is applicable only at FTU.	0: No-User must fill these fields manually. 1: Yes -Logon Manager populates these fields automatically (Default)	Yes	dword/Ø

2.17.3.13.3 Connection information

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Use SSL AUI\MSauth:UseSSL	Specifies whether to connect via SSL. **Note:** This setting applies only to Domain Change Password scenarios.	0: No (insecure) (default to port #389) 1: Yes (default to port #636) (Default)	Yes	dword/Ø

2.17.3.13.4 Credential sharing

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Include in Domain credential sharing group AUI\MSauth:PWSEnable	Enables credential sharing from the authenticator to credentials in a special credential sharing group called "Domain." Whenever the authenticator detects a new password, the password is automatically shared with the Domain credential sharing group.	0: No 1: Yes (Default)	Yes	dword/Ø
Share credentials with other authenticators AUI\MSauth: ShareCredsToAuths	Eliminates double authentication by linking authenticator credentials. If multiple authenticators use the same credentials, the duplicate credentials are used without requiring the user to reenter them. Enter a comma-separated list of authenticators to share the credentials with, for example "WinAuth, MSAuth." **Note:** To locate other authenticator names, refer to the list located under HKLM\ Software\ Oracle\AUI.		Yes	string/ string
Share credentials with synchronizers AUI\MSauth: ShareCredsToSyncs	This setting eliminates double authentication when an authenticator shares credentials with one or more synchronizers. Enter a comma-separated list of synchronizers to share the credentials with, for example "ADEXT,LDAPEXT." **Note:** To locate other synchronizer names, see the name listed in the registry for that synchronizer (located under HKLM\Software\Passlogix\Extensions\SyncManager).		Yes	string/ string

2.17.3.14 Windows v2 Authenticator Passphrase Settings

The Windows v2 Authenticator Passphrase settings configure options for users' Windows Authenticator version 2 passphrases.

2.17.3.14.1 User interface

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Message AUI\MSauth\Reset: PassphraseMessage	Use this setting to display a user agreement-style dialog where the user must check a checkbox to continue. This is typically used to suggest the importance of the passphrase that users enter. Check the box and enter the desired message. **Note:** This message can contain multiple lines, 180 character maximum. The character sequence "\n" will be replaced with carriage return and new line characters. If this setting is not set, the dialog is skipped.		Yes	string/ string
Message dialog title AUI\MSauth\Reset: PassphraseDialogTitle	Use this setting to customize the user agreement-style dialog title. Check the box and enter the desired title.		Yes	string/ string

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Checkbox label AUI\MSauth\Reset: PassphraseChkboxMsg	Use this setting to customize the user agreement style dialog checkbox. Check the box and enter the desired label. **Note:** The user must check this checkbox before the dialog can be dismissed. The **OK** button is disabled until this checkbox is checked.		Yes	string/ string

2.17.3.14.2 Options

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Minimum length AUI\MSauth\Reset: MinPassphraseLength	Default required length of a passphrase. You can override this setting by specifying the required length for a specific question.	8: Default	Yes	dword/int
User can change passphrase AUI\MSauth: ShowChange AnswerOption	Toggles availability of the user's option to change the answer to the verification question.	0: No 1: Yes (Default)	Yes	dword/Ø
Reset with old password AUI\MSauth:ResetWOP	Allows the previous password to be used in the passphrase process.	0: No (Default) 1: Yes	Yes	dword/Ø
Force password re-enrollment when using old password to reset AUI\MSauth: RWOPSkipReset	Specifies whether the user can skip the Logon Manager passphrase prompt. Enabling this feature ensures that after a user enters his previous Windows password, Logon Manager will prompt him to enter a new passphrase. **Warning:** Disabling this feature entails the risk of a complete lockout to Logon Manager. This can happen if a user no longer remembers his passphrase, and subsequently forgets his Windows password. In this scenario, a user would be completely locked out of Logon Manager.	0: Yes (Default) 1: No	Yes	dword/Ø

2.17.3.15 Windows Authenticator Settings

The Windows authenticator settings are the primary controls for the Windows Authenticator.

> **Note:** Windows Authenticator is deprecated as of version 11.1.2 and is listed for upgrade scenarios only. Do not use this authenticator for new configurations.

2.17.3.15.1 User interface

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Window title AUI\WinAuth: WindowTitle	Use this setting to customize the window title name for this authenticator. Check the box and enter the desired name. **Note:** This entry is not required.		Yes	string/ string
Window subtitle AUI\WinAuth: WindowSubTitle	Use this setting to customize the window subtitle name for this authenticator. Check the box and enter the desired name. **Note:** This entry is not required.		Yes	string/ string

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Custom image for authentication prompt AUI\WinAuth:ImagePath	Enter the fully-qualified path, including the file name, to the image, or click the ellipsis "..." button and browse to the image file. **Note:** The image file must be in bitmap (.bmp) format. The dimensions set for this image are 300 pixels wide by 100 pixels tall. You cannot change these dimensions. If the image is smaller it will be centered in this area; if it is larger, it will be cropped equally on all sides.		No	string/ filename
Require old password when Windows password changes AUI\WinAuth:PWEnable	Provides enhanced security by requiring the user to enter the previous password when changing to a new one.	0: No (Default) 1: Yes	Yes	dword/Ø

2.17.3.15.2 Credential sharing

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Share credentials with other authenticators AUI\WinAuth: ShareCredsToAuths	This setting eliminates double authentication by linking authenticator credentials. If multiple authenticators use the same credentials, the duplicate credentials are used without requiring the user to reenter them. Enter a comma-separated list of authenticators to share the credentials with, for example "WinAuth, MSAuth." **Note:** To locate other authenticator names, refer to the list located under HKLM\ Software\ Oracle\AUI.		Yes	string/ string
Share credentials with synchronizers AUI\WinAuth: ShareCredsToSyncs	This setting eliminates double authentication when an authenticator shares credentials with one or more synchronizers. Enter a comma-separated list of synchronizers to share the credentials with, for example "ADEXT,LDAPEXT." **Note:** To locate other synchronizer names, see the name listed in the registry for that synchronizer (located under HKLM\Software\Passlogix\Extensions\SyncManager).		Yes	string/ string

2.17.3.16 LDAP v2 Authenticator Settings

The LDAP v2 authenticator settings are the primary controls for enabling LDAP version 2 authentication.

2.17.3.16.1 Recovery

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Recovery method AUI\LDAPauth\ResetMethods:ResetMethodGUID	Specifies the method for recovering a user's lost password. **Note:** For an in-depth discussion of LDAP v2 configuration, see Chapter 7.2.6, "Understanding the Logon Manager Secondary Authentication API."	User passphrase (Default) Passphrase suppression using user's SID Passphrase suppression using secure key Passphrase suppression using entryUUID	Yes	string/Ø

2.17.3.16.2 Connection information

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Directory type `AUI\LDAPAuth:Director yType`	Specifies the type of the target directory server software. If your server software is not listed, select LDAP-compliant Directory Server.	Unspecified LDAP Directory Microsoft Active Directory Novell eDirectory LDAP-compliant Directory Server Oracle Directory Server Enterprise Edition IBM Tivoli Directory Server Oracle Internet Directory Siemens DirX Directory Server	Yes	dword/Ø

Servers
 	
`AUI\LDAPauth\ Servers:ServerN`
	Enter the servers to try, in the format "*computer[:port]*" (one server per line), where *computer* is the server name or IP, and *port* is assumed to be default (636 for SSL, 389 for no SSL) if not specified.
	
	Examples:
	
	`127.0.0.1`
	
	`127.0.0.1:456`
	
	`somewhereelse.com:8080`
	
	`·anotherplace.com`
	
	Note: You musty specify at least one server for this extension to work.
			No	string/Ø

User paths `AUI\LDAPauth: UserPathN`	Enter the fully-qualified path to where the user account is located. There can be unlimited paths to search. The extension searches these in order, looking for the user account. If not found, the extension will search the directory tree. **Note:** You must either specify a value for UserPrepend or at least one value for `UserPath` for this extension to work. If using `UserPaths`, do not use UserLocation.		Yes	string/Ø
Use SSL `AUI\LDAPauth:UseSSL`	Specifies whether to connect via SSL.	0: No (insecure) (default to port #389) 1: Yes (default to port #636) (Default)	Yes	dword/Ø

2.17.3.16.3 User interface

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Window title `AUI\LDAPauth: WindowTitle`	Use this setting to customize the Window title name for this authenticator. **Note:** This entry is not required.		Yes	string/ string
Show user path `AUI\LDAPAuth: ShowUserPath`	Enable this setting to display the User path combo box control in the LDAP v2 authentication dialog.	0: No 1: Yes (Default)	Yes	dword/Ø

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Custom image for authentication prompt AUI\LDAPAuth: ImagePath	Enter the fully-qualified path, including the file name, to the image, or click the ellipsis "**…**" button and browse to the image file. **Note:** The image file must be in bitmap (.bmp) format. The dimensions set for this image are 300 pixels wide by 100 pixels tall. You cannot change these dimensions. If the image is smaller it will be centered in this area; if it is larger, it will be cropped equally on all sides.		Yes	string/ filename

2.17.3.16.4 Credential sharing

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Share credentials with other authenticators AUI\LDAPauth: ShareCredsToAuths	Enter a comma-separated list of authenticators with which to share the credentials, for example "WinAuth, MSAuth." **Note:** For other authenticator names, refer to the list located under HKLM\Software\Oracle\AUI.		Yes	string/ string
Share credentials with synchronizers AUI\LDAPauth: ShareCredsToSyncs	Enter a comma-separated list of synchronizers to share the credentials with, for example "ADEXT,LDAPEXT." **Note:** For other synchronizer names, refer to the list located under HKLM\Software\Oracle\ Extensions\SyncManager.		Yes	string/ string
Include in LDAP credential sharing group AUI\LDAPauth: PWSEnable	Enables credential sharing from the authenticator to credentials in the Group Domain. (Also requires AccessManager:PWSEnable to be enabled.)	0: No 1: Yes (Default)	Yes	dword/Ø

2.17.3.17 LDAP v2 Authenticator Special Purpose Settings

The LDAP v2 Authenticator Special Purpose settings control special-case options for enabling standard LDAP v2 authentication.

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Naming attribute string AUI\LDAPauth: UserPrepend	String to prepend to UserPaths when the DN for a user is in the form of: cn=%UserName%,ou=people,dc=computer instead of the form: *namingattribute*= %UserName%, ou=people, dc=computer (where *namingattribute* can be any string). **Note:** Usually, you must set this value to cn for Novell eDirectory. If using UserPrepend, you must use UserPathN and do not use UserLocation.		Yes	string/ string
BIND timeout AUI\LDAPauth:Timeout	Enter the length of the timeout (in milliseconds) of LDAP BIND call.	(Default depends on the operating system)	Yes	dword/ int

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType

Alternate user ID location
 	
`AUI\LDAPauth:`
`UserLocation`
	Specifies where to locate a user object when the user validates against an attribute other than the username.
	
	Example
	
	If users authenticate with an employee ID # for logon (validation against the empid attribute) and the user object is in:
	
	`ou=people,dc=computer`
	
	set UserLocation to
	
	`empid=%USER,ou=people,dc=computer`
	
	instead of to
	
	`uid=user,ou=people,dc=computer`
	
	Note: For Novell eDirectory, UserLocation should be: `uid=%USER,path to the object`.
	
	If using `UserLocation`, do not use `UserPrepend` or `UserPaths`.
			Yes	string/ string

2.17.3.18 LDAP Authenticator Settings

The LDAP authenticator settings are the primary controls for enabling standard LDAP authentication. These settings must be used in order for the Agent to use LDAP as a primary logon method.

2.17.3.18.1   Connection information

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType

Directory type
 	
`AUI\LDAP:`
`DirectoryType`
	Specifies the type of directory server. If the directory server is not listed, select "Generic LDAP Directory."	0: Unspecified LDAP Directory
		
		3: Novell eDirectory
		
		5: Generic LDAP Directory (Default)
		
		8: Oracle Directory Server Enterprise Edition
		
		9: IBM Tivoli Directory Server
		
		10: Oracle Internet Directory
		
		11: Siemens DirX Directory Server
			Yes	dword/Ø

Servers
 	
`AUI\LDAP\Servers:`
`ServerN`
	Specifies the servers to try, in the format *computer[:port]* (one server per line), where *computer* is the server name or IP, and *port* is assumed to be default (636 for SSL, 389 for no SSL) if not specified.
	
	Examples
	
	`127.0.0.1`
	
	`127.0.0.1:456`
	
	`somewhereelse.com:8080`
	
	`anotherplace.com`
	
	Note: You must specify at least one server in order for this extension to work.
			No	string/Ø

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
User paths AUI\LDAP:UserPathN	Specifies the fully-qualified path to where the user account is located. There can be unlimited paths to search. The extension searches these in order, looking for the user account. If the account is not found, the extension will search the directory tree. **Note:** You must specify a value for either UserPrepend or at least one value for UserPaths for this extension to work. If using UserPaths, do not use UserLocation.		Yes	string/Ø
Use SSL AUI\LDAP:UseSSL	Specifies whether to connect via SSL.	No. (insecure) (default to port #389) Yes. (default to port #636) (Default)	Yes	dword/Ø

2.17.3.18.2   Active Directory

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Enable Domain name support AUI\LDAPauth:UsingAD	Enables Active Directory Domain name support. End users can specify the Domain name (for example, domainname\username) at primary logon. Alternatively, the administrator can specify a default Domain name (see the "Active Directory: Default Domain name" setting, below) to let end users log on by username alone. If you don't specify a Domain, Logon Manager uses the local workstation's Domain.	0: No (Default) 1: Yes	Yes	dword/Ø
Default Domain name AUI\LDAP:ADDomain	The Active Directory Domain name to use for primary logon if you don't specify a Domain for the username/ID credential (for example, domainname\username). Use this setting only if you set the "Active Directory: Domain name support enabled" setting to "Use AD Domain names." If you enable Domain name support and this setting is blank (and the end user does not specify a Domain), Logon Manager uses the local workstation's Domain.		Yes	string/ string

2.17.3.18.3   User interface

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Window title AUI\LDAP:WindowTitle	Use this setting to customize the Window title name for this authenticator. **Note:** This entry is not required.		Yes	string/ string
Password change window title AUI\LDAPauth: CAP_WindowTitle	Use this setting to customize the Active Directory Change Password Window title name for this synchronizer. **Note:** This entry is not required.		Yes	string/ string
Password change window subtitle AUI\LDAPauth: CAP_WindowSubTitle	Use this setting to customize the Active Directory Change Password Window subtitle name for this synchronizer. **Note:** This entry is not required.		Yes	string/ string

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Custom image for authentication prompt `AUI\LDAP:ImagePath`	Enter the fully-qualified path, including the file name, to the image, or click the ellipsis "**…**" button and browse to the image file. **Note:** The image file must be in bitmap (.bmp) format. The dimensions set for this image are 300 pixels wide by 100 pixels tall. You cannot change these dimensions. If the image is smaller it will be centered in this area; if it is larger, it will be cropped equally on all sides.		No	string/ filename
Show user path `AUI\LDAP:ShowUserPath`	Use this setting to show/hide the **User Path** combo box control in the LDAP authentication dialog.	0: No 1: Yes (Default)	Yes	dword/Ø

2.17.3.18.4   Credential sharing

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Share credentials with other authenticators `AUI\LDAP: ShareCredsToAuths`	Enter a comma-separated list of authenticators with which to share the credentials. For example "WinAuth, MSAuth." **Note:** To locate other authenticator names, refer to the name listed in the registry for that authenticator (located under: `HKLM\Software\Passlogix\AUI`).		Yes	string/ string
Share credentials with synchronizers `AUI\LDAP: ShareCredsToSyncs`	Enter a comma-separated list of synchronizers with which to share the credentials. For example "`ADEXT,LDAPEXT`." **Note:** To locate other synchronizer names, refer to the name listed in the registry for that synchronizer (located under: `HKLM\Software\Passlogix\Extensions\ SyncManager`).		Yes	string/ string

2.17.3.19 LDAP Authenticator Special Purpose Settings

The LDAP Authenticator Special Purpose settings control special-case options for enabling standard LDAP authentication.

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Naming attribute string `AUI\LDAP:UserPrepend`	Specifies the string to prepend to UserPaths when the DN for a user is in the form of: `cn=%UserName%,ou=people,dc=computer` instead of the form: `namingattribute=%UserName%, ou=people,dc=computer` (where `namingattribute` can be any string). **Note:** Usually, you must set this value to `cn` for Novell eDirectory. If using `UserPrepend`, you must use `UserPathN` and do not use `UserLocation`.		Yes	string/ string
BIND timeout `AUI\LDAP:Timeout`	Specifies the timeout (in milliseconds) of the LDAP BIND call.	Default depends on the operating system.	Yes	dword/ int

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Alternate user ID location AUI\LDAP:UserLocation	Specifies where to locate a user object when the user validates against an attribute other than the username. **Example** If users authenticate with an employee ID # for logon (validation against the empid attribute) and the user object is in: ou=people,dc=computer set UserLocation to empid=%USER,ou=people,dc=computer instead of to uid=user,ou=people,dc=computer **Note:** For Novell eDirectory, UserLocation should be: uid=%USER,path to the object. If using UserLocation, do not use UserPrepend or UserPaths.		Yes	string/ string
Enable directory search for users AUI\LDAP: LDAPBindSearch	Enables or disables directory search for the user account. When the user account is not found in the given path, the authenticator will search for it from that location down the directory tree. The search is performed whether using "User Paths" or the "Alternate User ID location."	0: No (Default) 1: Yes	Yes	dword/Ø

2.17.4 Using Strong Authenticators

Logon Manager includes both standard logon methods such as LDAP and Windows Logon, and strong authenticators such as smart cards, proximity devices, and RSA SecurID tokens. Logon Manager enables organizations to seamlessly bridge strong authentication to all of their applications. Users can employ different authenticators at different times and application access can be controlled based upon the authenticator used.

> **Note:** See the Oracle certification matrix for the most up-to-date list of supported authentication devices.

Logon Manager provides authentication support from a variety of strong authenticators for all authentication events: initial authentication, re-authentication, and forced authentication.

This section describes any specific settings that can be enabled within a strong authenticator in order for the authenticator to work with Logon Manager. It also describes all the Administrative Console settings and any steps that must be taken to integrate with Kiosk Manager, as well as any known issue or technical notes that apply to a specific strong authenticator.

2.17.5 Strong Authenticator Configuration Settings

If the strong authenticator you are using is not listed in this section, there are no specific settings that must be adjusted or relevant technical notes.

Select your strong authenticator, or see the Kiosk Manager integration notes, which apply to all authenticators:

- Smart Cards

- Read-Only Smart Cards

- Proximity Cards

- RSA SecurID

- Secure Data Storage

- Kiosk Manager Integration Notes

2.17.5.1 Smart Cards

Smart Card settings are available in the Authentication section of Global Agent Settings in the Administrative Console. This section also includes steps that you must take to integrate Smart Cards with Kiosk Manager, and other technical notes about using this authenticator.

2.17.5.1.1 Administrative Console Settings The smart card settings control special-case options for smart-card authentication. These settings are not required.

To access the smart card settings, click **Global Agent Settings > Live > Authentication > Smart Card**. See the Smart Card Authentication section for a full discussion of these settings.

2.17.5.1.2 Smart Card Initialization Prior to use with Authentication Manager, smart cards must be initialized and contain a valid PIN. If Authentication Manager is configured to use smart card certificates, smart cards must contain a valid PKI certificate. If the smart cards are also to be used with Kiosk Manager, they must have a serial number.

Authentication Manager does not provide any smart card initialization, configuration, or administration services, so this step must be performed using a third-party Card Management System (CMS) or middleware administration utility compatible with your smart card.

2.17.5.2 Integrating with Kiosk Manager

This section applies when using the Smart Card authenticator with Kiosk Manager.

2.17.5.2.1 Support for storing and passing through the synchronization credentials with Kiosk Manager and Smart Card integration. When using Smart Card authenticator with Kiosk Manager, the user's synchronization credentials can optionally be stored on the smart card by the authenticator. If stored in this manner, the credentials are then silently passed through to Logon Manager after a user initiates a Kiosk Manager session by inserting their smart card into the reader and entering the correct PIN. This feature prevents a double authentication when starting a Kiosk Manager session whereby the user authenticates with their smart card and PIN and then is subsequently prompted by Logon Manager to provide their synchronization username and password.

2.17.5.2.2 .NET Smart Cards. Due to technical limitations with the .NET cards, when using .NET smart cards with Kiosk Manager, inserting the smart card when Kiosk Manager is locked always causes a new session to start. To unlock an existing session, click the Unlock Existing Session link.

2.17.5.2.3 Separate Authentication Prompts Appear for the Kiosk Manager Session and Logon Manager when Smart Card is the Primary Logon Method. In a Kiosk Manager environment that uses smart cards as the primary logon method, users are prompted to authenticate separately to Kiosk Manager and Logon Manager.

This occurs because a smart card authentication is only valid for the process that initiated it and cannot be shared between processes. This is a design characteristic of the smart card middleware and not Oracle software.

When the Kiosk Manager session starts, Kiosk Manager queries the smart card middleware for authentication and the user is prompted to authenticate via smart card and PIN. This authentication is valid for the Kiosk Manager process only; therefore, when the Kiosk Manager session is successfully created and Logon Manager starts, the user is authenticated again, this time to Logon Manager.

This double-prompt can be eliminated by configuring an Active Directory/AD LDS (ADAM) synchronizer to use the card's certificate and the smart card authenticator to share credentials with synchronizers. Configure the following settings:

- On the Global Agent Settings' Smart Card Authenticator Settings, add ADEXT or ADAMSyncExt to the list for the setting, "Share credentials with synchronizers."

- On the Global Agent Settings' Active Directory/AD LDS (ADAM) synchronizer pages Credential sharing group, add SCAuth to the list for the setting, "Share credentials with authenticators."

- On the Global Agent Settings' Active Directory/AD LDS (ADAM) synchronizer pages' Connection information group, select **Use card's certificate** for Credentials to use.

- On the Global Agent Settings' Kiosk Manager page, disable the setting, **Pre-populate on startup** under the **Strong authenticator** options group.

2.17.5.2.4 HID Crescendo C200 and C700 smart cards. When using HID Crescendo C200 or C700 as smart cards with Kiosk Manager, a smart card-only reader should be used. Using a dual function smart card and proximity card reader is unsupported. The HID Crescendo C200 mini-driver should be installed from Microsoft's update catalog: http://test.catalog.update.microsoft.com/v7/site/search.aspx?q=umdf.

2.17.5.2.5 Using SSO-Generated Keys Technical Note. When the Use default certificate for authentication (located in the Logon Manager Administrative Console Global Agent Settings > Authentication > Smart Card) is set to No, users may be prompted to enter their PIN twice during the First Time Use (FTU) enrollment process.

This is normal and necessary in order to create the SSO keyset. Subsequent authentications after FTU only prompt users to enter their PIN once.

2.17.5.3 Smart Card Middleware

These technical notes are in reference to known issues and considerations with Smart Card middleware.

2.17.5.3.1 Gemplus Libraries 4.20 with Authentication Manager Re-authentication events do not display the PIN dialog. When authenticating to Logon Manager, the first authentication properly displays a PIN dialog and allows a successful authentication. Subsequent re-authentication events within a short period of time do not display the PIN dialog, preventing authentication from succeeding.

To work around this, restart the Logon Manager process requesting authentication.

2.17.5.3.2 Netmaker Net iD 4.6 with Kiosk Manager When starting a new Kiosk Manager session, the user's synchronization credentials are not read off the card. After entering their PIN, users must then manually enter their synchronization credentials to start the session.

2.17.5.3.3   RSA RAC 2.0 / Smartcard Middleware 2.0 with Kiosk Manager RSA Middleware reports that no smart cards are present when Kiosk Manager is locked and a smart card is inserted into a reader. Sessions must be manually started. After Kiosk Manager is unlocked, authentication to Logon Manager with smart cards will work as expected.

2.17.5.3.4   Smart Card and Read-Only Smart Card Middleware Default Library Path Locations
The following table provides the default installation paths for all supported smart card middleware. These are sample paths to enter in the PKCS #11 Library Path field located on the Read-Only Smart Card > Advanced and Smart Card > Advanced panels:

Smart Card Type	Library Path
Axalto Access Client Software 5.2	`C:\Program Files\Axalto\Access Client\v5\xltCk.dll`
GemSafe Libraries 4.2.0	`C:\Program Files\Gemplus\GemSafe Libraries\BIN\GCLIB.DLL`
HID C700 middleware	`aetpkss1.dll`
NetMaker Net iD 4.6	`iidp11.dll`
RSA Authentication Client 2.0 / Smartcard Middleware 2.0	`C:\Program Files\RSA Security\RSA Authentication Client\Pkcs11.dll`
SafeSign/RaakSign Standard 2.3	`aetpkss1.dll`
Schlumberger Cyberflex Access 4.5	`C:\Program Files\Schlumberger\Smart Cards` and `Terminals\Cyberflex Access Kits\v4\slbCk.dll`
Siemens 3.2.41 (CardOS API v3.2)	`siecap11.dll`

Read-Only Smart Card Type	Library Path
Fujitsu mPollux DigiSign Client 1.3.2-34(1671)	`C:\Program Files\Fujitsu Services\Fujitsu mPollux DigiSign Client\Cryptoki.dll`
SafeSign Identity Client 2.2.0	`aetpkss1.dll`

> **Note:** Any file without a fully-qualified path listed in the tables above resides in the system directory and therefore does not require a full path when being specified.

2.17.5.4 Smart Card Authenticator Settings

The Smart Card authenticator settings control special-case options for smart card authentication. Also see Smart Cards in the Strong Authenticators section for configuration with Kiosk Manager and technical notes.

2.17.5.4.1   Options

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Smart card library `AUI\SCauth: SmartCardAPI`	Specifies whether to use the Cryptographic Service Provider (CSP) or the PKCS #11 library to perform cryptographic operations on the smart card. **Note:** Set this to PKCS # 11 only if using SafeSign/RaakSign middleware.	0: CSP (Default) 1: PKCS#11	Yes	dword/Ø

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Use default certificate for authentication AUI\SCauth: UseCertOnCard	Specifies whether to use the default logon certificate (provided by the administrator) on the card for authentication. With this setting disabled (the default), the public/private keys in the SSO container on the card will be used (and created if necessary).	0: No (Default) 1: Yes	Yes	dword/Ø
Store synchronization credentials AUI\SCauth: StoreSyncCreds	Specifies whether to store the user's synchronization repository credentials on the smart card. Store credentials when using smart card authorization in conjunction with Kiosk Manager and/or if using the read-only smart card authenticator. **Note:** Performance improves when credentials are not stored on the smart card because the read/write operation adds time to the authentication process.	0: No (Default) 1: Yes	Yes	dword/Ø
Store the PIN AUI\SCauth: AuthOptions	Specifies whether to store the smart card PIN (creating the possibility that the Agent might prompt for the PIN), or to let the smart card drivers handle the PIN request.	0: No (Default) 1: Yes	Yes	dword/Ø
PKCS#11 Library Path AUI\SCAuth:PKCS11Path	Specifies the path to the smart card middleware file, which implements the PKCS#11 standard.		Yes	string/ string
Custom certificate check extension path AUI\SCAuth:CCCEPath	Specifies the path to the custom certificate check extension. **Note:** This entry is not required.		Yes	string/ string
Allow secure PIN entry AUI\SCAuth:AllowSPE	Specifies whether to allow users to enter a PIN on a smart card reader keypad that supports secure PIN entry. **Note:** You cannot use secure PIN entry in conjunction with a PIN recovery group.	0: Only allow non-SPE login (Default) 1: Only allow SPE login	Yes	dword/Ø
Lock desktop on smart card removal AUI\SCauth: LockDesktopOnRemoval	Specifies whether to lock the desktop when the smart card owner removes the smart card from the reader. By default, this value is set to **No**. If the value is set to **Yes**, the user's workstation locks when the smart card is removed. If the user locks the desktop using **Ctrl+Alt-Delete**, the authentication status remains unchanged.	0: No (Default) 1: Yes	Yes	dword/Ø
Allow forced verification AUI\SCauth: AllowForced Verification	Specifies whether Logon Manager should automatically authenticate users after they authenticate to Windows with a smart card. Setting this to **No** (the default) requires a user to enter a PIN for both Windows logon and to authenticate to Logon Manager. Setting this to Yes eliminates the double PIN prompt and the user needs to enter a PIN only to authenticate to Windows, while Logon Manager automatically authenticates the user. **Note:** To use this feature, you MUST install Network Provider with Logon Manager. This is available during the installation on the Advanced Setup panel under Authenticators. Refer to *Oracle Enterprise Single Sign-On Suite Installation Guide* for more information.	0: No (Default) 1: Yes	Yes	dword/Ø

2.17.5.4.2 User interface

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType

Window title
 	
`AUI\SCauth:`
`WindowTitle`
	Use this setting to customize the window title name for this authenticator. Check the box and enter the desired name.
	
	Note: This entry is not required.
			Yes	string/ string

Window subtitle
 	
`AUI\SCauth:`
`WindowSubTitle`
	Use this setting to customize the window subtitle name for this authenticator. Check the box and enter the desired name.
	
	Note: This entry is not required.
			Yes	string/ string

2.17.5.4.3 Recovery

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType

Recovery method
 	
`AUI\SCauth:`
`ResetEnable`
	Specifies which supplier of the reset passphrase to use:
	
	■ The user (entering the passphrase in a dialog);
	
	■ The newest non-default encryption certificate on the card itself;
	
	or
	
	■ The smart card PIN.
		1: Passphrase (Default)
		2: Encryption certificate
		3: Smart card PIN
			Yes	dword/Ø

Recovery certificate object identifier
 	
`AUI\SCAuth:`
`ResetCertOID`
	Specifies the object identifier of the certificate to use for the certificate-based passphrase feature. The authenticator searches the "Enhanced Key Attributes" of each certificate on the smart card for this Object Identifier.
	
	Note: You must set the "Recovery method" option to **Encryption certificate**.
	
	This entry is not required.
			Yes	string/ string

PIN recovery group
 	
`AUI\SCauth:`
`PINRecovery`
`DomainGroupName`
	Enter the domain security group name (in format `domain\group`) for the PIN Recovery Group. Members of this group have permission to authenticate to Logon Manager without a smart card, using only a PIN.
	
	This setting is useful in a scenario where users lose their cards and are waiting for replacements. In the interim, users can be added to this PIN recovery group so that they can authenticate to Logon Manager without their cards. To use this feature, you MUST set the "Recovery method" setting above to **Smart card PIN**.
	
	Note: You cannot use a PIN recovery group in conjunction with secure PIN entry.
			Yes	string/ string

2.17.5.4.4 Credential sharing

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType

Share credentials with synchronizers
 	
`AUI\SCauth:`
`ShareCredsToSyncs`
	This setting eliminates double authentication when an authenticator shares credentials with one or more synchronizers.
	
	Enter a comma-separated list of synchronizers to share the credentials with, for example `"ADEXT,ADAMSyncEXT."`
	
	Note: To locate other synchronizer names, see the name listed in the registry for that synchronizer (located under `HKLM\Software\Passlogix\Extensions\SyncManager`).
			Yes	string/ string

2.17.5.5 Read-Only Smart Cards

Read-Only Smart Card settings are available in the Authentication section of Global Agent Settings in the Administrative Console. This section also includes steps that you must take to integrate Smart Cards with Kiosk Manager, and other technical notes about using this authenticator.

2.17.5.5.1 Administrative Console Settings The read-only smart card settings control special-case options for read-only smart card authentication. These settings are not required.

To access the smart card settings, click **Global Agent Settings > Live > Authentication > Read Only Smart Card**. See the Read-Only Smart Cards section for a full discussion of these settings.

2.17.5.5.2 Read-Only Smart Card Initialization Prior to use with Authentication Manager, read-only smart cards must be initialized and contain a valid PIN and PKI certificate. If the smart cards are also to be used with Kiosk Manager, they must have a serial number.

Authentication Manager does not provide any smart card initialization, configuration, or administration services, so this step must be performed using a third-party Card Management System (CMS) or middleware administration utility compatible with your smart card.

2.17.5.6 Integrating with Kiosk Manager

The following notes explain special considerations when integrating a Read-Only Smart Card authenticator with Kiosk Manager.

2.17.5.6.1 Support for storing and passing through the synchronization credentials with Kiosk Manager and Read-Only Smart Card integration When using Read-Only Smart Card authenticator with Kiosk Manager, the user's synchronization credentials can optionally be stored by setting Store Synchronization Credentials to **Yes** and configuring the Secure Data Storage feature. If stored in this manner, the credentials are then silently passed through to Logon Manager after a user initiates a Kiosk Manager session by inserting their read-only smart card into the reader and entering the correct PIN. This feature prevents a double authentication when starting a Kiosk Manager session whereby the user authenticates with their read-only smart card and PIN and then is subsequently prompted by Logon Manager to provide their synchronization username and password.

2.17.5.6.2 Separate Authentication Prompts Appear for the Kiosk Manager Session and Logon Manager when Read-Only Smart Card is the Primary Logon Method In a Kiosk Manager environment that uses read-only smart cards as the primary logon method, users are prompted to authenticate separately to Kiosk Manager and Logon Manager.

This occurs because a smart card authentication is only valid for the process that initiated it and cannot be shared between processes. This is a design characteristic of the smart card middleware and not Oracle software.

When the Kiosk Manager session starts, Kiosk Manager queries the smart card middleware for authentication and the user is prompted to authenticate via smart card and PIN. This authentication is valid for the Kiosk Manager process only; therefore, when the Kiosk Manager session is successfully created and Logon Manager starts, the user is authenticated again, this time to Logon Manager.

There is currently no workaround for this behavior.

2.17.5.7 Read-Only Smart Card Authenticator Settings

The Read-Only Smart Card authenticator settings control special-case options for read-only smart card authentication.

2.17.5.7.1 Options

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Store synchronization credentials AUI\ROSCauth: StoreSyncCreds	Specifies whether to store the user's synchronization repository credentials using Secure Data Storage. **Note:** Using this setting requires that you enable and configure Secure Data Storage.	0: No (Default) 1: Yes	Yes	dword/Ø
PKCS#11 Library Path AUI\ROSCAuth: PKCS11Path	Specifies the path to the smart card middleware file, which implements the PKCS#11 standard. **Note:** This entry is not required unless you set "Store synchronization credentials" to **Yes** or are using read-only smart cards with Kiosk Manager.		Yes	string/ string
Custom certificate check extension path AUI\ROSCauth:CCCEPath	Specifies the path to the custom certificate check extension. **Note:** This entry is not required.		Yes	string/ string
Allow secure PIN entry AUI\ROSCauth:AllowSPE	Use this setting to allow users to enter a PIN on a smart card reader keypad that supports secure PIN entry.	0: Only allow non-SPE login (Default) 1: Only allow SPE login	Yes	dword/Ø

2.17.5.7.2 Recovery

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Recovery method AUI\ROSCauth: ResetEnable	Enables the use of the reset passphrase. The passphrase can be supplied either by the user (entering the passphrase in a dialog) or by the newest non-default encryption certificate on the card itself.	1: Passphrase (Default) 2: Encryption certificate	Yes	dword/Ø
Recovery certificate object identifier AUI\ROSCAuth: ResetCertOID	Specifies the object identifier of the certificate used for the certificate-based passphrase feature. The authenticator searches the "Enhanced Key Attributes" of each certificate on the smart card for this object identifier. **Note:** You must set the "Recovery method" option to **Encryption certificate**. This entry is not required.		Yes	string/ string

2.17.5.8 Proximity Cards

Proximity Card settings are available in the Authentication section of Global Agent Settings in the Administrative Console. This section also includes steps that you must take when using Active Directory or AD LDS (ADAM), and other technical notes about configuring and using this authenticator.

2.17.5.8.1 Administrative Console Settings To access proximity card settings, click **Global Agent Settings > Live > Authentication > Proximity Card**.

2.17.5.9 Integrating with Kiosk Manager

The following notes explain special considerations when integrating a Proximity Card authenticator with Kiosk Manager.

2.17.5.9.1   Support for storing and passing through the synchronization credentials with Kiosk Manager and Proximity Card integration Support for storing and passing through the synchronization credentials with Kiosk Manager and Proximity Card integration

When the Proximity Card authenticator's second factor is set to **User Defined PIN**, the user's synchronization credentials can optionally be stored by the authenticator by configuring the Secure Data Storage feature. If stored in this manner, the credentials are then silently passed through to Logon Manager after a user initiates a Kiosk Manager session by tapping a proximity card and entering the correct PIN. This feature prevents a double authentication when starting a Kiosk Manager session whereby the user authenticates with their proximity card and PIN and then is subsequently prompted by Logon Manager to provide a synchronization username and password.

2.17.5.9.2   Insufficient privileges for Guest User Accounts Guest User accounts do not have sufficient privileges to perform operations required for successfully completing the Logon Manager First-Time-Use wizard. Oracle recommends against using Guest Accounts as the kiosk account.

2.17.5.10 Active Directory Technical Notes

An Active Directory administrator must perform the following steps on the `CN=Users` container on the Active Directory controller to grant read/write access to the Creator Owner user.

Without these steps, users will not have sufficient rights to change their proximity card number. As a result, when a user enters the passphrase scenario to update his card information (lost card scenario), the error, "Proximity card assigning failed" displays.

1. Open **Active Directory Users and Computers** console on AD controller.

2. Right-click on the **Users AD** object (`CN=Users`).

3. Click **Properties** in pop-up menu.

4. Click the **Security** tab.

5. Click the **Add** button.

6. Under **Enter the object names to select**, type `CREATOR OWNER`.

7. Click the **Check Names** button to resolve the entry.

8. Click **OK**.

9. Under **Group or user names**: highlight **CREATOR OWNER**.

10. Click the **Advanced** button.

11. The **Advanced Security Settings for Users** window displays. Verify that **Allow inheritable permissions from the parent to propagate to this object and…** checkbox is checked (set to **TRUE**).

12. Double-click the **CREATOR OWNER** user.

13. Set **Apply Onto dropdown to Child Objects only**.

14. Set the **Read All Properties** and **Write All Properties** checkboxes under **Allow** to checked (set to **TRUE**).

15. **Apply** all changes.

To use the proximity card authenticator with Active Directory, you must enable the storing of credentials under user objects:

1. Open the Administrative Console.

2. Connect to the repository.

3. From the **Repository** menu, select **Enable Storing Credentials under User Objects** (Active Directory only).

2.17.5.11 AD LDS (ADAM) Technical Notes

An AD LDS (ADAM) administrator must perform the following steps on the `"OU=People"` container on the AD LDS (ADAM) server to grant read/write access to the users.

1. Open an AD LDS (ADAM) Tools Command Prompt on the AD LDS (ADAM) server.

2. Execute the following command to give users **Read** permission to the `People` container and its sub-objects:

   ```
   dsacls.exe \\<hostname>:<port>\<adam container dn> /I:T /G
   <user/group/role DN>:GR
   ```

3. Execute the following command to give users **Create Child** and **Write Self** permissions to the `People` container and its sub-objects:

   ```
   dsacls.exe \\<hostname>:<port>\<adam container dn> /I:T /G
   <user/group/role DN>:CCWS
   ```

2.17.5.12 OmniKey Proximity Card Reader Technical Note

When using the OmniKey family proximity card readers, it is recommended that the driver be installed through Windows updates.

2.17.5.13 Proximity Card Authenticator Settings

The proximity card authenticator settings are used for configuring proximity card authentication. Also see Proximity Cards in the Strong Authenticators section for configuration with Kiosk Manager and technical notes.

2.17.5.13.1 Options

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Card family `AUI\ProxCardAuth: ProximityCardFamily`	Specifies the proximity card family type.	0: HID ISO / DUO PROX (Default) 1: iClass 2: Indala / EM	Yes	dword/Ø
Reader type `AUI\ProxCardAuth: ReaderName`	Specifies the name of the proximity card reader to use.	OMNIKEY CardMan 5x25-CL 0-Omnikey CardMan 5125 (Default) OMNIKEY CardMan 5x21-CL 0-Omnikey CardMan 5121 OMNIKEY CardMan 5x21-CL 0-Omnikey CardMan 5321 No entry-RFIdeas (all readers)	Yes	string/Ø
Second factor authentication `AUI\ProxCardAuth: AuthenticationMethod`	Specifies whether to use the Active Directory password or a user-defined PIN for the second factor in authentication.	0: AD password (Default) 1: User-defined PIN	Yes	dword/Ø

2.17.5.13.2 PIN Settings

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Minimum length `AUI\ProxCardAuth: MinPINLength`	Specifies the minimum length of the user-defined PIN.	Default is 4	Yes	dword/ int
Maximum length `AUI\ProxCardAuth: MaxPINLength`	Specifies the maximum length of the user-defined PIN.	Default is 8	Yes	dword/ int
Maximum retries `AUI\ProxCardAuth: RetryPINCount`	Specifies the number of PIN attempts before the authentication fails.	Default is 3	Yes	dword/ int
Alphanumeric constraints `AUI\ProxCardAuth: Alphabetic Requirements`	Specifies the alphanumeric requirements of the user defined PIN.	1: Numbers only 2: Letters only 3: Numbers and letters (Default)	Yes	dword/Ø

2.17.5.14 RSA SecurID

This section lists steps that you must take to integrate RSA SecurID with Kiosk Manager, and other technical notes about installing and using this authenticator.

2.17.5.14.1 Installing the RSA SecurID Method Before installing the RSA SecurID authentication method, the RSA middleware must be installed and configured. There are two middleware options for the RSA SecurID authenticator:

- **RSA Local Authentication Client (LAC).** If using RSA LAC, you must install the RSA SecurID Logon Method in the Authentication Manager installer.

- **RSA Local Authentication Toolkit (LAT).** If using RSA LAT, you must install the RSA SecurID Logon Method as well as the Local Authentication Toolkit, if not previously installed, in the Authentication Manager installer. Installing RSA LAT will prompt you to reboot your machine so that it can start the service.

After RSA LAT is installed, according to the RSA documentation on LAT, you must perform the following two steps:

1. Get the server.cerfile from your RSA Authentication Manager administrator and place it in the subdirectory of the main installation directory. For example: `C:\Program Files\RSA Security\RSA Authentication Agent\Agenthost Autoreg Utility` directory.

2. Get the `sdconf.rec`file from your Authentication Manager administrator and place it in the `system32` directory.

> **Note:** These notes are stated in the *RSA SecurID Local Authentication Toolkit* document and also mentioned in *RSA Authentication Agent 6.1 for Microsoft Windows Installation and Administration Guide*.

After RSA SecurID is installed, there are no specific settings that must be set in the Administrative Console.

2.17.5.15 Configuring the SoftID Helper

The SoftID Helper is an extension helper that adds SSO support for SecurID applications. This section describes how to install and configure the SoftID helper and enable RSA SecurID application templates.

2.17.5.15.1 Prerequisites Logon Manager supports the following combinations of software and hardware tokens for SoftID applications:

■ RSA SecurID Software Tokens

■ RSA Authentication Client and RSA SecurID SID800 Hardware Authenticator

■ Both software and hardware tokens. If both are installed on the machine, Authentication Manager looks for the hardware token first, and if it cannot find the hardware token, it defaults to the software token.

One of the above combinations must be installed before installing and using the SoftID Helper.

2.17.5.15.2 Install Logon Manager Install Logon Manager with Authentication Manager and Authentication Manager with the SoftID helper. See the *Oracle Enterprise Single Sign-On Suite Installation Guide* for more information.

2.17.5.15.3 Configuring RSA SecurID Application Templates This example walks through setting up a new RSA SecurID application for an application called **Login Tester**.

1. Open the Administrative Console.

2. Launch the application for which you are defining a template.

3. Right-click **Applications** and select **New Windows Application**. The **Add Application** dialog appears.

Please select the application to add.

4. Enter the application Name and check the **RSA SecurID** check box. Click **Finish**. The Form Wizard appears.

5. Select the **SecurID Login** button. Click **Next**. If the application for which you are defining a template is running, the window title will appear in the next wizard panel.

6. Select the Window Title for your application. Click **Next**.
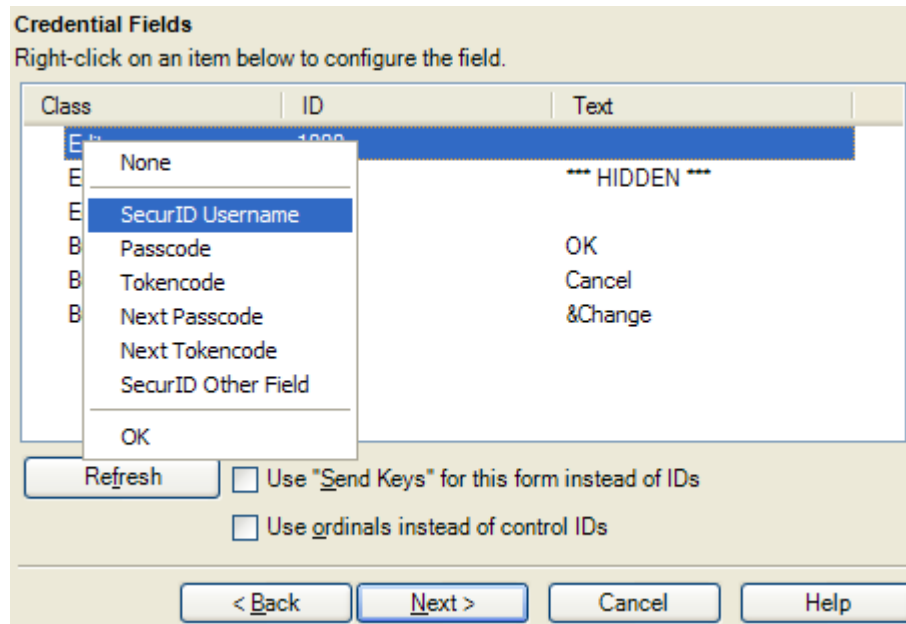
7. On this dialog, you configure the SecurID Username, Passcode, and OK button fields as well as any other applicable fields for your application. Right-click on the class and select the fields. Click the **Help** button for more information on configuring the credential fields. Click **Next** when you are done. A **Summary** panel appears.
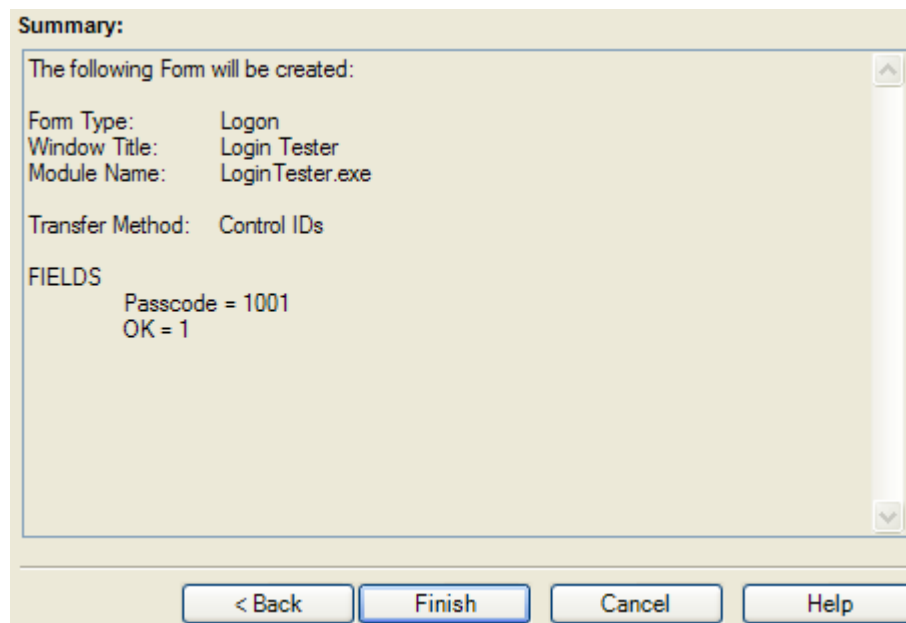
8. Review the summary. Click **Finish** when done.

9. The Windows Logon Form appears. Change any other applicable settings and click **OK**.

10. Export the template to the Agent. See Publish to Repository for more information on exporting applications.

11. When the Agent launches, the user will go through the FTU Wizard. They must select Authentication Manager as the primary logon method.

12. When the application for which you defined a template launches, the Agent will first ask the user if they want to add credentials for the application. If the user selects **Yes**, the Agent will prompt the user to enter their credentials into the New Logon for this application.

13. The user must enter the User ID, PIN and select the Software Token. The user's PIN is set up through the RSA middleware prior to use with Authentication Manager. Authentication Manager automatically populates the Software Token field as it detects the serial number of the available token.

14. Click **Finish** when done. The Agent will log the user onto the RSA SecurID application every time the application is started.

2.17.5.16 First-Time-Use Scenarios

In the setup phase, the user will go through the normal Logon Manager First-Time-Use (FTU) wizard until the **Select Primary Logon Method** dialog is displayed.

The behavior of this setup wizard is configured through the Administrative Console.

Setup Flow Example

1. The first dialog in the Setup Wizard lists the setup tasks necessary for the local installation of Logon Manager. Click **Next** to begin setup.
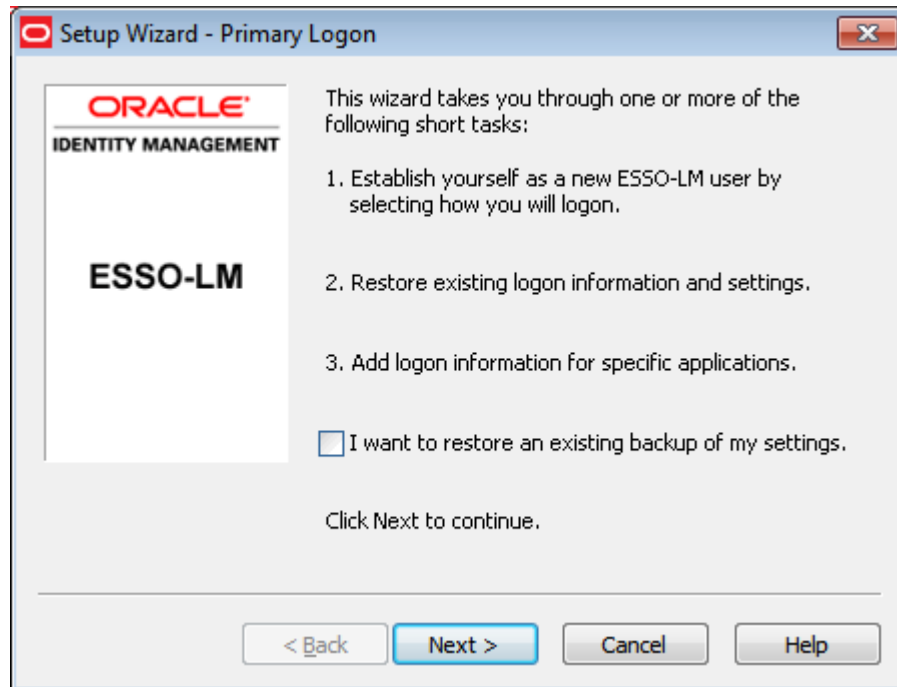
2. The dialog lists the setup tasks necessary for your local installation of Logon Manager, choosing your primary logon method and supplying the credentials for that method. Click **Next**.

3. The Primary Logon dialog prompts you to select a logon method. Select your desired primary logon method. Only methods that are currently installed will appear in the drop-down box. Click **Next**.
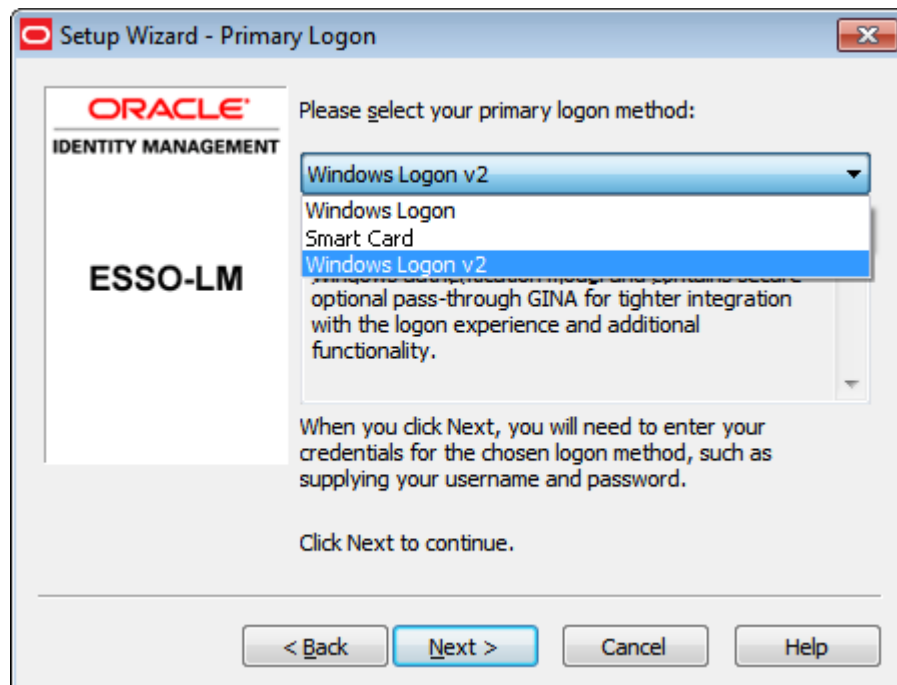
4. Enroll in your selected primary logon method. For example, if a smart card authenticator is installed, you will see the dialog below. Clicking **Cancel** for a required authenticator cancels the Setup Wizard.
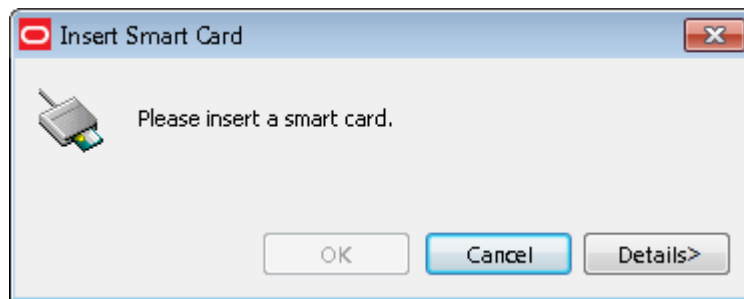
5. Insert your smart card. You are prompted to enter your PIN. Enter it and click **OK**. A message indicating enrollment success appears. Click **OK**.

6. If the passphrase option is enabled, you might be prompted to enter a passphrase with a minimum answer length of eight characters. Enter an answer, confirm (re-enter) it, and click **OK**.

7. The Setup Wizard indicates that the process is complete and Logon Manager is ready for use. Click **Finish** to complete.

2.17.5.17 Integrating with Kiosk Manager

When using the RSA SecurID authenticator with Kiosk Manager, you have to enable and configure Secure Data Storage in the Administrative Console.

RSA SecurID authenticator uses the user's PIN rather than the repository password for the pre-population of the synchronization dialog. Secure Data Storage is used to securely save the PIN which then is associated with the repository credentials on the server. See the Secure Data Storage section to set it up.

2.17.5.17.1 Support for storing and passing through the synchronization credentials with Kiosk Manager and RSA SecurID integration: When using the RSA SecurID authenticator with Kiosk Manager, the user's synchronization credentials can optionally be stored by the authenticator by configuring the Secure Data Storage feature. If stored in this manner, the credentials are then silently passed through to Logon Manager after a user initiates a Kiosk Manager session with an RSA SecurID token. This feature prevents a double authentication when starting a Kiosk Manager session whereby the user authenticates with a PIN and Tokencode and then is subsequently prompted by Logon Manager to provide a synchronization username and password.

2.17.5.18 Microsoft Visual C++ Technical Note

Microsoft Visual C++ 2005 Redistributable Package (x86) is required for the RSA SecurID authenticator. This can be downloaded from Microsoft's web site: http://www.microsoft.com/Downloads/details.aspx?FamilyID=32bc1bee-a3f9-4c13-9c99-220b62a191ee&displaylang=en.

2.17.5.19 PIN Mode Support Technical Note

Due to an incompatibility between RSA Local Authentication Toolkit and Visual Studio 2005, the RSA SecurID authenticator does not support New PIN Mode for SID700 and SID800. A support case has been opened with RSA (# C0842539).

2.17.5.20 Secure Data Storage

Secure data storage settings control the location for data storage. Secure data storage can be used for:

■ The RSA SecurID authenticator in a Kiosk Manager environment.

- The Proximity Card authenticator in a Kiosk Manager environment when using "User Defined PIN" as second factor authentication.

- The Read-Only Smart Card authenticator in a Kiosk Manager environment.

> **Note:** Secure Data Storage is supported for Active Directory, AD LDS (ADAM), and Oracle Internet Directory.

When using Secure Data Storage, you must log on to Windows using a domain user account.

To access the secure data storage settings, click **Global Agent Settings > Live > Authentication > Secure Data Storage**. See the Secure Data Storage section for a full discussion of these settings.

2.17.5.21 Enabling Secure Data Storage

Regardless of your repository, start the procedure for enabling secure data storage as follows:

1. On the **Secure Data Storage** pane, set Enable Data Storage to **Yes**.

2. Create a new Organizational Unit that will serve as the data storage location.

3. Specify the fully-qualified distinguished name for this object as the value of the **Data storage location** setting.

4. Continue to the next steps below for the appropriate repository.

5. Grant control:

   - **For Active Directory**

     a. Grant **FULL CONTROL** permission to this Organizational Unit to **Everyone**.

     b. Apply this to **This object and all child objects**.
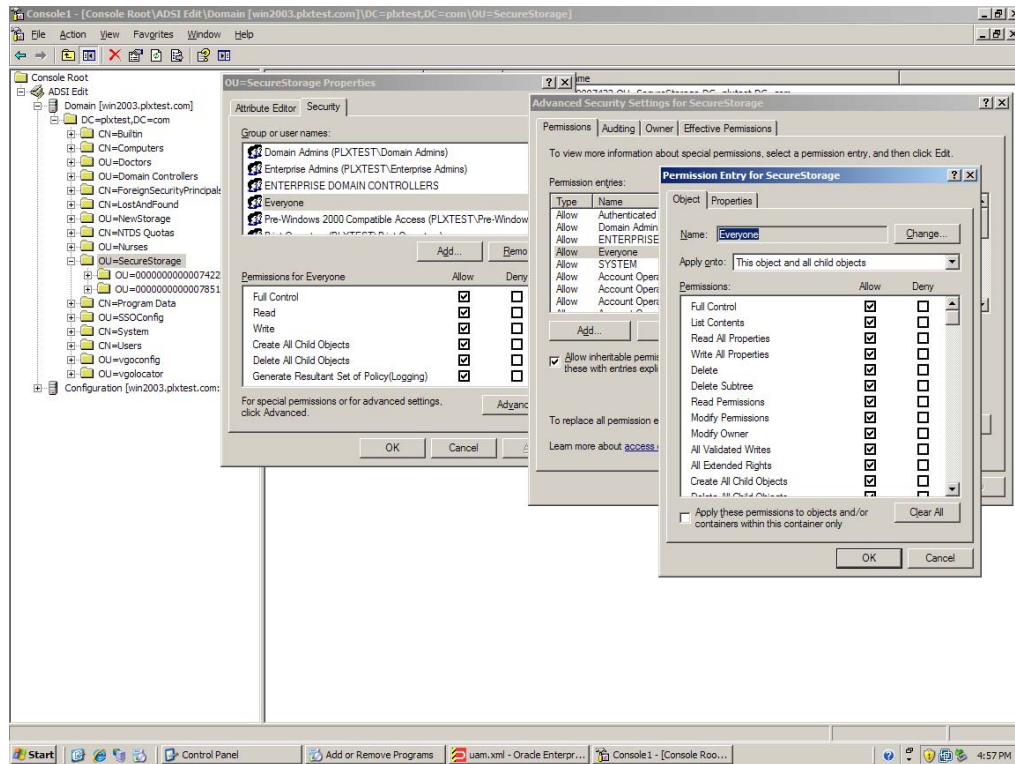
- **For AD LDS (ADAM)**

  Grant General Access (GA) permission to this Organizational Unit and its sub-objects for Everyone: `:dsacls.exe \\<hostname>:<port>\<adam container dn> /I:T /G "Everyone":GA`

- **For Oracle Internet Directory**

  a. Grant anonymous users access to the Secure Data Storage container.

  b. Log on to the Directory Services Manager as an administrator.

  c. Select the **Data Browser** tab.

  d. In the tree, navigate to and select the **Secure Data Storage** container that you created.

  e. Select the **Subtree Access** tab.

  f. Create a new access entry under Structural Access Control and Content Access Control. Accept the default permissions and click **OK**.

  g. Apply the changes. The default permissions grant **Everyone** with bind mode **None** the appropriate access:
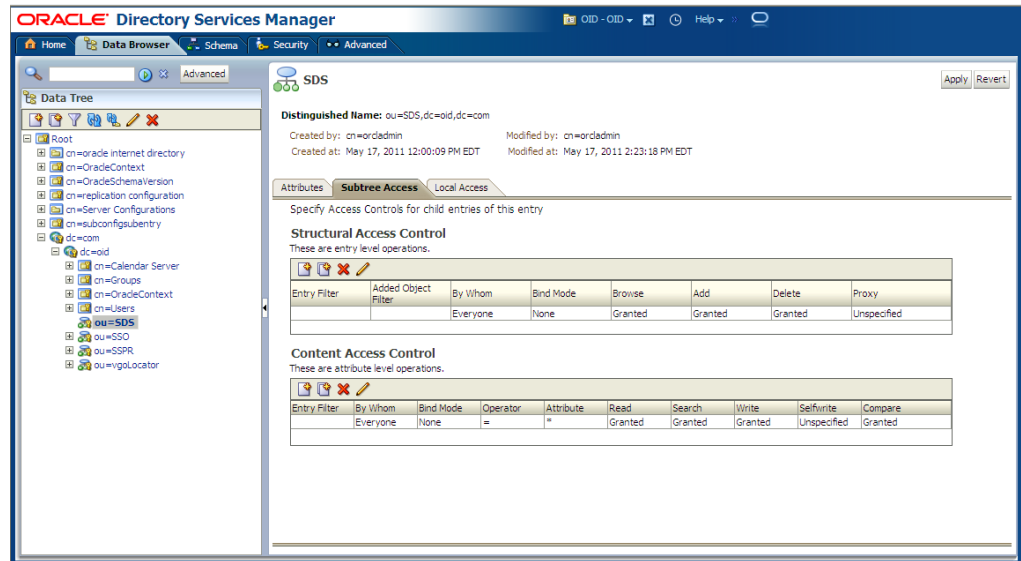
2.17.5.22 Secure Data Storage Authenticator Settings

These settings are used for configuring secure data storage.

Display Name/ Registry Path	Description Text	Options/ Default	Overridable	RegType/ DataType
Enable data storage DataStorage:Passlogix SecureDataStorage	Specifies whether to store users' synchronization credentials securely within the repository.	0: No (Default) 1: Yes	Yes	dword/Ø
Data storage location SecureDataStorage: LocationDN	Enter the fully-qualified path to the location in the repository where the data will be stored.		Yes	string/ string

2.17.5.23 Kiosk Manager Integration Notes

The following notes explain special considerations when integrating Secure Data Storage with Kiosk Manager.

2.17.5.23.1   Domain Password Change This issue occurs when using proximity devices, smart cards, and read only smart cards.

If a user's domain password is changed, the next time the user tries to start a session on a kiosk with the device within the lifetime period of the old password, depending on their sync repository, the following occurs:

- **Active Directory:** This error message displays: "Unable to connect to network…".

- **AD LDS (ADAM):** Kiosk Manager stops responding and requires a restart.

There are two workarounds to this issue:

- Users can manually start a Kiosk Manager session by authenticating with a username and new password within the password lifetime period.

- Administrators can change the lifetime period of an old password to decrease the probability that this issue will occur. Refer to Microsoft Help and Support for more details: http://support.microsoft.com/kb/906305.

2.17.5.23.2 Hardware Reassignment If a hardware device, such as a smart card, is ever reassigned to another user, it is possible that Kiosk Manager will log on as the original user. This occurs because Kiosk Manager keeps a device-to-username mapping.

There is no workaround for this issue. It is strongly recommended that these devices not be reassigned to avoid this issue.

2.17.6 Provisioning Gateway Server Locations

Use this tab to specify the location(s) of Provisioning Gateway Servers.

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
PG Server locations `Extensions\ProvManage r:PMLocationN`	Click the ellipsis ("...") button and enter the URL(s) for the Provisioning Gateway Server(s). For example: `http://localhost/v-GO PM Service` There is no default for this setting.		Yes	string/Ø
Request timeout `Extensions\ProvManage r:Timeout`	Specifies how long (in milliseconds) to wait for a response from the Provisioning Gateway Server This setting is not required.	60000 (Default)	Yes	dword/int

2.17.6.1 Delegated Credentials Settings

Use these settings to specify the server(s) and encryption for delegated credentials.

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
PM Locations `Extensions\ProvManage r\Plugins\ Delegate\PMLocations: PMLocationN`	Click the ellipsis ("...") button and enter the path, or list of paths, to the provisioning service. Enter one path per line. For example: `http://localhost/v-GO PM Service`		Yes	string
Encryption algorithm `Extensions\ EventManager:Retry`	Select the default encryption algorithm from the dropdown menu. **Note:** All algorithms except AES 256 have been deprecated as of version 11.1.2 and are listed for upgrade scenarios only. Do not select other algorithms for new configurations. This setting is not required.	AES 256 (Default) Triple DES (deprecated)	Yes	dword

2.17.6.2 Privileged Accounts Settings

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Allow password reveal
 	
 `EExtensions\OpamManag er:`
 	
 `RevealPasswordMode`
	Specifies whether the user is permitted to reveal the masked fields of checked out accounts.	0-Do not allow reveal (default)
		
		 1-Use application template setting.
			Yes	dword/Ø

Validate account status before each use
 	
 `Extensions\OpamManage r:`
 	
 `MustBeOnline`
	Specifies when the account status check should occur.
	
	 When set to "Before every use," a check is made when the user attempts to use a checked-out account (logon or reveal password). The OPAM Client will check to make sure that the Provisioning Gateway Server is reachable and that the account has not been checked in.
		0-During synchronization only (default)
		
		 1-Before every use
			Yes	dword/Ø

2.17.7 Synchronization Settings

The Synchronization settings are the general options for credential synchronization for all synchronizer extensions. Use these settings to control the following functions and features:

- Performance

- User Mobility

- Security and Management

2.17.7.1 Manage Synchronizers Dialog

The Synchronizers dialog displays the current set of available synchronizers and the order by which the Agent searches them.

To change the search order:

- Select a synchronizer and click the up or down buttons to reposition it.

To add a synchronizer:

- Click **Add**. The **Add Synchronizer** dialog appears.

To display this dialog:

- Select a set of Global Agent Settings.

- Do one of the following:

- Right-click **Synchronization** and choose **Manage Synchronizers** from the shortcut menu.

or

- Choose **Sync Extension** from the **Insert** menu.

2.17.7.2 Add Synchronizer Dialog

Use the **Add Synchronizer** dialog to include a synchronizer in the Agent's search list.

- Enter a Name for the new synchronizer.

- Select a Sync Type from the list.

- Click **OK** to add the synchronizer and return to the **Manage Synchronizers** dialog.

To display this dialog:

- Select a set of Global Agent Settings.

- Do one of the following:

- Right-click **Synchronization** and select **Manage Synchronizers** from the shortcut menu.

or

- Choose **Synchronizer** from the **Insert** menu.

- Click **Add**. The **Add Synchronizer** dialog displays.

2.17.7.3 Using the Edit List Dialog for Synchronizer Settings

The **Edit List** dialog displays when you click the ellipsis ("**…**") button for various synchronizer settings, as listed in the following table. Use this dialog to enter items described in the window title bar (for example, Servers).

- Type one item for each line. Press **Enter** at the end of each line. Do not use any other delimiter characters.

- Click **OK** when finished.

Use this dialog with the following Global Agent Settings:

Synchronizer	Setting
LDAP Synchronizer	`UserPaths`
LDAP Synchronizer Servers	`Servers`
LDAP Authenticator Servers	`Servers`
Active Directory Synchronizer	`UserPaths`
Active Directory Synchronizer Servers	`Servers`
Database Synchronizer Servers	`Servers`
Oracle Access Manager Endpoints Entry	`URLs`
Shell Tasks	`Deletion Tasks`
	`PreTasks`
	`RefreshTasks`
	`StartupTasks`

2.17.7.4 General Synchronization Options

Use this screen to configure non-synchronizer-specific settings.

2.17.7.4.1 Options

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Synchronizer order `Extensions\ SyncManager: SyncOrder`	Specifies the order of synchronization extensions to use. If no value is specified, all extensions are used (in an unpredictable order). For reads, the first operational synchronizer is authoritative, and no other synchronizer is queried. For writes, all synchronizers are updated, in the order specified in this setting. **Examples:** LDAPExt, ADExt, FileSync Remote, AD, FileSync Local, SmartCard, MySmartCard, ADExt, ADExtRemote		Yes	string/ synchroni zer
Use configuration objects `Extensions\ SyncManager: RetrieveCO`	When this setting is disabled, all templates and policies are consolidated into one of two objects: CN=vgoentlist and CN=vgoadminoverride. When this setting is enabled, all template and policies are independent objects for directory-based synchronizers. In this mode, additional features are available, including role/group security and directory hierarchy support.	0: No (Default) 1: Yes	Yes	dword/Ø
Allow disconnected operation `Extensions\ SyncManager: AllowDisconnected`	Specifies whether the offline cache is usable or the First-Time-Use Wizard executes when the Agent is unable to connect to any synchronizer repository. If this setting is disabled, and the repository is not available, the Agent shuts down.	0: No 1: Yes (Default)	Yes	dword/Ø

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Delete local cache `Shell: CleanupOnShutdown`	Specifies whether to delete the user's data files and registry keys upon shutdown of the Agent.	0: No (Default) 1: Yes	Yes	dword/Ø
Deleted credential cleanup `Shell:nDelDays`	Length of time (in days) for which a credential's "deleted" flag is retained after a credential is deleted. Used to ensure that the credential is deleted from all of a user's local caches on multiple systems.	(Default: 30)	Yes	dword/ int
Location of entlist.ini file `Extensions\ AccessManager: EntList`	Enter the fully-qualified path and filename to the `entlist.ini` file. Only applicable in standalone (no synchronizer) mode. This setting should be used only to deploy Administrative Console templates locally to the workstation when synchronization is not installed. The setting should NOT be used when synchronization is installed and application templates are deployed via a repository such as Active Directory. See Creating and Using Templates for more information.		Yes	string/ filename

2.17.7.4.2 Behavior

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Wait for synchronization at startup `Extensions\ SyncManager: WaitForStartupSync`	Specifies whether to wait for synchronization at startup, which ensures that the user's data is current, and new templates and policies are put into effect before Logon Manager logs on to applications. **Note:** With this setting enabled, Logon Manager does not respond until the synchronization is complete. Synchronization times vary based on your synchronization infrastructure and the number of templates and policies in the repository.	0: No 1: Yes (Default)	Yes	dword/Ø
Interval for automatic resynchronization `Extensions\ SyncManager: CycleInterval`	Interval (in minutes) between automatic resynchronizations. This synchronization interval is not reset if a manual, user-generated sync event (such as an Logon Manager refresh) takes place. A value of zero (0) disables this setting, which means that synchronization occurs only during normal sync events such as Logon Manager startup or user credential update. Generally set when Provisioning Gateway is in use, to ensure that updates are delivered in a timely manner.	(Default: 0)	Yes	dword/ int
Optimize synchronization `Extensions\ SyncManager: OptimizedSync`	With this setting enabled, the synchronization function uses a checksum object called SyncState to determine changed credentials, rather than retrieving all credentials. Changed credentials are then independently synchronized without synchronizing all credentials. Note that templates and policies are always synchronized in full during each sync event.	0: No 1: Yes (Default)	Yes	dword/Ø

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Use aggressive synchronization Extensions\ SyncManager: AggressiveSync	With this setting enabled, each time Logon Manager detects a logon event, a synchronization occurs before the target application credential is decrypted and passed to the application. This feature ensures that the most current credentials or settings are used at all times. The feature is normally only used in special cases where a user uses multiple systems to simultaneously access the same application (such as through a Citrix farm). **Note:** This feature can have a significant performance impact on both client and server computers.	0: No (Default) 1: Yes	Yes	dword/Ø
Resynchronize when network or connection status changes Shell:MonitorNetwork	Enables or disables monitoring for changes in the network connection status. Enabling this setting causes the Agent to perform resynchronization when a status change occurs (for example, reconnecting to the network).	0: No (Default) 1: Yes	Yes	dword/Ø

2.17.7.5 Active Directory Synchronization Settings

Use these settings to configure a Microsoft Active Directory (AD) synchronization.

Note: If users will be synchronizing with an Active Directory or AD LDS (ADAM) repository from outside of the corporate network, you must allow RPC protocol-based connections through the corporate firewall; otherwise, users will be unable to synchronize with the repository.

2.17.7.5.1 Synchronizer location

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
AD Sync DLL location Extensions\ SyncManager\ Syncs\%AD%:Path	Enter the path\filename of the Active Directory synchronizer extension.	Default: %INSTALLDIR% Plugin\SyncMgr\ ADEXT\adsync.dll	No	string/ filename

2.17.7.5.2 Data storage configuration

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Base location(s) for configuration objects Extensions\ SyncManager\ Syncs\%AD%\ COBaseLocations: LocationN	Specifies where to begin the search for Configuration Objects (templates and policies). This is a fully-qualified, distinguished path, such as: OU=SSOConfig,DC=Domain,DC=com The search starts from the specified location(s) and searches all subordinate OUs (if any) for Configuration Objects. To specify multiple locations, place one entry on each line.		No	string/ Ø
Location for storing user credentials Extensions\ SyncManager\ Syncs\%AD%: LocateInUser	Credentials can be stored either as objects subordinate to the Active Directory user object, or as specified by an Oracle locator object.	0: As specified by locator object (Default) 1: Under respective directory user objects	Yes	dword/Ø

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Prepend Domain when naming objects
 	
`Extensions\`
`SyncManager\`
`Syncs\%AD%:`
`AppendDomain`
	Enables prepending the user's Domain to the username in naming the user's container.
	
	Example:
	
	For the Domain "company" and user "jamesk" the container is named "jamesk" with this flag disabled and "company.jamesk" with this flag enabled.
	
	Note: If you enable this setting, do not select to enable storing credentials under User Object (in the Directory menu). If you enable credential storage in User Objects, you must disable this option (the default setting). If you enable both options, synchronization does not occur.
		0: No (Default)
		1: Yes
			Yes	dword/Ø

Base location(s) for UAM storage index
 	
`Extensions\`
`SyncManager\Syncs\%AD\`
`IndexBaseLocations:`
`LocationN`
	Fully qualified DN of the Universal Authentication Manager index container.		No	string/Ø

Use secure location for storing user settings
 	
`Extensions\`
`SyncManager\Syncs\%AD%`
`:UseSecureLocation`
`ForUserRegistry`
	Set to **Yes** if you want the synchronizer to use a secure location for storing user registry settings in Active Directory.
	
	Set to **No** only for the duration of the Logon Manager client's upgrade period for backward compatibility with Logon Manager versions prior to 11.1.2.
	
	Note: You should not select **Yes** for this setting until you have upgraded all Logon Manager clients to version 11.1.2.
	
	You must select **Yes** for this setting under the following conditions:
	
	■ If version 11.1.2 is your first installation of Logon Manager.
	
	■ After you have upgraded all Logon Manager clients to version 11.1.2, and before upgrading to versions beyond 11.1.2.
		0: No (Default)
		1: Yes (recommended)
			Yes	dword/Ø

2.17.7.5.3 Connection information

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Credentials to use
 	
`Extensions\`
`SyncManager\`
`Syncs\%AD%:AuthType`
	Specifies which credentials to use when authenticating to the Active Directory Server.	0: Use local computer credentials only	Yes	dword/Ø

		1: Use Active Directory server account only (recommended that UserPathN be set)		
		2: Try local computer credentials; if it fails, use Active Directory server account (Default)		
		3: Use card's certificate. Use this setting to allow users to authenticate to the repository using a smart card's certificate and their PIN instead of a username and password.		
		4: Try card's certificate; if logon is canceled, use Active Directory server account.		

Prompt when disconnected
 	
`Extensions\`
`SyncManager\`
`Syncs\%AD%:`
`AllowOffline`
	Allows the user to work offline without prompting/notification if a synchronization event fails.	0: No
		
		1: Yes (Default)
			Yes	dword/Ø

Servers
 	
`Extensions\`
`SyncManager\`
`Syncs\%AD%\Servers:`
`ServerN`
	Servers to try, in the format *computer[:port]* (one server per line), where *computer* is the server name, and *port* is assumed to be the default (636 for SSL, 389 for no SSL) if not specified.
	
	Example:
	
	`DC1.company.com`
	
	`DC2.company.com`
	
	`company.com:8080`
	
	`companylab.com`
	
	Note: This setting is not normally used when storing Oracle data in Active Directory.
	
	Active Directory requires use of computer names (not IP addresses).
			No	string/Ø

User Paths
 	
`Extensions\`
`SyncManager\`
`Syncs\%AD%:UserPathN`
	Enter the fully-qualified path to where the user account is located. There can be unlimited paths to search. The extension searches these in order, looking for the user account. If not found, the extension will search the directory tree.
	
	Note: This entry is not required for this extension.
			Yes	string/Ø

Use SSL
 	
`Extensions\`
`SyncManager\`
`Syncs\%AD%:UseSSL`
	Specifies to connect via SSL.	0: No (insecure) (default to port #389)
		
		1: Yes (default to port #636) (Default)
			Yes	dword/Ø

Logon attempts
 	
`Extensions\`
`SyncManager\`
`Syncs\%AD%:`
`RetryLockCount`
	Specifies the number of times to present the Synchronization dialog to the user. For example, if you set this value to 3, the Synchronization dialog displays a maximum of three times if the user submits incorrect credentials.	Default: 3	Yes	dword/ int

2.17.7.5.4 User interface

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Descriptive name Extensions\ SyncManager\ Syncs\%AD%: DisplayName	Enter a logon dialog title to differentiate between multiple synchronizer extensions having the same name. **Note:** This entry is not required.		Yes	string/ string
Password change window title Extensions\ SyncManager\ Syncs\%AD%:CAP_ WindowTitle	Use this setting to customize the Active Directory Change Password window title name for this synchronizer. **Note:** This entry is not required.		Yes	string/ string
Password change window subtitle Extensions\ SyncManager\ Syncs\%AD%:CAP_ WindowSubTitle	Use this setting to customize the Active Directory Change Password window subtitle name for this synchronizer. **Note:** This entry is not required.		Yes	string/ string

2.17.7.5.5 Credential sharing

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Share credentials with authenticators Extensions\ SyncManager\ Syncs\%AD%: ShareCredsToAuths	This setting eliminates double authentication by linking authenticator and synchronizer credentials. If authenticators and synchronizers use the same credentials, the duplicate credentials are used without requiring the user to reenter them. Enter a comma-separated list of authenticators with which to share the credentials, for example WinAuth, MSAuth. **Note:** To locate other authenticator names, see the name listed in the registry for that authenticator (located under HKLM\Software\Passlogix\AUI).		Yes	string/ string

2.17.7.5.6 File mode configuration

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Limit search to server root Extensions\ SyncManager\ Syncs\%AD%:StopAtRoot	Specifies how the Agent searches for locator and override objects.	0: No 1: Yes (Default)	Yes	dword/Ø

2.17.7.6 AD LDS (ADAM) Synchronization Settings

Use these settings to configure an AD LDS (ADAM) synchronization.

> **Note:** If users will be synchronizing with an Active Directory or AD LDS (ADAM) repository from outside of the corporate network, you must allow RPC protocol-based connections through the corporate firewall; otherwise, users will be unable to synchronize with the repository.

Configuring the Agent with Global Agent Settings

2.17.7.6.1 Synchronization location

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

ADAM Sync DLL location
 	
`Extensions\`
`SyncManager\`
`Syncs\%ADAM%:Path`
	Enter the path\filename of the AD LDS (ADAM) synchronizer extension.	Default:
		`%INSTALLDIR%Plugin\`
		`SyncMgr\ ADAMext\`
		`ADAMsyncExt.dll`
			No	string/ filename

2.17.7.6.2 Data storage configuration

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Base location(s) for configuration objects
 	
`Extensions\`
`SyncManager\`
`Syncs\%ADAM%\`
`COBaseLocations:`
`LocationN`
	Specifies where to begin the search for Configuration Objects (templates and policies). This is a fully-qualified, distinguished path, such as:
	
	`OU=SSOConfig,DC=Domain,DC=com`
	
	The search starts from the specified location(s) and searches all subordinate `OU`s (if any) for Configuration Objects. To specify multiple locations, place one entry on each line.
			No	string/Ø

Prepend Domain when naming objects
 	
`Extensions\`
`SyncManager\`
`Syncs\%ADAM%:`
`AppendDomain`
	Enables prepending of the user's Domain to the username in naming the user's container.
	
	Example:
	
	For the Domain "`company`" and user "`jamesk`" the container is named "`jamesk`" with this flag disabled and "`company.jamesk`" with this flag enabled.
		0: No (Default)
		1: Yes
			Yes	dword/Ø

User Domain name to use
 	
`Extensions\`
`SyncManager\`
`Syncs\%ADAM%:`
`UserDomain`
	Specifies the domain name to use in the container name (for example, `DomainName.UserName`) when you enable the **Prepend Domain** setting. The user can specify another domain the in the logon dialog.
	
	`Example:`
	
	If User Domain is "`MyDomain`" (with Prepend Domain enabled) and the user logs on as jamesk, the container name used is `MYDOMAIN.jamesk`. If the user logs on as `HISDOMAIN\jamesk` the container name used is `HISDOMAIN.jamesk`.
			Yes	string/ string

2.17.7.6.3 Connection information

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Credentials to use
 	
`Extensions\`
`SyncManager\`
`Syncs\%ADAM%:AuthType`
	Specifies which credentials to use when authenticating to the AD LDS (ADAM) server.	0: Local computer credentials
		
		1: ADAM server account
		
		2: Try local computer credentials before using ADAM server account (Default)
		
		3: Use card's certificate. Use this setting to allow users to authenticate to the repository using a smart card's certificate and their PIN instead of a username and password.
		
		4: Try card's certificate; if logon is canceled, use ADAM server account.
			Yes	dword/Ø

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Prompt when disconnected Extensions\ SyncManager\ Syncs\%ADAM%: AllowOffline	Allows the user to work offline without prompting/notification if a synchronization event fails.	0: Yes 1: No (Default)	Yes	dword/Ø
Servers Extensions\ SyncManager\ Syncs\%ADAM%\ Servers:ServerN	Specifies the servers to try, in the format *computer[:port]* (one server per line), where *computer* is the server name, and *port* is assumed to be the default (636 for SSL, 389 for no SSL) if not specified. Examples: Adam1.company.com Adam2.company.com Adam3.company.com:50389		No	string/ string
Use SSL Extensions\ SyncManager\ Syncs\%ADAM%:UseSSL	Specifies to connect via SSL.	0: No (insecure) (default to port #389) 1: Yes (default to port #636) (Default)	Yes	dword/Ø

2.17.7.6.4 User interface

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Descriptive name Extensions\ SyncManager\ Syncs\%ADAM%: DisplayName	Specify a logon dialog title to differentiate among multiple synchronizer extensions having the same name. **Note:** This entry is not required.		Yes	string/ string
Password change window title Extensions\ SyncManager\ Syncs\%ADAM%: CAP_WindowTitle	Use this setting to customize the AD LDS (ADAM) Change Password window title name for this synchronizer. **Note:** This entry is not required.		Yes	string/ string
Password change window subtitle Extensions\ SyncManager\ Syncs\%ADAM%: CAP_WindowSubTitle	Use this setting to customize the AD LDS (ADAM) Change Password window subtitle name for this synchronizer. **Note:** This entry is not required.		Yes	string/ string

2.17.7.6.5 Credential sharing

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Share credentials with authenticators Extensions\ SyncManager\ Syncs\%ADAM%: ShareCredsToAuths	This setting eliminates double authentication by linking authenticator and synchronizer credentials. If authenticators and synchronizers use the same credentials, the duplicate credentials are used without requiring the user to reenter them. Enter a comma-separated list of authenticators with which to share the credentials, for example WinAuth, MSAuth. **Note:** To locate other authenticator names, see the name listed in the registry for that authenticator (located under HKLM\Software\Passlogix\AUI).		Yes	string/ string

2.17.7.7 Database Synchronization Settings

Use these settings to configure database synchronization.

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

DB Sync DLL location
 	
`Extensions\`
`SyncManager\`
`Syncs\%DB%:Path`
	Enter the path\filename of the Database synchronizer extension.	Default: `%INSTALLDIR%`
		`Plugin\ SyncMgr\`
		`DBEXT\ DBExt.dll`
			No	string/ string

Servers
 	
`Extensions\`
`SyncManager\`
`Syncs\%DB%\Servers:`
`Server`
	Specifies the database servers and the order to attempt connection for synchronization. Select the checkbox and click the ellipsis "**…**" button to open the "Edit List" dialog. Enter the full connection address (`computerName.dbServerName`) for one database server on each line; end each line by pressing Enter. Do not use any other delimiter characters.
	
	You must specify at least one server for the extension to work.
	
	For Oracle
	
	To connect to an Oracle database, use the following connection string:
	
	`Provider=OraOLEDB.Oracle;`*`Data`*
	`Source=%MachineName%``;Extended`
	`Properties='OSAuthent=1'`
	
	where the *`Data Source`* value will be different for each configuration.
	
	To connect to the Oracle database, the Oracle client must be installed on the same machine as the Administrative Console.
	
	For SQL Server
	
	To connect to a SQL Server that is hosting multiple instances, use the following connection string (with no manual line break):
	
	`Provider=SQLOLEDB; Data`
	`Source="ServerName\Instance"; Initial`
	`Catalog="DatabaseName" Trusted_`
	`Connection=Yes; Use Encryption for`
	`Data=True;`
			No	string/ string

Append Domain when naming objects
 	
`Extensions\`
`SyncManager\`
`Syncs\%DB%:`
`AppendDomain`
	Enables appending the user's Domain to the username in naming the user's container.
	
	Example:
	
	For the Domain "`company`" and user "`jamesk`" the container is named "`jamesk`" with this flag disabled and "`jamesk.company`" with this flag enabled.
		0: No (Default)
		1: Yes
			Yes	dword/Ø

2.17.7.8 File System Synchronization Settings

Use these settings to configure a File System synchronization.

2.17.7.8.1 Synchronizer location

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

File Sync DLL location
 	
`Extensions\`
`SyncManager\`
`Syncs\%File%:Path`
	Enter the `path\filename` of the File System synchronizer extension.	Default: `%INSTALLDIR%`
		`Plugin\ SyncMgr\`
		`FileSyncExt\`
		`filesync.dll`
			No	string/ filename

2.17.7.8.2 Data storage configuration

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Prepend Domain when naming user folders
 	
`Extensions\`
`SyncManager\`
`Syncs\%File%:`
`AppendDomain`
	Enables prepending the user's Domain to the username in naming the user's container.
	
	Example:
	
	For the Domain "`company`" and user "`jamesk`" the container is named "`jamesk`" with this flag disabled and "`company.jamesk`" with this flag enabled.
		0: No
		1: Yes (Default)
			Yes	dword/Ø

2.17.7.8.3 Connection information

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Prompt when disconnected
 	
`Extensions\`
`SyncManager\`
`Syncs\%File%:`
`AllowOffline`
	Allows the user to work offline without prompting/notification if a synchronization event fails.	0: Yes
		1: No (Default)
			Yes	dword/Ø

Server
 	
`Extensions\`
`SyncManager\`
`Syncs\%File%\Servers:`
`Server1`
	Enter the list of UNC paths to try for synchronization. You must specify Server1 for this extension to work.
	
	Examples:
	
	`\\FS1\Users\FS2\ExtrasD:\Backup`
	
	The File System extension requires use of proper UNC paths. Only one path is supported. Failover is not supported.
			Yes	string/ string

Logon attempts
 	
`Extensions\`
`SyncManager\`
`Syncs\%File%:`
`RetryLockCount`
	Specifies the number of times to present the Synchronization dialog to the user. For example, if you set this value to 3, the **Synchronization** dialog displays a maximum of three times if the user submits incorrect credentials.	Minimum value of 1
		Default: 3
			Yes	dword/ int

2.17.7.8.4 User interface

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Descriptive name
 	
`Extensions\`
`SyncManager\`
`Syncs\%File%:`
`DisplayName`
	Specifies a logon dialog title to differentiate among multiple synchronizer extensions having the same name.
	
	Note: This entry is not required.
			Yes	string/ string

2.17.7.9 LDAP Synchronization Settings

The LDAP/IBM Synchronization settings must be set for all LDAP synchronizer extensions.

You can bind to a directory before or after searching for a specific user account. If you choose to search for a user account before binding, Logon Manager begins searching at the user path you specify and continues down the tree until it locates the user account and binds to that directory, or it exhausts all paths. If Logon Manager does not find the user account you specify, the user receives a message that the system has been configured incorrectly and to contact the administrator.

Typically, Logon Manager uses anonymous binding for LDAP directories, but it also allows you to create a browse-only account to search for a user in scenarios where anonymous binding is disabled. In such cases, the account name is not the user's name and therefore is not readily identifiable (for instance, an employee ID or social security

number). The browse-only account facilitates user searches when the alternate user ID option is enabled, identifying the user who belongs to the alternate user ID. Use the Alternate User ID location, BIND User Name, and BIND User Password settings to configure the browse-only account.

2.17.7.9.1   Synchronizer location

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

LDAP Sync DLL location
 	
`Extensions\`
`SyncManager\`
`Syncs\%LDAP%:Path`
	Enter the `path\filename` of the LDAP Directory Server synchronizer extension.	Default:
		`%INSTALLDIR%Plugin\`
		`SyncMgr\ LDAP\`
		`ldapsync.dll`
			No	string/ filename

2.17.7.9.2   Data storage location

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Base location(s) for configuration objects
 	
`Extensions\`
`SyncManager\`
`Syncs\%LDAP%\`
`COBaseLocations:`
`LocationN`
	Specifies where to begin the search for Configuration Objects (templates and policies). This is a fully-qualified, distinguished path, such as:
	
	`OU=SSOConfig,DC=Domain,DC=com`
	
	The search starts from the specified location(s) and searches all subordinate `OU`s (if any) for Configuration Objects. To specify multiple locations, place one entry on each line.
			No	string/Ø

2.17.7.9.3   Connection information

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Prompt when disconnected
 	
`Extensions\`
`SyncManager\`
`Syncs\%LDAP%:`
`AllowOffline`
	Allows the user to work offline without prompting/notification if a synchronization event fails.	0: Yes
		1: No (Default)
			Yes	dword/Ø

Directory type
 	
`Extensions\`
`SyncManager\`
`Syncs\%LDAP%:`
`DirectoryType`
	The specific type of directory server. If the directory server is not listed, select Unspecified LDAP Directory (the default) for backwards compatibility in upgrade scenarios; otherwise select Generic LDAP Directory.	0: Unspecified LDAP Directory (Default)
		3: Novell eDirectory
		5: Generic LDAP Directory
		8: Oracle Directory Server Enterprise Edition
		9: IBM Tivoli Directory Server
		10: Oracle Internet Directory
		11: Siemens DirX Directory Server
			Yes	dword/Ø

Servers
 	
`Extensions\`
`SyncManager\`
`Syncs\%LDAP%\Servers:`
`ServerN`
	Servers to try, in the format `computer[:port]` (one server per line), where `computer` is the server name, and `port` is assumed to be the default (636 for SSL, 389 for no SSL) if not specified.
	
	Example:
	`LDAP1.company.com`
	`LDAP2.company.com`
	`LDAP3.company.com:50389`
			No	string/Ø

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

User paths
 	
`Extensions\`
`SyncManager\`
`Syncs\%LDAP%:`
`UserPathN`
	Enter the fully-qualified (distinguished) path to the location of the user account when LDAP Directory Search is not enabled. There can be unlimited paths to search. The extension searches these in order, looking for the user account. When using LDAP Directory Search, if the user account is not found in the given userpath, the extension searches down the directory tree from that path.
	
	Example:
	
	`OU=Users,DC=Domain,DC=com`
	
	Note: You must specify at least one value for UserPath for this extension to work.
			Yes	string/Ø

Use SSL
 	
`Extensions\`
`SyncManager\`
`Syncs\%LDAP%:UseSSL`
	Specifies to connect via SSL.	0: No (insecure) (default to port #389)
		
		1: Yes (default to port #636) (Default)
			Yes	dword/Ø

2.17.7.9.4 Administrative security

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Administrative group DN
 	
`Extensions\`
`SyncManager\`
`Syncs\%LDAP%:`
`AdminGroup`
	Enter the Distinguished Name for the administrative group. This value is placed in the ACI.
	
	Example:
	
	`cn=configuration administrators,ou=groups,`
	`ou=topologymanagement, o=netscaperoot`
			Yes	string/ string

Security version
 	
`Extensions\`
`SyncManager\`
`Syncs\%LDAP%:`
`SecurityVersion`
	Updates the ACI with a new :AdminGroup value when this value is higher than :SecurityUpgrade.
	
	Use this setting in conjunction with the Administrative Group DN setting to update of the security rights on the people container used by Logon Manager to store LDAP user credentials for deployed environments.
	
	To do this:
	
	1. Provide the new Administrative Group DN to be used for the new security. This is the Distinguished Name of the security group.
	
	2. Set the Security Version to one higher than its current value.
	
	3. Deploy the settings.
	
	The next time Logon Manager performs a synchronization, it updates the security to the new Administrative Group DN and sets its current internal Security Version to the one configured. This forces the security update to run only once.
	
	Note: This setting is not meant to be used as a typical upgrade path for the security change. It is recommended that you use in-place mechanisms that exist for the various servers.
			Yes	dword/ string

2.17.7.9.5 User interface

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Descriptive name
 	
`Extensions\`
`SyncManager\`
`Syncs\%LDAP%:`
`DisplayName`
	Specifies a logon dialog title to differentiate among multiple synchronizer extensions having the same name.
	
	Note: This entry is not required.
			Yes	string/ string

Show user path
 	
`Extensions\`
`SyncManager\`
`Syncs\%LDAP%:`
`ShowUserPath`
	Use this setting to show/hide the User Path combo box control in the LDAP synchronizer authentication dialog.	0: No
		1: Yes (Default)
			Yes	dword/Ø

Logon attempts
 	
`Extensions\`
`SyncManager\`
`Syncs\%LDAP%:`
`RetryLockCount`
	Specifies the number of times to present the Synchronization dialog to the user. For example, if you set this value to 3, the **Synchronization** dialog displays a maximum of three times if the user submits incorrect credentials.	Minimum value of 1
		Default: 3
			Yes	dword/int

2.17.7.9.6 Credential sharing

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Share credentials with authenticators
 	
`Extensions\`
`SyncManager\`
`Syncs\%LDAP%:`
`ShareCredsToAuths`
	This setting eliminates double authentication by linking authenticator and synchronizer credentials. If authenticators and synchronizers use the same credentials, the duplicate credentials are used without requiring the user to reenter them.
	
	Enter a comma-separated list of authenticators with which to share the credentials, for example WinAuth, MSAuth.
	
	Note: To locate other authenticator names, see the name listed in the registry for that authenticator (located under `HKLM\Software\Passlogix\AUI`).
			Yes	string/Ø

2.17.7.10 LDAP Special Purpose Synchronization Settings

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Naming attribute string
 	
`Extensions\`
`SyncManager\`
`Syncs\%LDAP%:`
`UserPrepend`
	String to prepend to User Paths. This is required when the domain name for a user is in the form:
	
	`cn=%UserName%,ou=people,dc=computer;`
	
	instead of the form:
	
	namingattribute=%UserName%,ou=people, dc=computer
	
	(where *namingattribute* can be any string). If needed, set to cn.
	
	Note: Typically, you must set this value to cn for Novell eDirectory.
	
	If you use UserPrepend, you must use User PathN and not use UserLocation.
			Yes	string/ string

BIND timeout
 	
`Extensions\`
`SyncManager\`
`Syncs\%LDAP%:Timeout`
	Enter the length of the timeout (in milliseconds) of the LDAP BIND call.	Default depends on the operating system	Yes	dword/ int

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

BIND user DN
 	
`Extensions\`
`SyncManager\`
`Syncs\%LDAP%:`
`BindUserName`
	Specifies LDAP "browse only" account user DN. This must be in the format:
	
	`uid=%username%, ou=people,`
	`dc=%CompanyName%`
	
	(for example, `uid=jsmith, ou=people,`
	`dc=passlogix, dc=com`).
	
	You must enable anonymous binding on the directory for LDAP Directory Search functionality. If you do not enable anonymous binding, you must use this account to perform the directory search. The search is performed whether using "User Paths" or the "Alternate User ID location."
			Yes	string/ string

BIND user password
 	
`Extensions\`
`SyncManager\`
`Syncs\%LDAP%:`
`BindUserPassword`
	Specifies LDAP "browse only" account user password.
	
	You must enable anonymous binding on the directory for LDAP Directory Search functionality. If you do not enable anonymous binding, you must use this account to perform the directory search. The search is performed whether using "User Paths" or the "Alternate User ID location."
			Yes	string/ Masked String

Alternate user ID location
 	
`Extensions\`
`SyncManager\`
`Syncs\%LDAP%:`
`UserLocation`
	Specifies where to locate a user object when the user validates against an attribute other than the username.
	
	Example:
	
	If users authenticate with an employee ID # for logon (validation against the empid attribute) and the user object is in:
	
	`ou=people,dc=computer`
	
	set UserLocation to
	
	`empid=%USER,ou=people,dc=computer`
	
	instead of to
	
	`uid=user,ou=people,dc=computer`
	
	Note: For Novell eDirectory, UserLocation should be: `uid=%USER,path to the object`.
	
	If using `UserLocation`, do not use `UserPrepend` or `UserPaths`.
			Yes	string/ string

Enable directory search for users
 	
`Extensions\`
`SyncManager\`
`Syncs\%LDAP%:`
`LDAPBindSearch`
	Enables or disables directory search for the user account. When the user account is not found in the given path, the extension will search for it from that location down the directory tree. The search is performed whether using "User Paths" or the "Alternate User ID location."
	
	If you enable this setting and have moved a user to a different OU in the LDAP directory since the last synchronization, the user will receive a prompt for credentials at the next logon.
		0: No (Default)
		
		1: Yes
			Yes	dword/Ø

2.17.7.11 Roaming Profile Synchronization Extension Settings

Note: Roaming Profile is deprecated as of version 11.1.2 and is listed for upgrade scenarios only. Do not use this synchronizer for new configurations.

The Administrative Console uses the Roaming Profile synchronizer to support file system synchronization with roaming profiles. You can use the Roaming Profile synchronizer in deployments that meet the following conditions:

- Users are set up to use roaming profiles on the server.

- The **Delete Local Cache** setting has not been enabled for synchronization.

- You are using v1 Authentication.

If the above conditions exist, set up the roaming profile environment as follows:

1. Set Logon Manager to operate in a multi-sync environment, where one of the sync extensions installed is the roaming sync extension. A multi-sync environment is one in which at least two sync extensions are installed. For example, if you are using AD sync extension, you must install AD sync extension and Roaming profile extension.

2. The Roaming Profile Synchronizer extension must be first in the synchronizer configuration order. To set this order, expand **Global Agent Settings > Live** and click on **Synchronization**. In the **Synchronizer order** field, click the ellipsis "**…**" button. On the Synchronizers panel, make sure that the **Roam** setting is in the top position, and the other synchronizer type (for example, Active Directory) being used is second.

3. You do not need to change any other synchronizer settings when using Roaming Profiles.

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Roaming Sync DLL location
 	
`Extensions\`
`SyncManager\`
`Syncs\%ROAM%:Path`
	Enter the path\filename of the roaming synchronizer extension.	Default: `%INSTALLDIR%`
		`Plugin\ SyncMgr\`
		`RoamExt\`
		`RoamSyncExt.dll`
			No	string/
				filename

2.17.8 Security Settings

The Security settings control the frequency with which end-users must re-enter their primary logon passwords, their ability to view their application logon passwords, and the preferred encryption provider and strength.

2.17.8.1 Security Options

Display Name/ Registry Path	Description	Options/Default	Overridable	RegType/ DataType

Store user data on disk in encrypted file
 	
`Extensions\`
`StorageManager\`
`InMemShr:LocalStorage`
	Specifies to store a copy of user data (for example, credentials) locally in an encrypted database file in each user's `ApplicationData` folder.	0: No
		1: Yes (Default)
			Yes	dword/Ø

Display Name/ Registry Path	Description	Options/Default	Overridable	RegType/ DataType
Default encryption algorithm `CSP:PreferredCSP`	Select the default encryption algorithm from the dropdown menu. **Note:** Non-MS CAPI algorithms have been deprecated and are listed for upgrade scenarios only. Do not select these algorithms.	0: Cobra 128-bit (deprecated) 512: Cobra 128-bit (also) (deprecated) 513: Blowfish 448-bit (deprecated) 1028: Triple-DES 168-bit (deprecated) 1285: AES 256-bit (deprecated) 25700: Triple-DES (MS CAPI) (All OSs) (deprecated) 25723: Triple-DES (MS CAPI) (XP/2003 only) (deprecated) 25956: RC-4 (MS CAPI) (All OSs) (deprecated) 25979: RC-4 (MS CAPI) (XP/2003 only) (deprecated) 26491: AES (MS CAPI) (All OSs) (Default)	Yes	dword/Ø
Reauthentication timer `Extensions\ AccessManager: AutoLogin`	Time (in milliseconds) between reauthentication requests. If set to 4,294,967,295 (0xFFFFFFFF), the time never expires and the user will never need to reauthenticate, except in forced authentication scenarios.	Default for client-side installations: 900000 Default for Terminal Services environments: 4,294,967,295 (disabled)	Yes	dword/int
Require reauthentication before updating account credentials `Extensions\ AccessManager: RequireAuthCred`	Specifies whether the user must enter Logon Manager credentials before changing application credentials, even though the authentication timer has not expired.	0: No (Default) 1: Yes	Yes	dword/Ø

2.17.8.2 Masked fields

Display Name/ Registry Path	Description	Options/Default	Overridable	RegType/ DataType
Obfuscate length `Extensions\ AccessManager: HideMaskedFieldLength`	Specifies whether to display encrypted fields with a string of blank characters different from the length of the obfuscated data.	0: No 1: Yes (Default)	Yes	dword/Ø
Allow revealing `Extensions\ AccessManager: AllowReveal`	Specifies whether the user is permitted to reveal masked fields.	0: No 1: Yes (Default)	Yes	dword/Ø
Require reauthentication to reveal `Extensions\ AccessManager: ReauthOnReveal`	Specifies whether the user must enter Logon Manager credentials in order to reveal masked fields, assuming that you have set "Allowed revealing" to **Yes**.	0: No 1: Yes (Default)	Yes	dword/Ø

2.17.9 Custom Actions Settings

The Custom Actions settings control the tasks (lists of commands) that should execute when specific Agent actions occur.

For each event, select the checkbox and click the ellipsis ("**…**") button to open the list dialog for that event. Enter one command on each line; end each line by pressing Enter. Do not use any other delimiter characters. They run one at a time, sequentially.

Logon Manager will not respond until all of the tasks complete.

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
After Agent starts `Shell\Tasks: StartupTaskN`	Command(s) that will run every time the background task starts (the Tray Icon appears).		Yes	string/Ø
Before each instance of the Agent executable starts `Shell\Tasks:PreTaskN`	Command(s) that will be run before each agent executable is started. **Note:** The intention of this option is to enable license checking before any part of the Agent is executed. The Agent will stop running if any of these tasks fails to set the registry value located at: `HKEY_CURRENT_USER\Software\Passlogix\ License\PreCheck:PreCheck` to 1. Each task should reset this to 0 when starting. **Warning:** Anything run in this way will impact performance of the Agent, as these tasks will run every time a new Agent process starts.		Yes	string/Ø
When logons are deleted `Shell\Tasks: DeletionTaskN`	Command(s) that will run every time a user deletes an application configuration.		Yes	string/Ø
When logons change (add, delete, copy, modify) `Shell\Tasks: RefreshTaskN`	Command(s) that will run every time a user modifies credentials and configurations.		Yes	string/Ø

2.17.10 Windows Event Log-Based Reporting

Large deployments of Logon Manager will often see the need for frequent auditing of user actions and information describing each action (such as date, time, and the name of the user). Logon Manager records this information through the Windows Event Log mechanism, enabling you to easily leverage your existing infrastructure to collect source data for system-wide audits.

Using the event log data recorded by Logon Manager, you can:

- Track the actions of Logon Manager users, such as logons and password changes. This includes associated information such as the action type, AD account name, date, time, and the credentials used to perform the action, if applicable.

- Track the credentials that were used to log on to an application over time by each user. This can help detect attempts of unauthorized access by users who share their credentials without permission.

- Track the actions of Logon Manager administrators. For example, if someone pushes a misconfigured template to the repository, you can find out when the update was performed on that particular Logon Manager object and by whom.

- Track application usage. You can use the event log data to analyze application usage by user, time, and date. Such information can aid you in gauging system loads, for example when setting up load balancing in large deployments.

2.17.10.1 Technical Prerequisites

The required event data is recorded on the machine hosting your Active Directory repository. In order to generate reports based on this data, you must:

- Enable the required level of log verbosity for your Active Directory instance by setting the following registry value:

- Path: `HKLM\SYSTEM\CurrentControlSet\Services\<AD_instance>\Diagnostics`

- Key: `8` Directory Access (DWORD)

- Value: `0x00000005` (hex)

- Query the `Win32_NTLogEvent` handler and filter your queries by event type SSO `EventMgr`. This is the event type used by Logon Manager when recording data in the Windows Event Log.

2.17.11 Audit Logging Settings

The Audit Logging settings let you specify the retry interval and size of the logging cache.

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Cache limit
 	
`Extensions\`
`EventManager:`
`CacheLimit`
	Maximum number of event log entries to be cached before old events are discarded.	Default: 200	Yes	dword/ int

Retry interval Extensions\EventMana ger:Retry	Interval (in minutes) between retries for all Event Logging extensions. **Note:** If you are using Reporting, you should set this value to zero (0).	Default: 30	Yes	dword/ int

2.17.11.1 Configuring the Windows Event Logging Server

Note: Domain users do not have permissions to write to a Microsoft Windows 2008 or 2012 Server application log by default. You must use the command-line tool `wevtutil`, which is a Microsoft utility for `eventvwr`. Contact Microsoft support if you need assistance using this command-line tool.

To configure a server to receive Event Log messages:

1. Install the Agent on that server.

   or

1. Copy `SSOeventmessage.dll` from an Agent installation to the server, preferably in the `System32` directory.

2. Create the following registry keys under `HKEY_LOCAL_MACHINE\System\CurrentControlSet\ Services\Eventlog\Application\v-GO SSO`:

Field	Function
Name	EventMessageFile
Type	STRING
Value	Full path to the file SSOeventmessage.dll, including filename (recommended: %WinDir%\System32\SSOeventmessage.dll)

Field	Function
Name	TypesSupported
Type	DWORD
Value	7

Field	Function
Name	CategoryMessageFile
Type	STRING
Value	Full path to the file SSOeventmessage.dll, including filename (recommended: %WinDir%\System32\SSOeventmessage.dll)

Field	Function
Name	CategoryCount
Type	DWORD
Value	4

2.17.11.2 Configuring the Reporting Server

The Reporting tool allows you to generate reports on user activities. Refer to Chapter 6, "Using the Administrative Console to Configure the Reporting Client" for complete information on using this tool.

2.17.11.2.1 Database

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Connection string Reporting\Extensions\ Database: ConnectionString	Database connection string in the OLE DB format: Provider=SQLOLEDB;Data Source=myServerName; Initial Catalog=myDatabaseName;Integrated Security=SSPI;Use Encryption for Data=True; Use Encryption for Data=True		No	string/ string
Stored procedure Reporting\Extensions\ Database: StoredProcedure	The name of the stored procedure used to populate the database with events. When encoded events are sent to the database, the stored procedure is called to decode the XML file and store the events in the database.	Default: dbo.sp_ WriteEvents	No	string/ string

2.17.11.2.2 Options
In order for Reporting to function properly, it is important that the following parameter values be set to zero (0):

- HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix\Extensions\EventManager\ CacheLimit:DWORD = 0

and

- `HKEY_LOCAL_
MACHINE\SOFTWARE\Passlogix\Extensions\EventManager\Retry:DWORD = 0`

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Batch size `Reporting:BatchSize`	Defines the group size of events to be sent to the database Stored Procedure in one batch. For example, if you have 1000 events in the Reporting Service cache and the Batch Size = 100, you will have 10 database Stored Procedure calls.	Default: 100	Yes	dword/ int
Cache limit `Reporting:CacheLimit`	Maximum number of reporting events to cache before discarding old events. When this number is reached, the oldest events are discarded. For example, if the batch size is 100 and an end-user's system cannot connect to the reporting service, it will keep logging events. When it reaches 1000, the oldest events will be discarded. (Default is `4294967295`, or `0xFFFFFFFF`.)	Default: `4294967295`, or `0xFFFFFFFF`	Yes	dword/ int
Retry interval `Reporting: RetryInterval`	Specifies the timeout (in minutes) between sequential operations of the Reporting Service Cache offloading events to the database. An interval is necessary to reduce database connection load. **Note:** You must restart the ESSO Reporting Service for your changes to take effect.	Default: 30	Yes	dword/ int

2.17.11.3 Configuring Windows Event Viewer

The Windows Event Viewer settings enable event logging on a remote server. Specify which events should be logged. You can also change the default path to the Windows Event logging extension and Windows event message components, and you can modify the retry interval of the logging cache.

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Windows event logging server `Extensions\ EventManager\ WindowsEvent: EventServer`	Specifies the server name for the Windows Event Logging extension (do not provide leading "\\" characters). If you do not specify a server, logging is performed on the local workstation. The server should have a trusted relationship with the user's account and the user's workstation, depending on access rights and restrictions.		Yes	string/ string
Retry interval `Extensions\ EventManager\ WindowsEvent:Retry`	Specifies the interval (in minutes) between retries for the Windows Event Logging extension.	Default: 30	Yes	dword/ int

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Events to log
 	
`Extensions\`
`EventManager\`
`WindowsEvent:Filter`
	Event logging filter delineating which events (of those logged by the root Filter setting) to log to the Windows Event Logging extension.
	
	Click the ellipsis "**…**" button to open the Events to log window, which presents a checklist of events for you to select.
		Default: 0
		
		4: Credential Edit
		
		8: Credential Delete
		
		10: Credential Copy
		
		20: Credential Add
		
		100: Provisioning
		
		200: Startup/Shutdown
		
		400: Help
		
		800: Settings Change
		
		1000: Reauthentication
		
		10000: Sync User Information
		
		20000: Logon Field: System Username
		
		40000: Logon Field: System Domain
		
		80000: Logon Field: Third Field
		
		100000: Logon Field: Username
		
		200000: Logon Field: Fourth Field
		
		800000: Application Password Change
		
		1000000: Primary Logon Method Change
		
		4000000: Backup/Restore
		
		40000000: Event Types: Info
			Yes	dword/Ø

2.17.11.3.1   Event Logging Filter Options Select the events you want to log, then click **OK**. The table below groups the filters by function.

> **Note:**   You must select **Event Types Info** to enable Event Logging.

Event Type	Name
Changes to user data (Credential)	Credential Add
	Credential Copy
	Credential Delete
	Credential Edit
Agent controls used (Feature)	Help
	Reauthentication
	Settings Change
	Startup / Shutdown
Credential data supplied (Logon)	Logon Field: Fourth Field
	Logon Field: System Domain
	Logon Field: System Username

Event Type	Name
	Logon Field: Third Field
	Logon Field: Username
	Sync User Information
Agent actions and changes (Application)	Primary Logon Method Change
	Backup/Restore
	Application Password Change
Event Types	Event Types Info (must be selected to enable Event Logging)

To display this dialog, select the Filter option and click the ellipsis ("**…**") button on any of the following settings panels:

- Event Logging (general)
- XML File (for local storage)
- Windows Event logging (advanced).

2.17.11.4 Configuring the Syslog Server

The Syslog settings control how the Agent records program events.

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Destination host Extensions\ EventManager\ Syslog:RemoteAddress	Specifies the hostname to send messages to, using either a hostname or dotted IP v4 address. Use 0.0.0.0 to disable sending to Syslog-Daemon, or use 255.255.255.255 to send to any daemon that is set up to receive broadcast messages. It must be on your local network as broadcast does not reach beyond a router.	Default: localhost	No	string/ string
Destination port Extensions\ EventManager\ Syslog:RemotePort	Specifies the destination port for syslog messages using a number.	Default: 1468	Yes	dword/ int
Protocol for sending messages Extensions\ EventManager\ Syslog:UseTCP	Specifies whether to send messages via TCP or UDP protocol. Note that the UDP protocol is connectionless, so it is impossible to tell whether the Syslog Daemon is reachable at the specified hostname and port. If the UseTCP parameter is set to "Use UDP," the Syslog Extension returns S_OK on both success and failure. If it is necessary to make the Syslog Extension return the correct state, enable TCP in the Syslog Daemon and set this parameter to "Use TCP."	0: Use UDP 1: Use TCP (Default)	Yes	dword/Ø
Retry interval Extensions\ EventManager\ Syslog:Retry	Specifies the interval (in minutes) between retries for the Syslog extension.	Default: 30	Yes	dword/ int

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Events to log
 	
`Extensions\`
`EventManager\`
`Syslog:Filter`
	Event Logging filter delineating which events (of those logged by the root Filter setting) to log to the Syslog extension. Click the ellipsis "**…**" button to see a list of events to log.	Default: 0
		
		4: Credential Edit
		
		8: Credential Delete
		
		10: Credential Copy
		
		20: Credential Add
		
		100: Provisioning
		
		200: Startup/Shutdown
		
		400: Help
		
		800: Settings Change
		
		1000: Reauthentication
		
		10000: Sync User Information
		
		20000: Logon Field: System Username
		
		40000: Logon Field: System Domain
		
		80000: Logon Field: Third Field
		
		100000: Logon Field: Username
		
		200000: Logon Field: Fourth Field
		
		800000: Application Password Change
		
		1000000: Primary Logon Method Change
		
		4000000: Backup/Restore
		
		40000000: Event Types: Info
			Yes	dword/Ø

2.17.11.5 XML File Event Logging

The XML File Event Logging settings let you specify which events should be logged locally. You can also change the default path to the local logging extension, and you can modify the retry interval of the logging cache.

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Retry interval
 	
`Extensions\`
`EventManager\`
`LocalStorage:Retry`
	Specifies the interval (in minutes) between retries for the Local (XML) File Logging extension.	Default: 30	Yes	dword/ int

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Events to log
 	
`Extensions\`
`EventManager\`
`LocalStorage:Filter`
	Event Logging filter delineating which events (of those logged by the root Filter setting) to log to the Local (XML) File Logging extension.
	
	Click the ellipsis "**…**" button to see a list of events to log.
		Default: 0
		
		4: Credential Edit
		
		8: Credential Delete
		
		10: Credential Copy
		
		20: Credential Add
		
		100: Provisioning
		
		200: Startup/Shutdown
		
		400: Help
		
		800: Settings Change
		
		1000: Reauthentication
		
		10000: Sync User Information
		
		20000: Logon Field: System Username
		
		40000: Logon Field: System Domain
		
		80000: Logon Field: Third Field
		
		100000: Logon Field: Username
		
		200000: Logon Field: Fourth Field
		
		800000: Application Password Change
		
		1000000: Primary Logon Method Change
		
		4000000: Backup/Restore
		
		40000000: Event Types: Info
			Yes	dword/Ø

2.17.11.6 Database Event Logging

Use the **Database Event Logging** menu to specify the server instance and table name where you want to send log data, as well as the fields to write to the database.

In addition to the fields, users must specify the server instance and table name. These are previously defined in the Database Setting and should not be required for Database Fields. If the database and table name are not specified for each field, events will not be written to the database.

The XML File Event Logging settings let you specify which events should be logged locally. You can also change the default path to the local logging extension, and you can modify the retry interval of the logging cache.

> **Note:** You must specify the database instance and table name in the Database Fields in order for events to be written to the database.

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Servers
 	
`Extensions\`
`EventManager\`
`Database\Servers:`
`ServerN`
	Click the ellipsis "…" button to open a window in which to enter Database servers. Enter one server name per line, using the OLE DB format:
	
	`"Provider=sqloledb; Data`
	`Source=myServerName; Initial`
	`Catalog=myDatabaseName; User`
	`Id=myUsername; Password=myPassword; Use`
	`Encryption for Data=True"`
			No	string/Ø

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Default server Extensions\ EventManager\ Database:Default Server	If no other server is specified, the server to which the database log will be written. (OLE DB connection string)	Default: Server1	No	string/ string
Default table Extensions\ EventManager\ Database:Default Table	If no other table is specified, the table to which the database log will be written.		Yes	string/ string
Retry interval Extensions\ EventManager\ Database:Retry	Interval (in minutes) between retries for the Database extension.	Default: 30	Yes	dword/ int
Events to log Extensions\ EventManager\ Database:Filter	Event Logging filter delineating which events (of those logged by the root Filter setting) to log to the Database extension. Click the ellipsis "…" button to see a list of events to log.	Default: 0 4: Credential Edit 8: Credential Delete 10: Credential Copy 20: Credential Add 100: Provisioning 200: Startup/Shutdown 400: Help 800: Settings Change 1000: Reauthentication 10000: Sync User Information 20000: Logon Field: System Username 40000: Logon Field: System Domain 80000: Logon Field: Third Field 100000: Logon Field: Username 200000: Logon Field: Fourth Field 800000: Application Password Change 1000000: Primary Logon Method Change 4000000: Backup/Restore 40000000: Event Types: Info	Yes	dword/Ø

2.17.11.6.1 Event Fields The **Event Field**s screen lists the data assigned to each field in the event log. The fields are mapped to the log information as specified in the table below.

You can select which events to include in your log by checking the box next to the desired field(s). Fields 9 and 10 have no pre-assignment. Assign categories to these fields by checking their boxes and entering the name of the desired field next to the check box. Refer to the **Events to log** list on the Database screen for the available event names.

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
AppName Extensions\EventManager\ Database\EventFields: AppName	The name of the application of the event log.	Default: AppName	Yes	string/ string
Category Extensions\EventManager\ Database\EventFields: Category	The category of the event.	Default: Category	Yes	string/ string
Type Extensions\EventManager\ Database\EventFields:Type	The specific type of event.	Default: Type	Yes	string/ string
TimeStamp Extensions\EventManager\ Database\EventFields: TimeStamp	The time of the event.	Default: TimeStamp	Yes	string/ string
Field1 Extensions\EventManager\ Database\EventFields: Field1	EventType	Default: Event type	Yes	string/ string
Field2 Extensions\EventManager\ Database\EventFields: Field2	UserID	Default: User ID	Yes	string/ string
Field3 Extensions\EventManager\ Database\EventFields: Field3	ThirdField	Default: Third field	Yes	string/ string
Field4 Extensions\EventManager\ Database\EventFields: Field4	FourthField	Default: Fourth field	Yes	string/ string
Field5 Extensions\EventManager\ Database\EventFields: Field5	WindowsUser	Default: Windows user	Yes	string/ string
Field6 Extensions\EventManager\ Database\EventFields: Field6	Domain	Default: Domain	Yes	string/ string
Field7 Extensions\EventManager\ Database\EventFields: Field7	ComputerName	Default: Computer name	Yes	string/ string
Field8 Extensions\EventManager\ Database\EventFields: Field8	SSOSyncUser	Default: SSO synchronization user	Yes	string/ string
Field9 Extensions\EventManager\ Database\EventFields: Field9	Customizable for your needs.	Open	Yes	string/ string
Field10 Extensions\EventManager\ Database\EventFields: Field10	Customizable for your needs.	Open	Yes	string/ string

2.17.11.7 Kiosk Manager Settings

Use the Kiosk Manager settings to configure sessions in a kiosk environment.

> **Note:** When using Kiosk Manager, you must disable response to hidden or minimized windows in User Experience settings.

2.17.11.7.1 Session termination

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Allow administrator to closeKiosk Manager
 	
`SM\Agent:`
`AdministrativeClose`
	Specifies whether an administrator has the ability to close Kiosk Manager. With this setting enabled, only a user with administrator credentials can close the Agent.	0: No
		1: Yes (Default)
			Yes	dword

Number of times to process termination
 	
`SM\Agent:`
`TerminationIteration`
	Enter the number of times that Kiosk Manager should process the termination of an application.
	
	This setting instructs the termination process to loop a certain number of times or until it is done (whichever comes first). This allows Kiosk Manager to react to an application if it displays multiple screens during the termination process.
		Default: 1	Yes	dword/
				int

Timeout for locked session `SM\Agent:ExpireTerm`	Enter the length of time (in seconds) of inactivity after which Kiosk Manager should close a suspended/locked session.	Default: 600 (15 minutes)	Yes	dword/ int

2.17.11.7.2 Multisession configuration

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Maximum number of sessions `SM\Agent: MaxSessions`	Specifies the maximum number of sessions allowed at one time. A setting of zero will be interpreted as one session. **Note:** There is no maximum number for this setting.	Default: 1	Yes	dword/ int

Track memory consumption
 	
`SM\Agent:TrackMemory`
`Consumption`
	Specifies the level of memory usage at which Kiosk Manager should automatically close sessions. When system memory use has reached the percentage set by this value, Kiosk Manager automatically closes the oldest user sessions.	Minimum: 0 (disabled)
		Maximum: 100
		Default: 90
			Yes	dword/
				int

2.17.11.7.3 Cached credentials

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

Use cached credentials
 	
`SM\Agent:`
`UseCachedCredentials`
	Specifies whether to use cached credentials. If this setting is enabled, at logon the Agent displays a list of cached credentials for users to choose from. If this setting is disabled, the Agent does not display the list, and users must enter a user name at logon.
	
	Enabling cached credentials improves performance.
	
	Note: When using Universal Authentication Manager as the primary logon method, you cannot use cached credentials (that is, select No for this setting). For a full discussion about configuring and deploying Universal Authentication Manager, see the *Oracle Enterprise Single Sign-On Suite Installation Guide* and Chapter 5, "Configuring Strong Authenticators with Universal Authentication Manager".
		0: No (Default)
		1: Yes
			Yes	dword

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Storage path `SM\Agent: CachedCredentials StoragePath`	Specifies the default folder to store the cached credentials. The default is an empty string. If this value is empty, the default folder is: `C:\Documents and Settings\<Kiosk User>\Local Settings\ Application Data\ Passlogix\ SessionData\Kiosk Manager User.`	Default: An empty string	Yes	string
Expiration date `SM\Agent: CachedCredential Expiration`	Specifies the number of days to retain cached credentials. Zero indicates that this feature is disabled.	Default: 30	Yes	dword/ int

2.17.11.7.4 Strong authentication options

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Lock session on smart card removal `AUI\SCauth: LockSMOnRemoval`	Specifies whether to lock a session when the session owner removes the smart card from its reader. If set to not lock, the session remains open after smart card removal. This setting is useful in a scenario where employees must display their smart cards at all times, and therefore cannot leave them in a reader.	0: No 1: Yes (Default)	Yes	dword
Lock session on read-only smart card removal `AUI\ROSCauth: LockSMOnRemoval`	Specifies whether to lock a session when the session owner removes the read-only smart card from its reader. If set to not lock, the session remains open after read-only smart card removal. This setting is useful in a scenario where employees must display their read-only smart cards at all times, and therefore cannot leave them in a reader.	0: No 1: Yes (Default)	Yes	dword
Lock session on ESSO-UAM token removal `AUI\SCauth: LockSMOnRemoval`	Specifies whether to lock a session when the session owner removes a Universal Authentication Manager logon token from its reader (or taps out, in the case of passive proximity tokens). If set to not lock, the session remains open after token removal. This setting is useful in a scenario where employees must display their tokens at all times, and therefore cannot leave them in a reader. **Note:** Any value other than zero (0) will result in token events being forwarded to Kiosk Manager. Whatever setting you select here will apply to all Universal Authentication Manager authenticators.	0: No 1: Yes (Default)	Yes	dword
Pre-populate on startup `SM\Agent:Prepopulate`	Specifies whether to run a pre-populate step at startup. If an authenticator requires this step and Authentication Manager is not installed, this setting enables Kiosk Manager to perform the required pre-population, eliminating the need for the synchronization manager to reauthenticate. **Note:** When using Universal Authentication Manager as the primary logon method, you must pre-populate on startup (that is, select Always for this setting). For a full discussion about configuring and deploying Universal Authentication Manager, see the Oracle Enterprise Single Sign-On Suite Plus Installation Guide and the Universal Authentication Manager Administrator's Guide.	0: On device-in event (Default) 1: Always 2: Never	Yes	dword

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Monitor for device events SM\Agent: DeviceMonitoring	Specifies whether Kiosk Manager should actively monitor for device insertion and removal events. **Note:** For integration with Universal Authentication Manager, you must select **Always** for this setting.	0: Never 1: Only when Access Manager is installed (Default) 2: Always	Yes	dword

2.17.11.7.5 Audit Logging

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Event log name SM\Agent:EventLogName	Enter the name of the Windows event log for Kiosk Manager events.	Default: Application	Yes	string
Event log machine name SM\Agent: EventLogMachine	Enter the name of the local machine to log Kiosk Manager events.		No	string

2.17.11.8 Kiosk Manager User Interface

The User Interface settings control the appearance and interaction of Kiosk Manager with end-users.

2.17.11.8.1 Options

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Allow computer restart SM\Agent:AllowRestart	Specifies whether the restart computer option is enabled in the Kiosk Manager Desktop Manager. You can also choose to allow only an administrator to have privileges to restart the computer by selecting Administrator must supply password. **Note:** If the Kiosk account does not have sufficient privileges, restarting might still be disabled.	0: No (Default) 1: Yes 2: Administrator must supply password	Yes	dword
Allow computer shutdown SM\Agent: AllowShutdown	Specifies whether the shutdown computer option is enabled in the Kiosk Manager Desktop Manager. You can also choose to allow only an administrator to have privileges to shut down the computer by selecting Administrator must supply password. **Note:** If the Kiosk account does not have sufficient privileges, shutting down might still be disabled.	0: No (Default) 1: Yes 2: Administrator must supply password	Yes	dword
Show confirmation message when restarting kiosk SM\Agent: ConfirmRestart	Specifies whether to prompt the user with a confirmation message after choosing to restart the kiosk.	0: No (Default) 1: Yes	Yes	dword
Show confirmation message when shutting down kiosk SM\Agent: ConfirmShutdown	Specifies whether to prompt the user with a confirmation message after choosing to shut down the kiosk.	0: No (Default) 1: Yes	Yes	dword

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Lock session when screen saver times out SM\Agent: LockOnScreenSaver	Specifies whether to lock a session after the screen saver timeout occurs. A blank value has the same effect as setting the value to "No." Specifies whether Kiosk Manager should lock a session when the screen saver timeout occurs. If you set this value to **No** (default value) or do not specify a setting, Kiosk Manager does not lock the session after the screen saver timeout occurs if device detection is used to control the session. If you set this value to **Yes**, Kiosk Manager locks the session.	0: No (Default) 1: Yes	Yes	dword
Timeout for authentication prompt SM\Agent:AuthTerm	Enter the length of time (in seconds) after which the synchronization/authentication dialog closes (due to inactivity).	Default: 600 [15 minutes]	Yes	dword/ int

2.17.11.8.2   Status window

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Show desktop status window SM\Agent: DisplayDesktopStatus	Specifies whether to show the optional window that displays the current session owner.	0: No (Default) 1: Yes	Yes	dword
X coordinate SM\Agent: DesktopStatusX	Enter the X coordinate (horizontal location) for the status window. **Note:** Negative values are represented by large positive numbers in the registry. For example: -1 = 4294967295 and -2 = 4294967294.	Default: 0	Yes	dword/ int
Y coordinate SM\Agent: DesktopStatusY	Enter the Y coordinate (vertical location) for the status window. **Note:** Negative values are represented by large positive numbers in the registry. For example: -1 = 4294967295 and -2 = 4294967294.	Default: 0	Yes	dword/ int

2.17.11.8.3   Transparent screen lock

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Use transparent lock SM\Agent: TransparentLock	Specifies whether to enable the transparent screen lock. Specifies whether to enable the transparent screen lock. The transparent screen lock provides the ability to lock the desktop inputs (keyboard and mouse) in view mode. For example, a monitoring application can be viewed without starting a session. When there are multiple sessions running, the last active session displays when transparent screen lock engages.	0: No (Default) 1: Yes, but only for active session 2: Yes	Yes	dword
Delay period SM\Agent: TransparentLockTime	Specifies the number of seconds to wait for mouse and keyboard inactivity before showing the desktop. **Note:** You must enable the **Use transparent lock** setting above in order to use this feature.	5: Default	Yes	dword/ int

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Ignore delay period if authentication is canceled SM\Agent: TransparentDisplay AfterCancel	Specifies whether transparency should take effect immediately after canceling an authenticator or synchronizer dialog. **Note:** You must enable the Use transparent lock setting above in order to use this feature.	0: No (The desktop displays when the inactivity timer expires.) (Default) 1: Yes (The desktop displays instantly.)	Yes	dword
Only recognize Ctrl-Alt-Del SM\Agent: TransparentOnly RecognizeCAD	Specifies whether the Agent should recognize only Ctrl-Alt-Del and authenticators that support "device-in" to display the Desktop Manager.	0: No (Any keyboard or mouse activity results in displaying the Desktop Manager.) (Default) 1: Yes (The Agent ignores all keyboard or mouse activities. Only Ctrl-Alt-Del and authenticators that support "device-in" will be recognized to display the Desktop Manager.)	Yes	dword

2.17.11.8.4 Setting the Kiosk Manager Background Image Use this panel to place a background image, such as your company logo, on the Kiosk Manager Desktop Manager.

To configure the administrative settings for the Desktop Manager background image:

See Customizing the Desktop Manager for examples of using all Kiosk Manager desktop customization settings.

1. Open the Administrative Console.

2. Navigate to **Global Agent Settings > Live > Kiosk Manager > User Interface > Background Image**.

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Location of image file SM\Agent\Desktop: LogoPath	Fully-qualified path and filename of the image file. Enter the fully-qualified path, including the filename, to the image file. Click the ellipsis "..." button to locate the file.		Yes	string/ filename
X coordinate SM\Agent\Desktop: LogoX	Enter the X coordinate (horizontal location) for the image. **Note:** Negative values are represented by large positive numbers in the registry. For example: -1 = 4294967295 and -2 = 4294967294.	Default: 0	Yes	dword/ int
Y coordinate SM\Agent\Desktop: LogoY	Enter the Y coordinate (vertical location) for the image. **Note:** Negative values are represented by large positive numbers in the registry. For example: -1 = 4294967295 and -2 = 4294967294.	Default: 0	Yes	dword/ int
Width SM\Agent\Desktop: LogoWidth	Enter the width of the image (in pixels).	Default: 300	Yes	dword/ int
Height SM\Agent\Desktop: LogoHeight	Enter the height of the image (in pixels).	Default: 300	Yes	dword/ int

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Placement behavior SM\Agent\Desktop: LogoMode	Specifies how to handle the image with respect to its coordinates and dimensions.	0: Normal (Place image in upper left corner of coordinates and clip if larger than specified height and width) (Default) 1: Auto (Place image in upper left corner of coordinates) 2: Center (Center image within coordinates and clip if larger than specified height and width) 3: Stretch (Stretch or shrink image to fit within specified coordinates) 4: Maximize (Stretch image to full screen size)	Yes	dword

2.17.11.8.5 Message

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Message text SM\Agent\Desktop: MOTDText	Enter a message to display on Desktop Manager. This message appears when the user unlocks a new session.		Yes	string/ string

2.17.11.8.6 Font

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Name SM\Agent\Desktop: MOTDFontName	Specifies the Message Text font. Select a font from the drop-down list.		Yes	string/ string
Size SM\Agent\Desktop: MOTDFontSize	Specifies the Message Text font size.	Default: 0	Yes	dword/ int
Style SM\Agent\Desktop: MOTDFontStyle	Specifies the Message Text font style.	0: Regular (Default) 1: Bold 2: Italic	Yes	dword

2.17.11.8.7 Color

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Background SM\Agent\Desktop: MOTDBackColor	Click the ellipsis "…" button to select the background color for the Message Text.		Yes	string/ color
Foreground SM\Agent\Desktop: MOTDForeColor	Click the ellipsis "…" button to select the foreground color for the Message Text.		Yes	string/ string

2.17.11.8.8 Placement

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType

X coordinate
 	
`SM\Agent\Desktop:`
`MOTDX`
	Enter the X coordinate for the Message Text, positioned relative to the Status image on the Kiosk Manager Desktop screen. A negative value places the message to the left of the Status image.
	
	Note: Negative values are represented by large positive numbers in the registry. For example: -1 = 4294967295 and -2 = 4294967294.
		Default: 0	Yes	dword/ int

Y coordinate
 	
`SM\Agent\Desktop:`
`MOTDY`
	Enter the Y coordinate for the Message Text, positioned relative to the Status image on the Kiosk Manager Desktop screen. A negative value places the message above the Status image.
	
	Note: Negative values are represented by large positive numbers in the registry. For example: -1 = 4294967295 and -2 = 4294967294.
		Default: 0	Yes	dword/ int

Width
 	
`SM\Agent\Desktop:`
`MOTDWidth`
	Specifies the width of the Message Text (in pixels).	Default: 300	Yes	dword/ int

Height
 	
`SM\Agent\Desktop:`
`MOTDHeight`
	Specifies the height of the Message Text (in pixels).	Default: 300	Yes	dword/ int

Size automatically
 	
`SM\Agent\Desktop:`
`MOTDAutoSize`
	Specifies whether to auto-size the Message Text to fit the available area.	0: No (Default)
		
		1: Yes
			Yes	dword

2.17.12 Oracle Access Manager Support

Logon Manager provides transparent single sign-on capability to Oracle Access Management Access Manager-protected Web applications by securely authenticating to Access Manager via one or more Access Manager endpoints using SSL, obtaining the Access Manager authentication cookie, and transparently injecting it into the current Web browser session. This 100% seamless integration completely eliminates the visibility of the logon process to Access Manager-protected Web applications, allowing for instant application availability without compromising security.

> **Note:** Logon Manager ships with a pre-configured template for Access Manager. You must publish this template to the repository and propagate it to Access Manager-enabled Logon Manager client machines to use this feature.
>
> Integration with Access Manager is only possible when using the Embedded Credential Collector; the Distributed Credential Collector is not supported.

To enable this capability, you must:

1. Install and configure at least one Access Manager endpoint within your Access Manager deployment.

2. Install the "OAM Support" component of Logon Manager on end-user machines as described in the *Oracle Enterprise Single Sign-On Suite Installation Guide*.

3. Publish the OAM Protected Resources template to the repository. This template is included in the Administrative Console installation.

   a. Launch the Administrative Console.

    b. Right-click on the **Applications** node and select **New Web App**.

    c. Select **OAM Protected Resources** from the dropdown list of available applications.
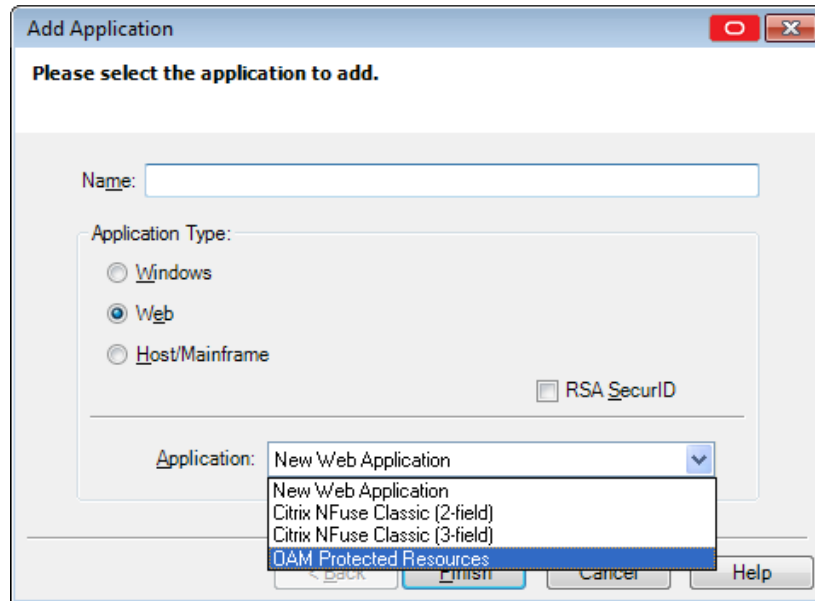
    d. Click **Finish**. The OAM Protected Resources application is now listed under the Applications node. There is no need to modify the URLs or logon fields; the template is configured for immediate use.

4. Configure Logon Manager to connect to the desired Access Manager endpoint(s) as described in Access Manager Settings. (If more than one endpoint is specified, Logon Manager will attempt connecting to each specified endpoint, in the order entered in the Administrative Console, until a connection is established.)

> **Note:** You must enter the endpoint URL(s) in the following format only:
>
> ```
> https://<server>:<port>/oam/services/rest/11.1.2.0.0/sso/tok
> en/
> ```
>
> where `<server>` is the full network address of the target endpoint and `<port>` is the number of the port on which the endpoint is listening for connections.

5. Provide Logon Manager with the end-user's Access Manager credentials using one of the following methods:

- Remotely provisioning the credentials via Provisioning Gateway;

- Configuring Logon Manager to use the user's repository credentials to authenticate to Access Manager;

- Capturing the Access Manager credentials from the end-user during Logon Manager's first attempt to authenticate to Access Manager. (The captured credentials are stored in Logon Manager's secure cache once captured; the user will not be prompted to provide them again unless the secure cache is erased.)

The following session attributes are pushed by Logon Manager into the session:

Attribute	Description
$session.attr.client.firewallenabled	Specifies whether a firewall is active on the client machine.
$session.attr.client.antivirusenabled	Specifies whether an anti-virus application is active on the client machine.
$session.attr.client.fingerprint	Specifies a unique identifier for the client machine.

After being positively authenticated to Access Manager, the session cookie remains in the Web browser's cache as long as Logon Manager is running and is periodically updated according to an update interval configured by the administrator, or upon expiration. When Logon Manager shuts down, the cookie is removed from the Web browser's cache.

> **Note:** Logon Manager does not support password change for Access Manager credentials. If the user's Access Manager password expires, it must be reset via other means. If Logon Manager cannot authenticate with the currently supplied credentials to Access Manager, it will prompt the user to enter valid credentials.

You can change the message that prompts the user to enter Access Manager credentials using the Authentication dialog message setting in the User interface settings group, or leave the default message. If you choose to change it, select a message that will be meaningful to the user in your particular environment.]

2.17.12.1 Access Manager Settings

The following settings configure Access Manager integration with Logon Manager.

2.17.12.1.1 Connection Information

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Endpoints Extensions\ AccessManager\ WebHO\OAM:EndpointN	A list of URLs that the Agent should use as Access Manager token endpoints. Check the box and click the ellipsis (…) button, then enter the URLs in the Endpoints window, one per line. Click OK when you have entered all the URLs you want the Agent to try. The Agent attempts to use the URLs in the order that you enter them; if the first URL fails, the Agent proceeds to the second one, and so on.		Yes	string/Ø
Use sync credentials to authenticate to OAM Extensions\ AccessManager\ WebHO\OAM:CredUseSync	Allows Logon Manager to use the synchronizer's credentials to automatically create an account for an Access Manager template. **Note:** This feature supports only Active Directory, AD LDS (ADAM), and LDAP synchronizers. You cannot enable this setting with the Active Directory synchronizer unless you select **Use Active Directory server account only** for the Credentials to use setting. You cannot enable this setting with the AD LDS (ADAM) synchronizer unless you select **ADAM server account** for the Credentials to use setting.	0: No (Default) 1: Yes	Yes	dword/Ø

2.17.12.1.2   Behavior

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Perform OAM server certificate validation `Extensions\AccessManager\ WebHO\OAM: PerformCertificate Validation`	Specifies whether the Agent should check the Access Manager server certificate when connecting to the endpoint. If the certificate is invalid, no connection is established.	0: No. The Agent ignores the server certificate (less secure) (Default) 1: Yes. The Agent checks the server certificate.	Yes	dword/Ø
OAM credentials request retry interval `Extensions\AccessManager\ WebHO\OAM: CredRetryInterval`	Specifies the interval (in seconds) after which the Agent will ask for Access Manager credentials again if the user cancels an Access Manager credentials request. Values can range from zero (the Agent request credentials immediately) to 300 (the Agent requests credentials after five minutes).	Any integer between 0 and 300. Default is 30.	Yes	dword/ int
OAM session renewal interval `Extensions\AccessManager\ WebHO\ OAM: SessionRenewalInterval`	Specifies the interval (in minutes) that the Agent uses for polling an Access Manager endpoint in order to detect whether the Access Manager session token is valid. The minimum value is one minute, which means that the Agent checks the Access Manager session token validity at one minute intervals. **Note:** Greater interval values create less network traffic but lower sensitivity to Access Manager session token expiry.	Any positive integer. Default is 1.	Yes	dword/ int

2.17.12.1.3   User interface

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Authentication dialog message `Extensions\ AccessManager\WebHO\ OAM:AuthWindowSubtitle`	The message that Logon Manager displays to prompt the user for Access Manager credentials. This message should be meaningful to the user in your environment and approximately the same length as the default message.	Default: Logon Manager needs your credentials for Access Manager. If you do not know these credentials, contact your administrator.	Yes	string/ string

2.17.13 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 Installation Guide*.

2. Install and configure Password Reset as described in the *Oracle Enterprise Single Sign-On Suite Installation Guide*.

3. Obtain the Password Reset synchronization URL.The URL will have the following format:

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

4. Configure Universal Authentication Manager to synchronize with Password Reset as described in Chapter 5.2.5, "Integrating with Password Reset".

5. Configure the challenge questions as desired within Password Reset. For more information, see Chapter 4, "Using the Administrative Console to Configure Password Reset".

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 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/Synchronizati
on.asmx
```

Note: 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.

Note: The Console produces a `.REG` file compatible only with 32-bit systems. If you are merging the `.REG` file on a 64-bit system, you must run the following command to move the merged registry data to the correct location within the registry (otherwise, Universal Authentication Manager will not function):

```
reg.exe COPY HKLM\Software\Passlogix
HKLM\Software\Wow6432Node\Passlogix /s
```

2.17.13.1 Password Reset Settings

Display Name/ Registry Path	Description	Options/ Default	Overridable	RegType/ DataType
Password Reset synchronization URL `SSPR\Sync:SyncURL`	Specifies the URL to the Password Reset synchronization server when configuring Universal Authentication Manager to leverage Password Reset's enrollment interview as challenge questions for authentication purposes. Example `https://server/vGOSelfServiceReset/WebServices/Synchronization.asmx` **Note:** If you have not configured your Password Reset deployment for SSL connectivity, replace `https://` with `http://`.		Yes	string/ string

2.17.14 Using the Configuration Test Manager

This tool enables you to test your Global Agent Settings to ensure that they are properly configured.

> **Note:** You can only run these tests on an Active Directory repository.

To access this tool, either:

- Select Test Global Agent Settings from the Tools menu. If you access the test manager from this location, you are required to pick a set of Global Agent Settings to test.

  or

- Right-click on a set of Global Agent Settings and click **Test**. If you access the test manager from this location, the tests will run on that set of Global Agent Settings only.

All changes made in the test manager are reflected in the Administrative Console. Upon launching the test manager, a dialog appears, informing you that any changes you make in the test manager will be reflected in the Administrative Console. You can dismiss this message by selecting **Do not show this notice again**.

> **Note:** Before using this tool, in addition to reading this help information, Oracle strongly recommends that you read *Deploying Logon Manager with a Directory-Based Repository* and the Configuring the Agent with Global Agent Settings.
>
> These describe best practices and recommended procedures for deploying Logon Manager on your repository and configuring the Logon Manager Agent with Global Agent Settings and administrative overrides.

There are three stages in the testing process:

1. **Select Categories.** Select the test categories to determine which tests to run.

2. **Enter Parameters.** Enter all data needed to run the tests.

3. **Execution and Results.** Run tests, view results, and make changes if necessary.

2.17.14.1 Categories

When you open this tool, the Categories stage is selected in the left pane. The **Test Categories** pane lists the categories and individual tests.

The **Test Categories** list is interactive—you can check or uncheck desired categories, and expand or collapse the categories to view the individual tests. You can click on any category or test and a description appears in the right pane.

By default, all categories are selected. Individual tests cannot be selected.

As long as at least one test category is selected, the **Next** button and the **Parameters** stage are enabled. The **Execution and Results** stage is unavailable until all of the data parameters are satisfied.

The **Synchronization** test category contains the following individual tests, which verify synchronization settings.

Test Name	Test Description
Server Validation	Verifies that the specified server is a valid server name and is accessible. If an IP address is entered as the server name, or the server cannot be accessed, this test will fail.
SSL Configuration	Checks the server to determine if SSL is enabled. If SSL is not enabled on the server, and SSL is enabled in the Administrative Console, this test will fail.
Schema Extension	Verifies that the schema is extended. If the schema is not extended, this test will fail.
User Object Schema Extension	Verifies that the schema is extended under the Active Directory User Object. If the schema is not extended, this test will fail. This test applies to Active Directory synchronizers only.
Configuration Object Retrieval	Verifies that the Configuration Object Base Location path is valid and that the configuration objects can be retrieved with the test credentials. If the path is not valid or the test credentials supplied do not have permission to retrieve configuration objects, this test will fail.
Credential Location Access Rights	Verifies the proper access rights are assigned to the credential location on the server to upload, retrieve, and delete credentials. If the supplied test credentials do not have permission to perform any of these actions, this test will fail.

Ensure the **Synchronization** test category is selected and click **Next**, or click the Parameters stage from the left pane.

2.17.14.2 Parameters

The **Parameters** stage collects all the data necessary to run the tests. The data requested during this stage is dependant upon the test categories selected in the **Categories** stage.

The **Execution and Results** stage is unavailable until all of the data parameters are satisfied.

2.17.14.2.1 Test Parameters The parameters are listed in the **Test Parameters** pane and are dynamic based upon the tests selected. Each parameter has a status icon of Needed or Acquired to visually indicate which parameters need attention. For example, if the

User Credentials have not been acquired, and the Global Agent Settings have been acquired, the Test Parameter list will look like this:

Test Parameters

User Credentials	✗ Needed
Global Agent Settings	✓ Acquired

2.17.14.2.2 Data The data needed for each parameter is entered in the Data pane on the right.

You must input all needed data before running any tests. After all parameters are successfully acquired, the **Next** button and **Execution and Results** stage become available.

The **Next Parameter** button, located on the bottom of the **Data** pane, is available when there are multiple parameters. It enables you to quickly click through all the parameters.

> **Note:** It is important that you ensure that the quality of the data parameters entered is good. Just because data exists and a status is set to acquired, does not mean the data is correct.

As you enter, it is captured for the current session. You can either save or clear the data for future sessions:

- **Saving the data.** If you want to save the data for future sessions, ensure the **Save this value** check box located below the **Data** pane is checked.

- **Clearing the data.** If you want to clear the data for this and future sessions, click the **Clear All Data** button at the top of the **Data** pane. A message will appear asking if you are sure you want to do this. Confirming this action will clear all entered parameters, turning all of the parameter statuses to **Needed**. It will also disable the option to proceed to the **Execution & Results** stage.

After you have entered all data, click **Next >**, or select the **Execution & Results** stage in the left pane.

After all data has been acquired, move on to the next stage.

2.17.14.3 Execution and Results

The **Execution & Results** stage is where you run the tests, view the results, and make changes if necessary.

You cannot proceed to the **Execution & Results** stage until you have entered all of the data required during the **Parameters** stage.

The **Test Execution and Results** pane lists all the tests to be run, in the order that they will be run. After you click **Execute Tests**, the tests begin to run; while a test is in progress, an icon appears indicating the status of the testing. There are five possible statuses:

- **Passed.** The test has completed and passed.

- **Need info.** The test is paused to allow the user to enter prompted information.

- **Warning.** The test has paused, prompting the user with a warning.

- **Failed.** The test has failed. Information is provided explaining why the test failed. All testing stops when a single test fails.

- **In Progress.** Test is in progress.

After the tests have run, you can click through them and read the results and messages about each test in the Description pane.

2.17.14.3.1 Description The **Description** pane provides a description of the test. As tests run, the lower portion of the **Description** pane will provide messages such as warnings, passed and failed situations, and fields to change information and continue testing.

The **Execute Tests** button begins the testing. When tests are running, the **Execute Tests** button toggles to **Stop Tests**, allowing you to cancel the testing if desired.

In this pane, you can interact with either **Failed** or **Need Info** tests results. You are presented with information and actions or fields you can make changes to and re-run the tests.

2.17.14.3.2 Clear All Data If you want to clear the data for this test and future sessions, click the **Clear All Data** button at the top of the **Description** pane. A message will appear asking if you are sure you want to do this and provide two paths:

- Click **OK** to clear ALL parameters.

- Click **Cancel** to close the dialog, and all data is retained.

If you click **OK**, and tests were previously run with results available in the right frame, the test results persist, but the **Execute Test** button is disabled.

After the configuration passes all the tests, you can exit by closing the Test Manager from the **X** in the top right title bar. You may also use the **Clear All Data** button, navigate to the **Categories** or **Parameters** page, and set things up to run different tests.

2.18 Deploying Logon Manager

The topics in this section describe the options for packaging, deploying, and managing Logon Manager in a networked environment:

- Default MSI Deployment Options

- Deploying the Agent with Anywhere

- Using the MSI Generator

- Using Other Deployment Tools

2.18.1 Default MSI Deployment Options

This section describes using the default MSI package from the following perspectives:

- Performing an Installation with the Shipped MSI Package

- Installing from the Command Line

- Installing the MSI Package Remotely

- Editing the MSI Package

- Adding Console-Created Application Logons and Global Agent Settings

- Using Other Deployment Tools

2.18.1.1 Performing an Installation with the Shipped MSI Package

To perform an installation using the shipped MSI package, run the program setup from the network share and follow the prompts. Because each environment is different and each organization has different needs, Oracle recommends you perform a custom installation and select the desired components.

See the *Oracle Enterprise Single Sign-On Suite Installation Guide* for complete information.

2.18.1.2 Installing from the Command Line

The MSI package can be installed from the command line. To do this, run the setup program with the appropriate parameters. The components of the command line are the executable name, InstallShield parameters (for example, /qn for a quiet install), and the Logon Manager feature names.

Command	Purpose
/qn	The MSI package should install quietly (optional)
RUNVGO	Whether the Agent should be launched after the install: YES or NO
MDAC	Whether to install MDAC: YES or NO
ADDLOCAL "*FeatureNames*"	*FeatureNames* is a comma-delimited list of the Logon Manager features to install. Refer to the *Oracle Enterprise Single Sign-On Suite Installation Guide* section on MSI Package Contents for a list of acceptable values.

> **Note:** Quoting is critical. There must be quotes around each option's value (following the equal (=) sign, and the MSI features list.

Example

Install (without seeing any visual signs) the core, the Windows authenticator, NO support for Microsoft Internet Explorer or hosts, and the Microsoft Active Directory synchronizer, and then start the Agent, as follows:

```
Msiexec /i ProductName.msi /qn RUNVGO="YES"
ADDLOCAL="Core,Authenticators,SLA,LogonMgr,SetupMgr,SyncMgr,AD_
Sync,English_Pack"
```

2.18.1.3 Installing the MSI Package Remotely

To install Logon Manager to a computer remotely, verify that your system meets the following conditions:

- Windows Installer must be present on the remote computer.

- The MSI package must be accessible to the remote computer.

- The person performing the remote installation must have administrator access rights to the remote computer.

2.18.1.3.1 Editing the MSI Package Some organizations want to distribute MSI packages without Oracle-supplied optional components or with additional components (for

example, alternative authenticators). The Administrative Console includes an MSI Generator that you can use to create custom `MSI`s to suit the needs of your enterprise.

2.18.1.3.2   Adding Console-Created Application Logons and Global Agent Settings   You can also use the **Custom MSI Generator** to create a modified Logon Manager installation package. The modified `MSI` package you create with this feature can include:

- Selected application logons from an `entlist.ini` file or from the current Administrative Console configuration.

- Agent settings from an administrative overrides (`.ini`) file or from the current Administrative Console configuration.

To do this use the **Generate Customized MSI** command on the **Tools** menu.

> **Note:**   Use the Configuration Test Manager to verify that you have configured your Global Agent Settings correctly.

2.18.1.4 Microsoft Windows Installer (MSI) Package

Logon Manager ships as an `MSI` package, a standard format used by installers from Microsoft and other vendors. Many other installers can read `MSI` files. For information on the contents of the **Logon Manager Setup MSI**, see the *Oracle Enterprise Single Sign-On Suite Release Notes*.

You might want to create an `MSI` package to meet special requirements, such as:

- Providing custom applications and Logon Manager Agent configurations.

- Deactivating some options or components (for example, different authenticators) before end users install the Agent.

- Adding options or components to accommodate a complex environment, for example, one using biometric security devices or having an unusual network topology.

To meet these needs, there are these options:

- Use a command-line installation.

- Customize the installer package using the Administrative Console **Custom MSI Generator**.

- Include logons and Global Agent Setting configurations that you created in the Administrative Console in the installer.

> **Note:**   Use the Configuration Test Manager to verify that you have configured your Global Agent Settings correctly.

- Deploy using a third-party deployment tool.

2.18.2 Deploying the Agent with Anywhere

Anywhere provides a simple and flexible method for deploying configurations of Logon Manager, Authentication Manager, Provisioning Gateway, and Provisioning Gateway in any combination, all with little or no administrator involvement.

You can create as many configurations as necessary for members of your enterprise, and use Anywhere to take snapshots and compile complete deployment packages,

which you then distribute to the appropriate users. Anywhere also simplifies the upgrade and rollback process, all with virtually no hands-on involvement on your part.

See Chapter 3, "Configuring an Agent Deployment with Anywhere" for complete instructions to configure and deploy Logon Manager using the Anywhere component.

2.18.3 Using the MSI Generator

The MSI Generator enables you to create a custom `MSI` package to use for mass deployment to Logon Manager end-users, based on an existing `MSI` package.

Generate `MSI` is typically used to modify the Logon Manager installation package (`\Full\setup.msi` on the Logon Manager distribution disk) to include logons or settings in the initial desktop installation of Logon Manager. The `MSI` file you create can include:

- Selected application logons from an `entlist.ini` file or from the current Administrative Console configuration.

- Agent settings from an administrative overrides (`.ini`) file or from the current Administrative Console configuration.

To access this tool, select **Generate Customized MSI** from the **Tools** menu.

> **Note:** Before using this tool, in addition to reading this help information, Oracle strongly recommends that you refer to the *Oracle Enterprise Single Sign-On Suite Installation Guide* for a discussion of packaging Logon Manager for mass deployment.

There are three stages in the .MSI generation process:

1. **Base MSI Selection.** Select a **Base MSI** file.

2. **Selecting MSI Features.** Select the features to include in your custom `MSI` file.

3. **Selecting a Set of Global Agent Settings and Generating a New MSI.** Select the **Global Agent Settings** file to include, and an output file location.

2.18.3.1 Base MSI Selection

Upon opening this tool, the **Base MSI Selection** stage is selected in the left pane. All other stages are unavailable until the base `MSI` file is selected.

Element	Function
Base (MSI)…	The base installer package to customize. Type the filename or click the ellipsis ("**…**") button to select the .msi file.
Output (MSI)…	The customized installer package that you will send to end users. Type a filename or click the ellipsis ("**…**") button to select an existing .msi file.

1. In the **Path** field, click **Browse…**, navigate to the `MSI` file, and click **Open**. If an invalid `MSI` file is selected, a message appears indicating that the `MSI` file failed to open.

2. Click **Next >**, or select the stage in the left pane.

2.18.3.2 Selecting MSI Features

The **Feature Selection** stage becomes available after you select a valid `MSI` file. The features display in a tree structure.

Make your selections and click **Next >**, or select the **New MSI Generation** stage in the left pane.

There are three possible states for the check boxes:

- **Unchecked.** A state of no check in the parent node indicates that no child nodes are checked. The reverse is also true - if no child nodes are checked, the parent node is unchecked.

- **Partial Check.** If any (but not all) of the child nodes are checked, the parent reflects this with a partial check state. A partial check in a parent node indicates that at least one of the non-default child nodes is checked.

- **Checked.** If a parent is checked, all of its children are checked as well. The reverse is also true—if all of the children are checked, the parent is checked as well.

There might be some default items in the list that are required in the installer, and cannot be changed. An example of this is the **English** item in the **Languages** node in the Logon Manager `MSI` file. English is installed as the default language. Default items have no influence on the state of the checkboxes and are unavailable for selection.

2.18.3.3 Selecting a Set of Global Agent Settings and Generating a New MSI

The **New MSI Generation** stage becomes available after you select a valid MSI file. In this stage you choose the set of Global Agent Settings that you want to include, and Output location for the MSI file.

1. If you want to include a Global Agent Settings file in the MSI file, select it from the **Global Agent Settings** drop-down box. You can leave the default selection of **<None>** if you do not want to include a Global Agent Settings file.

2. In the **Output MSI** field, click the **Browse (…)** button. Select a valid path and enter a **File Name** for the output MSI file. Click **Save**. If you enter an invalid path or name, a message appears indicating that the output MSI file name is invalid.

3. Click **Generate**. A message appears indicating that the file has been saved. Click **OK**.
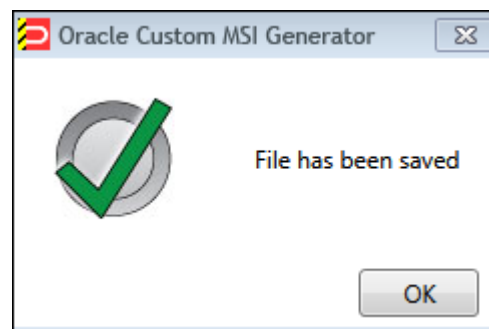
> **Note:** If an error occurs, ensure that you have entered a valid path and file name.

2.18.3.4 Testing and Deploying to End-Users

After you have tested and verified the MSI file fully, use a deployment tool (such as Microsoft Systems Management Server) to deploy Logon Manager enterprise-wide.

2.18.4 Using Other Deployment Tools

Logon Manager works with numerous deployment methods and tools, including (but not limited to):

- Manual installation (for example, from a CD-ROM or network share)
- Microsoft Windows Installer (MSI) service (local or remote installation)
- Network remote installation (for example, copy files and install registry entries remotely to a desktop)
- Microsoft SMS
- IBM Tivoli
- Attachmate NetWizard

- Intel LANDesk

- Novadigm Radia/EDM

- Novell ZENworks

- HP OpenView

- Seagate Desktop Management Suite

- McAfee ZAC Suite

- Veritas WinINSTALL

2.19 Using Kiosk Manager

Kiosk Manager delivers a secure, easy to use and easy to administer solution that addresses the needs of traditional single sign-on in a kiosk environment. Kiosk Manager has a client-side agent that provides user identification to the kiosk by prompting users to log on with a Windows password or any supported primary authenticator. The Agent suspends or closes sessions and seamlessly shuts down all applications after a specified period of inactivity.

The following topics are covered in this section:

- Events and Actions

- Session States

- About Desktop Manager

- Event and Audit Logs

- Configuring Strong Authentication Options

- Linking to Password Reset

- Command Line Options

- The .NET API

- Kiosk Manager Best Practices

The Administrative Console cannot run simultaneously with the Kiosk Manager Session Agent. If you launch the Session Agent while the Administrative Console is running, an error message displays saying, "Cannot run Kiosk Manager until Administrative Console is closed."

It is recommended that you do not use the Administrative Console on a workstation running Kiosk Manager.

2.19.1 Events and Actions

The following overview describes Kiosk Manager session functionality.

2.19.1.1 Types of Events

Kiosk Manager can be configured so that actions can be performed by any combination of the events below for all types of authenticators supported by Logon Manager:

- After Session Unlocked

- AM Device In

- AM Device Out

- AM Grace Period

- Authenticator Logon

- Authenticator Timeout

- Before Session Unlocked

- Cached Credential Session Start

- Session End

- Session Locked

- Session Start

- Timer Expired

- Transparent Screen Displayed

- Transparent Screen Hidden

- User Change

2.19.1.2 Configuring Events and Action Lists

Based upon the above events, Kiosk Manager can run a specified terminate list, launch a custom task (`.NET` application or script) through a run list, or specify a special action:

- Terminate list. A list of applications to be closed by Kiosk Manager on a specified event. (Previously known as black lists or applications to close on session end.)

- Run list. Either a `.NET API` to call or a script of command lines to be executed by Kiosk Manager on a specified event.

- Special actions list. Special action lists specify how to handle application windows, such as the positioning of the application and the order that this application has actions performed on it.

These features are configured through the Logon Manager Administrative Console under Kiosk Manager > Actions and Session States:

- An Action tells Kiosk Manager to do something, such as call a `.NET` method or terminate a specific application.

- Session States are a list of events, authenticators, and security settings to associate with actions. For example, a defined Session State can instruct Kiosk Manager to perform a specified list of actions when a session ends.

See the following sections for instructions on:

- Creating an Action List.

- Creating a Session State.

2.19.1.3 Creating an Action List

An action tells Kiosk Manager to do something, such as call a `.NET` method or terminate a specific application.

There are two ways to create an action list:

1. Open the Administrative Console.

2. Expand the **Kiosk Manager** node.

3. Click **Actions**.

4. Click **Add** or right-click and select **New Action**.
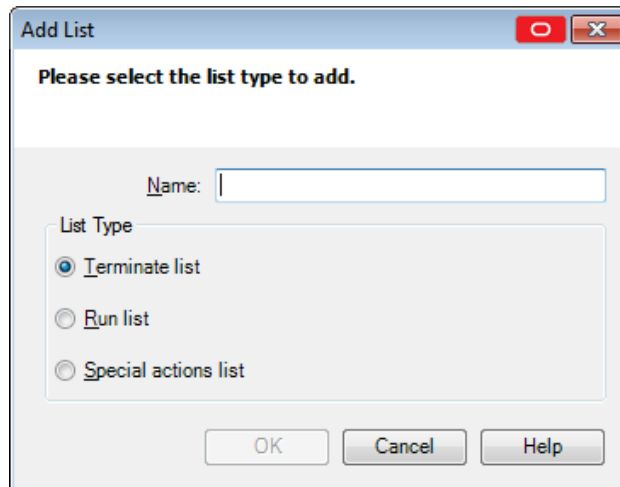
5. Enter a **Name**, and then select the **List Type**. Click **OK** when complete. The three types of actions lists are:

   ■ **Terminate List.** A list of applications to be closed by Kiosk Manager on session end.

   ■ **Run List.** Either a `.NET API` to call or a script of command lines for Kiosk Manager to execute.

   ■ **Special Action List.** Specifies how to handle application windows, such as the positioning of the application and the order of the actions performed on this application.

   > **Note:** For more information, refer to the specific list section for complete instructions on creating all lists.

Another way to create an action list is:

1. Expand the **Kiosk Manager** node.

2. Click **Session States**.

3. Select a Session State and click the **Actions** tab.

4. Click **Add**.

2.19.1.4 Creating and Using Terminate Lists

Use terminate lists to specify applications for Kiosk Manager to close on session end.
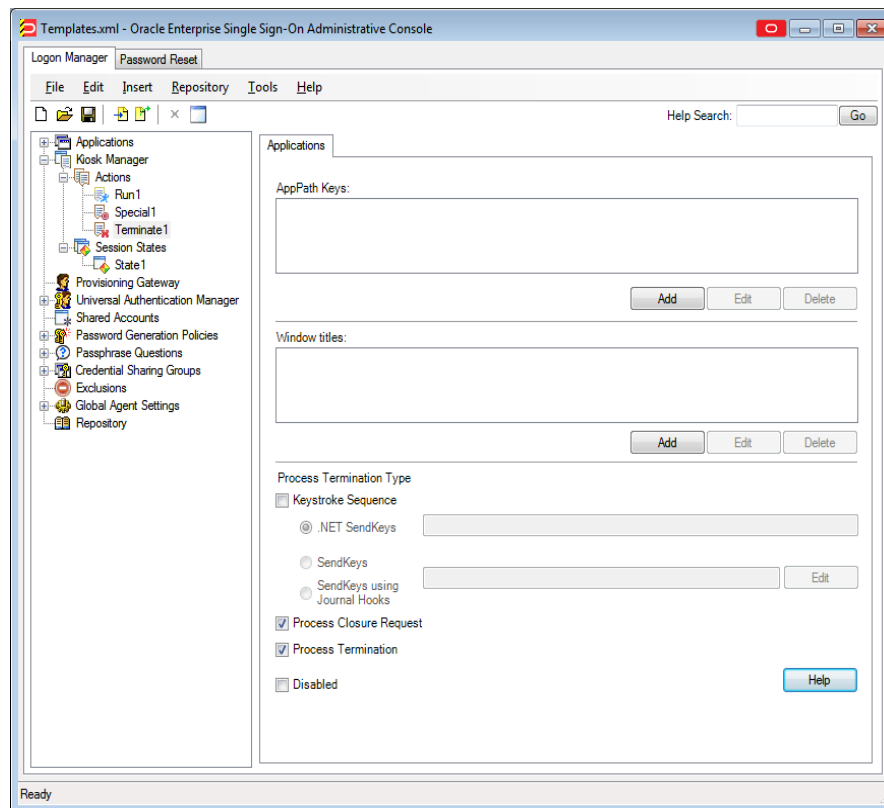
To display this tab:

1. Expand the **Kiosk Manager** node and select **Actions**.

2. Click on any **Terminate List**.

Control	Function
AppPathKeys	The Windows registry key identifying an application associated with this logon to match against running processes. (Usually the application executable's name, such as Notepad.exe)
Window Titles	Text matched against logon window titles to identify logon requests.

Control	Function
Process Termination Type	Select the methods of termination for applications to be closed on session end:
	■ Keystroke Sequence
	■ .NET SendKeys
	■ SendKeys: Configure fields by transmitting a keystroke series to the form. Click **Edit** to enter or change the series.
	■ SendKeys using Journal Hook: Configure fields by transmitting a keystroke series to the form using Journal Hook. Click **Edit** to enter or change the series.
	– Process closure requests
	– Process termination
	Note: When using keystroke sequences to terminate an application, a visual flicker occurs on the end user's screen. This flicker is a function of using SendKeys to terminate an application.
Disabled	Select this checkbox to disable this list. Disabling a list allows you to retain the settings in a list without deleting the original list, allowing you to refer to the settings and use them with other lists.

2.19.1.5 Configuring Kiosk Manager to Terminate an Application

To have Kiosk Manager terminate an application:

1. Under the **AppPath Keys** box, click **Add**. The **Process Path Key** dialog displays.

2. Enter a valid application key (usually the application executable's name, such as Notepad.exe). Click **OK**.

3. The application has been added to the list of applications to close on session end. Kiosk Manager will terminate these applications when a session ends.

4. Use the **Edit** and **Delete** buttons to modify or remove applications from this list.

5. In the Window Titles box, click **Add**. The **Windows Title** dialog appears.

6. Enter a valid windows title. Click **OK**.

2.19.1.6 Specifying a Window Title for Matching

To specify a window title for matching:

1. Enter (or edit) the exact Window Title.

2. Click **OK**.

2.19.1.7 Using SendKeys with Kiosk Manager

> **Note:** When using keystroke sequences to terminate an application, a visual flicker occurs on the end user's screen. This flicker is a function of using SendKeys to terminate an application.

Each key is represented by one or more characters. To specify a single keyboard character, use the character itself. For example, to represent the letter A, pass in the string "A" to the method. To represent more than one character, append each

additional character to the one preceding it. To represent the letters A, B, and C, specify the parameter as "ABC."

The plus sign (+), caret (^), percent sign (%), tilde (~), and parentheses () have special meanings to SendKeys. To specify one of these characters, enclose it within braces ({}). For example, to specify the plus sign, use "{+}". To specify brace characters, use "{{}" and "{}}". Brackets ([ ]) have no special meaning to SendKeys, but you must enclose them in braces. In other applications, brackets do have a special meaning that might be significant when dynamic data exchange (DDE) occurs.

To specify characters that aren't displayed when you press a key, such as ENTER or TAB, and keys that represent actions rather than characters, use the codes in the following table.

Key	Code
BACKSPACE	{BACKSPACE}, {BS}, or {BKSP}
BREAK	{BREAK}
CAPS LOCK	{CAPSLOCK}
DEL or DELETE	{DELETE} or {DEL}
DOWN ARROW	{DOWN}
END	{END}
ENTER	{ENTER}or ~
ESC	{ESC}
HELP	{HELP}
HOME	{HOME}
INS or INSERT	{INSERT} or {INS}
LEFT ARROW	{LEFT}
NUM LOCK	{NUMLOCK}
PAGE DOWN	{PGDN}
PAGE UP	{PGUP}
PRINT SCREEN	{PRTSC} (reserved for future use)
RIGHT ARROW	{RIGHT}
SCROLL LOCK	{SCROLLLOCK}
TAB	{TAB}
UP ARROW	{UP}
F1	{F1}
F2	{F2}
F3	{F3}
F4	{F4}
F5	{F5}
F6	{F6}
F7	{F7}
F8	{F8}
F9	{F9}

Key	Code
F10	{F10}
F11	{F11}
F12	{F12}
F13	{F13}
F14	{F14}
F15	{F15}
F16	{F16}
Keypad add	{ADD}
Keypad subtract	{SUBTRACT}
Keypad multiply	{MULTIPLY}
Keypad divide	{DIVIDE}

To specify keys combined with any combination of the SHIFT, CTRL, and ALT keys, precede the key code with one or more of the following codes:

- SHIFT +
- CTRL ^
- ALT %

To specify that any combination of SHIFT, CTRL, and ALT should be held down while several other keys are pressed, enclose the code for those keys in parentheses. For example, to specify to hold down SHIFT while E and C are pressed, use "+(EC)." To specify to hold down SHIFT while E is pressed, followed by C without SHIFT, use "+EC."

To specify repeating keys, use the form {key number}. You must put a space between key and number. For example, {LEFT 42} means press the LEFT ARROW key 42 times; {h 10} means press H 10 times.

> **Note:** In addition to the above SendKeys, there is also a wait command. The wait command is in the format {WAIT number} where "number" is the number of milliseconds delay. The wait can be anywhere in the string (that is, beginning, middle, end} and can be used as many times as needed.
>
> For example, if you want to send Ctrl+Shift+F7, then wait for 5 seconds, and then send Alt+F4, the format should be as follows:
>
> ```
> ^+{F7}{WAIT 5000}%{F4}
> ```

© 2001-2002 Microsoft Corporation. All rights reserved.

2.19.1.8 Creating and Using Run Lists

Use this panel to define either a .NET API to call or a script of command lines to be executed by Kiosk Manager.

1. Expand the **Kiosk Manager** node and select Actions.

2. Select a **Run** list.

Setting	Control	Function
.NET API	Assembly	Click the ellipsis "**…**" button to locate the .NET assembly to use. The assembly loads.
	Class	Select a `.NET` class using the drop-down box. The `.NET` classes listed will be those that are available in the selected assembly.
	Method	Select a method to call using the drop-down box. The `.NET` methods listed will be those that are available in the selected class. The method will be limited to the following signature and will not take any parameters or return any values: `void MethodName();` Unlike the script, processing will not continue until the method returns.
		See The .NET API for an example of a command line script. **Note:** `.NET API` calls are synchronous (Kiosk Manager waits for the call to complete).
Script		Enter a command line script for Kiosk Manager to execute. If this list contains multiple commands, each line starts without waiting for the previous task to terminate or checking the previous task's return code. **Note:** Command line calls are asynchronous (run in parallel to other tasks, including Kiosk Manager).
Disabled		Select this checkbox to disable this list. Disabling a list allows you to retain the settings in a list without deleting the original list, allowing you to refer to the settings and use them with other lists.

2.19.1.9 Creating and Using Special Actions Lists

Special action lists are used to specify how to handle application windows, such as the positioning of the application and the order that this application has these actions performed on it.

If an application window does not appear in a special actions list, it will be hidden.

To display this tab:

1. Expand the **Kiosk Manager** node and select Actions.

2. Click on any **Special Actions** list.

Control	Function
AppPathKeys	The Windows registry key identifying an application associated with this logon to match against running processes. (Usually the application executable's name, such as Notepad.exe.)
Window Titles	Text matched against logon window titles to identify logon requests.
Reposition Application	This setting and those below it allow you to specify the position of the application.The state of this checkbox determines if the actions listed below it will be applied to the application window.
	Options:
	■ Maximize
	■ Minimize
	■ Restore
	■ Move to: Enter the coordinates for the applications position.
	■ Resize: Enter the width and height for the applications position.

Control	Function
Sort Order	This setting determines the order in which special actions are executed. This ensures that windows which are brought to the foreground can be in a specific order with a preferred window displayed on top when multiple windows are repositioned.
Bring to foreground	This setting ensures that the application window is always first in the application windows order.
Shared Application	Check this box to enable an application to be shared among user sessions. For example, if "Notepad.exe" is designated as a shared application, if user1 opens a document in notepad and then locks the session, notepad will be running when user2 starts a session. If user2 then closes notepad and locks the session, notepad will no longer be running when user1 logs back on.
Disabled	Select this checkbox to disable this list. Disabling a list allows you to retain the settings in a list without deleting the original list, allowing you to refer to the settings and use them with other lists.

To configure an application:

1. Under the **AppPath Keys** box, click **Add**. The **Process Path Key** dialog displays.

2. Enter a valid application key (usually the application executable's name, such as Notepad.exe). Click **OK**.

3. The application has been added to the list of applications to close on session end. Kiosk Manager will terminate these applications when a session ends.

4. Use the **Edit** and **Delete** buttons to modify or remove applications from this list.

5. In the Window Titles box, click **Add**. The Windows Title dialog appears.

6. Enter a valid windows title. Click **OK**.

To specify a window title for matching

1. Enter (or edit) the exact Window Title.

2. Click **OK**.

2.19.1.10 Adding Applications with Process Path Keys

The **Process Path Key** is the name of the process executable; for example, IEXPLORE.EXE is the process path key for Internet Explorer. Use this dialog to add an application to the list of applications.

■ Enter a **Process Path Key** and click **OK**.

The **Process Path Key** is then created in the **AppPath Keys** dialog.

To display this tab:

1. In the left pane, click **Kiosk Manager** > **Actions**.

2. Click either:

   ■ **Terminate list**

   ■ **Special Actions list**

3. Click **Add**.

2.19.1.11 Selecting Default Applications to Leave Running

Use this dialog to add default applications to the list of applications to keep running on session end.

■ Select the desired applications to keep running on session end and click **OK**.

The selected applications are then listed in the **AppPath Keys** dialog.

To display this tab:

1. In the left pane, click **Kiosk Manager**.

2. Click **Actions**.

3. Select a **Keep running** list.

4. Click **Defaults**.

2.19.2 Session States

The Session States panel contains the list of existing Session States. Session States are a list of events to associate with an action. For example, a defined Session State might tell Kiosk Manager to perform a specific list of actions when a session ends.

2.19.2.1 Creating a Session State

To create a session state:

1. Open the Administrative Console.

2. Expand the **Kiosk Manager** node.

3. Click **Session States**.

4. Click **Add** or right-click and select **New Session State**.
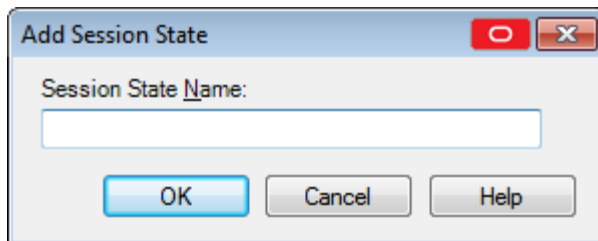
5. Type a Session State Name and click **OK**.

6. The new Session State is created. Each Session State has four tabs associated with it:

   ■ **Events**

   ■ **Authenticators**

   ■ **Actions**

   ■ **Security**

2.19.2.2 Copying a Session State

To copy a Session State:

1. Select a Session State.

2. Right-click **Make Copy** to quickly make a copy of this Session State. To change the name, right-click the Session State in the left pane and click **Rename**. You can also perform a copy by right-clicking the Session State in the left pane and clicking **Copy**.

2.19.2.3 Deleting a Session State

To delete a Session State:

1. Click **Delete** to delete a Session State. A confirmation message appears before the Session State is deleted.

2. Expand the **Kiosk Manager** node.

3. Right-click the Session State that you want to delete. Then either:

   ■ From the context menu, select **Delete**.

     or

   ■ From the context menu, select **Edit**, then select **Delete**.

2.19.2.4 Selecting Session State Events

The **Events** tab contains a list of all the possible events that Kiosk Manager can respond to and the option to add custom events. Each listed event has a checkbox next to it that when checked indicates that the associated action lists should be executed when this event occurs. When a new Session State is created, Session End is checked by default.

To display this tab:

1. Expand the **Kiosk Manager** node.

2. Click **Session States**.

3. Create an event in one of the following ways:

   ■ Select the predefined events for this Session State.

     or

   ■ Create your own custom events by clicking the **Add** button. Use the **Edit** button to edit the custom event name and the **Delete** button to delete a custom event.

   The following figure contains a list of the pre-defined events available to you.
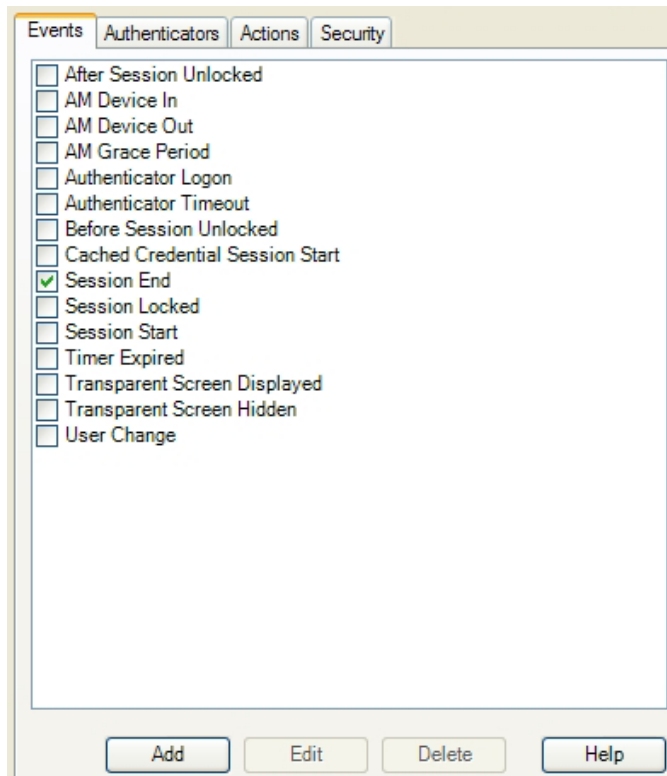
2.19.2.5 Selecting a Predefined Event

From the **Events** tab, select from:

- **After Session Unlocked**

  This event runs when the user unlocks their session after authentication has taken place. If an authentication is canceled, this event will not be triggered.

- **AM Device In**

  This event is triggered when the SSO device monitor is enabled and detects a monitored authenticator (for example, a smart card is inserted or a biometrics device is in range).

- **AM Device Out**

  This event is triggered when the SSO device monitor is enabled and detects a monitored authenticator (for example, a smart card is removed or a biometric goes out of range). This event will only be triggered when:

  – A session is open or locked

  – A "Device-In" event started the session

- **AM Grace Period**

  This event is triggered if an authenticator which uses a grace period function is being used and a user returns to an open session within the grace period.

- **Authenticator Logon**

  This event is triggered when an authenticator has accepted a logon. For example, the correct password for WinAuth or the correct PIN for smart card is entered.

- **Authenticator Timeout**

This event is triggered when Logon Manager's internal timer has expired.

- Before Session Unlocked

  This event is triggered when a user unlocks a session before authentication takes place.

- Cached Credential Session Start

  This event is triggered when a session is started and the user has cached credentials stored on the local computer.

- Session End

  This event is triggered when the session ends and the timer expires, or when another user starts a session.

- Session Locked

  This event is triggered when a user manually locks the session via the system tray.

- Session Start

  This event is triggered when a user starts a new session.

- Time Expired

  This event is triggered when the locked session timer has reached 00:00:00.

- Transparent Screen Displayed

  This event is triggered when the transparent lock initiates and the screen is visible to the user in locked mode.

- Transparent Screen Hidden

  This event is triggered when the transparent lock is ending.

- User Change

  This event is triggered when a user logs on to Kiosk Manager. This event sets two properties on the .NET object if they exist:

  – UserName. The sync user name.

  – DomainName. The sync domain name.

  If the properties do not exist, nothing happens

  > **Note:** Authentication Manager events run when the authenticator sends a message to Kiosk Manager indicating the event type.

2.19.2.6 Adding a Custom Event

To add a custom event, click the **Add** button on the **Events** tab. The **Custom Event** dialog appears:

1. Enter an **Event Name**. This is the event name that displays.

2. Enter an **Event Value**. An external application generates the custom event, sending a message to the Kiosk Manager hidden window. The value is the custom value that the other application sends.

3. Click **OK**. The custom event is created.

2.19.2.7 Selecting a Session State Authenticator

The Authenticators tab contains a list of all the authenticators that Logon Manager supports as well as the option to add a custom authenticator. Each authenticator has a checkbox next to it that when checked indicates if the associated action lists should be executed when the selected events occur and the selected authenticator was used to authenticate the user.

When a new Session State is created, all authenticators are checked by default.

There are two ways to select authenticators:

- Create your own custom authenticator by clicking the **Add** button. Use the **Edit** button to edit the custom event authenticator and the **Delete** button to delete a custom authenticator.

- Select the pre-defined authenticator for this Session State. Available authenticators are:

  - Authentication Manager

  - Entrust

  - ESSO-UAM: Challenge Questions

  - ESSO-UAM: Fingerprint

  - ESSO-UAM: Proximity Card

  - ESSO-UAM: Smart Card

  - ESSO-UAM: Windows Password

  - LDAP

  - LDAP v2

  - Proximity Card

  - Read-Only Smart Card

  - SecurID

  - Smart Card

  - Universal Authentication Manager

  - Windows Logon (deprecated)

  - Windows Logon v2

    > **Note:** To configure Kiosk Manager to use the Universal Authentication Manager authenticator, you must set Kiosk Manager to broadcast/monitor for token events. To do this, set the following registry key to a value of 2 (Always):
    >
    > ```
    > HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix\SM\Agent
    > ```

To display this tab:

1. Expand the **Kiosk Manager** node.

2. Click **Session States**.

3. Select a Session State and click the **Authenticators** tab.

2.19.2.8 Adding a Custom Authenticator

Custom authenticators allow you to filter events based on that authenticator. To add a custom authenticator, click the **Add** button on the **Authenticators** tab. This opens the Custom Authenticator dialog:

1. Enter an **Authenticator Name**. This is the authenticator name that displays.

2. Enter an **Authenticator Value**. The authenticator value is the name that the authenticator is known by within the code. This name comes from the authenticator itself. For example, the value for Windows Authenticator v2 is MSAuth and for Smart Card is SCAuth.

3. Click **OK**.

To display this dialog:

1. Expand the **Kiosk Manager** node.

2. Click **Session States**.

3. Select a Session State and click the **Authenticators** tab.

4. Click **Add**.

2.19.2.9 Using the Actions Tab to Add Session States

The **Actions** tab contains a list of all the actions associated with a specific Session State. This panel is empty for newly-created Session States. After you associate actions with the Session State, the actions appear in this panel.

Use this panel to create, associate, edit and delete actions.

To display this tab:

1. Expand the **Kiosk Manager** node.

2. Click **Session States**.

3. Select a **Session State** and click the **Actions** tab.

To use the **Actions** tab:

- To define a new action list, click **Add**. There are two types of action lists: **Terminate** lists and **Run** lists. A new action that you create from this panel is automatically added to this session state.

- To associate a defined action with this Session State, click **Associate** and select an action from the list.

- To make changes to an action, highlight it and click **Edit**.

- To delete an action from a Session State, click **Delete**. This deletes the action only from the current Session State, not the actions list.

2.19.2.10 Associating Actions to a Session State

Use the **Select Actions** dialog to select one or more actions to associate to this Session State.
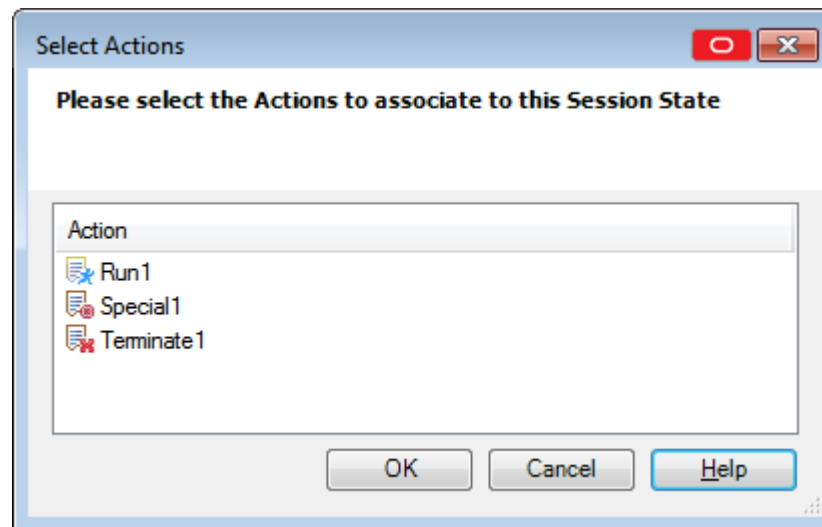
Select the actions to add to this Session State (use **Ctrl+Click** or **Shift+Click** to select multiple entries). Click **OK**.

> **Note:** If actions are associated with this Session State and you are adding new actions, you must reselect ALL actions; otherwise the previous list of actions will be replaced with the newly-selected actions.

To display this tab:

- In the left pane, click **Kiosk Manager**.

- Click **Session States**.

- Select a session state and click the **Actions** tab.

- Click **Associate**.

2.19.2.11 Configuring Session State Security

Use the **Security** tab to set the access rights for this Session State. You can assign access rights to these items:

- Application logons (including associated credential sharing groups)

- Password generation policies

- Global Agent settings

- Passphrase question sets

> **Note:** The security tab is available only if Role/Group security is enabled.

Control	Function
Directory	Select the target directory server.
Access information	
Name	Lists the groups or users who currently have access to this Session State.
ID	The user account name.
Access	Indicates whether the user or group has read/write or read-only access rights to the currently selected Session State. To change a user or group's access rights, right-click the user or group and select **Read** or **Read/Write** from the shortcut menu.
Action	
Add	Displays the **Add User or Group** dialog (for LDAP or Active Directory) to select the users or groups who should have access to the currently selected Session State.
Remove	Removes selected user(s) or group(s) from the list. Select a user or group to remove; use **Ctrl+Click** or **Shift+Click** to select multiple entries.

To display this tab:

1. Expand the **Kiosk Manager** node.

2. Click **Session States**.

3. Select a Session State and click the **Security** tab.

2.19.3 About Desktop Manager

The Desktop Manager is the logon dialog that manages the Kiosk Manager sessions on the kiosk. End users can start and unlock sessions from this dialog. Administrators can terminate sessions, shut down the computer, restart the computer, and exit Kiosk Manager.

> **Note:** The Desktop Manager is configured through the Administrative Console under Global Agent Settings > Kiosk Manager. The following sections contain all the necessary information to configure these settings.

2.19.3.1 Administration Menu

The Administration menu is located on the top of the Desktop Manager.
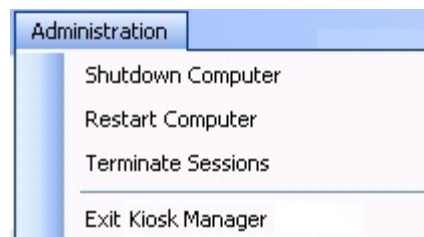
The settings that are used to configure this menu are:

- Restart Computer

  Options are **Yes**, **No**, or **Administrator must supply password**. Default is **No**.

- Shutdown Computer

  Options are **Yes**, **No**, or **Administrator must supply password**. Default is **No**.

- Allow administrator to close Kiosk Manager

  Options are **Yes** or **No**. Default is **Yes**. This setting controls the **Exit Kiosk Manager** option and the **X** in the title bar.

> **Note:** If the Kiosk account does not have sufficient privileges, the **Restart Computer** and **Shutdown Computer** options may not work even if they are disabled.

2.19.3.2 Session Termination

In addition to providing an administrator with rights to close sessions, there are other session termination settings you can configure. For information about configuring these settings, see Global Agent Kiosk Manager Settings.

2.19.3.3 Open Sessions (Multi-Sessions)

The Desktop Manager includes a list that displays all open sessions. Multiple sessions can be running at one time. There is no maximum amount of sessions. For information about configuring these settings, see Global Agent Kiosk Manager Settings.

2.19.3.4 Transparent Screen Lock

The transparent lock feature provides the ability to lock desktop inputs (keyboard and mouse) in view mode, so for example, a monitoring application can be viewed without starting a session. It is similar to the screen saver functionality. When Kiosk Manager invokes the transparent lock, the desktop and applications on the desktop continue to display on the monitor in real time. Transparent lock is disabled by default.

When there are multiple sessions running, the last active session is displayed when transparent lock engages.

Application priorities and positioning are configurable in the Special Actions lists.

Transparent lock events are set up in the Events panel of the Session States section.

- Transparent Screen Displayed

  This event is triggered when the transparent lock initiates and the screen is visible to the user in locked mode.

- Transparent Screen Hidden

  This event is triggered when the transparent lock is hidden.

Transparent lock can be invoked in the following ways:

- Timeout

- Canceling out of an authentication ONLY if **Transparent Display After Cancel** is set to **Enable**.

To initiate a session while transparent lock is running, move the mouse or click any keyboard button. If **Transparent Only Recognize Ctrl-Alt-Delete** is set to **Enable**, users will have to click **Ctrl+Alt+Delete** to disengage Transparent Lock.

> **Note:**   Transparent screen lock is configured through the Administrative Console on the Global Agent Settings > Kiosk Manager > User Interface panel.

2.19.3.5 Terminating Sessions

Administrators can terminate Kiosk Manager user sessions from the Desktop Manager by clicking Terminate Sessions from the **Administration** menu. This menu option is not configurable.

When you click **Terminate Sessions**, the **Authenticate as Administrator** dialog appears, prompting you to enter administrative credentials before performing this action.

After you submit your credentials, the **Terminate Sessions** dialog appears.
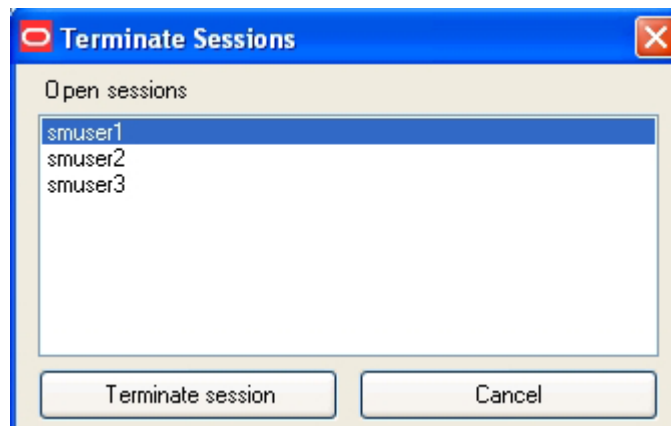
You can select only one session at a time. Select **Cancel** and use the **X** to close this dialog.

2.19.3.6 Customizing the Desktop Manager

The Desktop Manager can be customized in several ways. Refer to the following sections for more information about each option.

- General Custom User Interface Options. See Global Agent Settings Kiosk Manager User Interface.

- Upload a background image around the logon dialog. See Setting the Kiosk Manager Background Image.

- Add a custom text message around the logon dialog. See Global Agent Kiosk Manager Message Settings.

- Replace the Oracle and Kiosk Manager logo banner on the logon dialog. You may choose to display a company logo as the background image, or an important custom text message to inform your users of any important information. See Replacing the Logo Banner.

The information in the following section provides instructions to replace the logon dialog logo banner and an example of a customized desktop.

2.19.3.6.1 Replacing the Logo Banner You can modify the Oracle Kiosk Manager logo banner on the Desktop Manager logon dialog through a manual step. To replace the logo:

1. Create a `branding` folder within the `SMAgent.exe` home directory.

2. Place the customized logo banner in the branding folder with the name `banner.gif`.

3. The customized banner appears the next time you start Kiosk Manager.

2.19.3.6.2 Examples of a Customized Background Image and Text Message

Customized Background Image on an 800x600 Display

The following screen shot illustrates the horizontal and vertical dimension of the **Desktop Manager** logon dialog and the coordinates and dimensions used to position it.
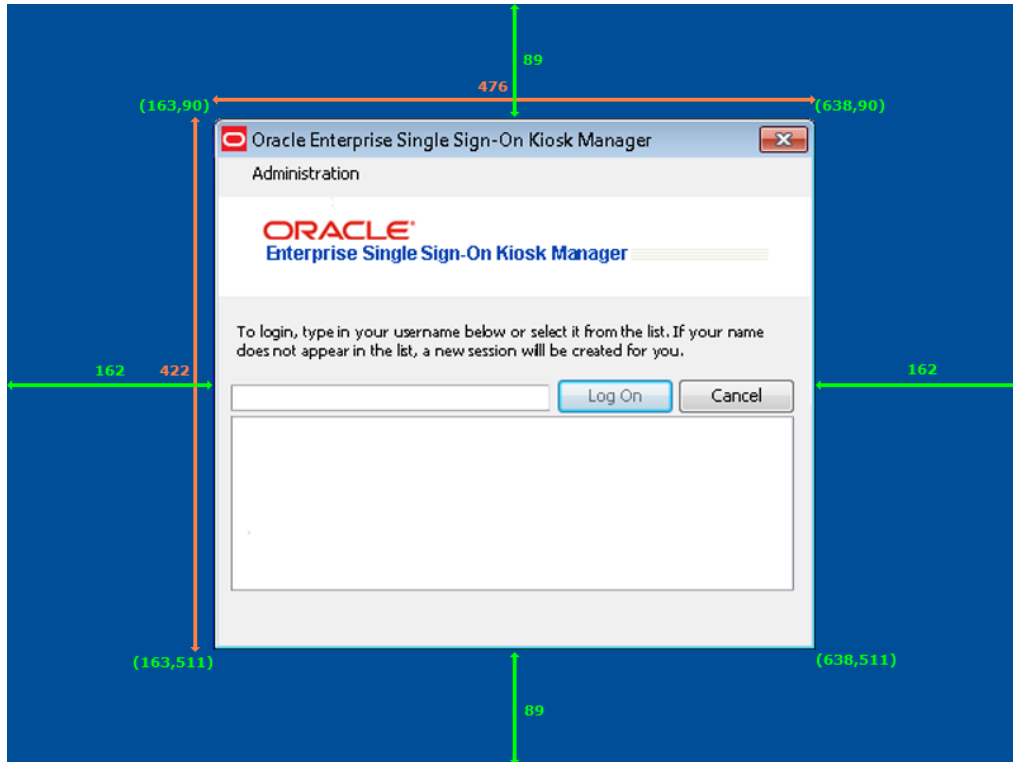
Customized Text Message on an 800x600 Display

The following screen shot illustrates an example of a text message. This text message displays the values used to customize the text message as seen in this screen shot.
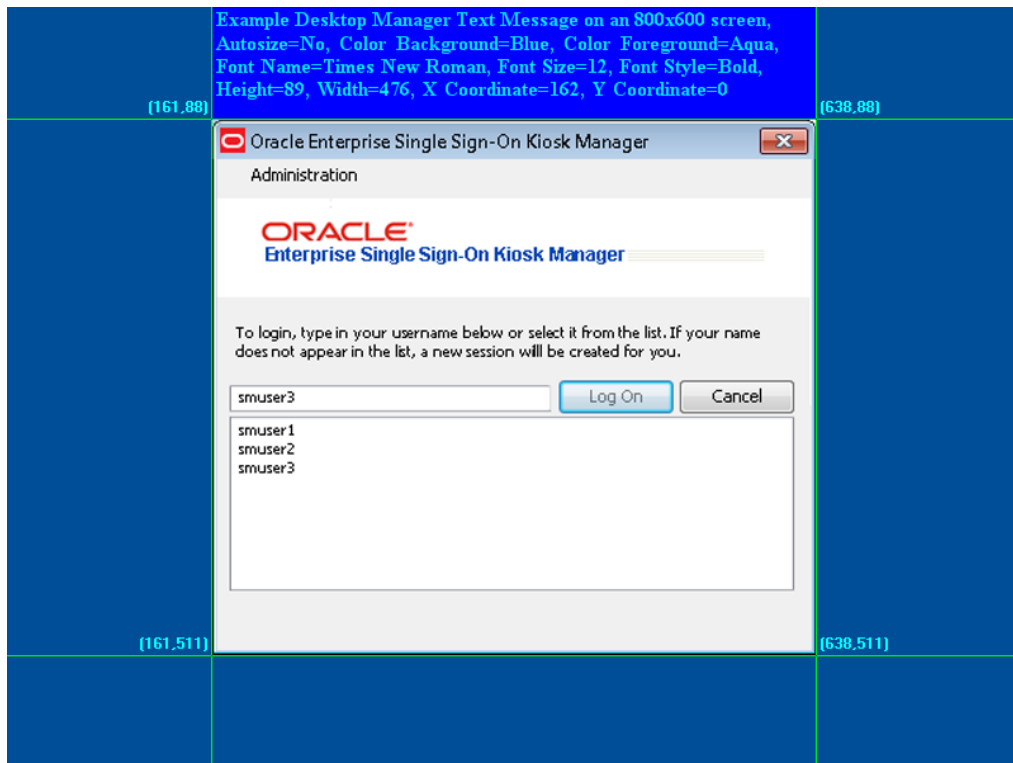
The following screen shot displays the actual values used to produce the text message as seen above.

2.19.3.7 Desktop Status Window

The **Desktop Status** window is a small window that displays during a Kiosk Manager session. It allows you to conveniently view the current session owner and lock the session. If enabled, its default location is the upper right corner of the desktop during a session.

The **Desktop Status** window is hidden by default. The default values are calculated at runtime. The window is placed in the upper-right hand corner of the display with 10 pixels between the edge of the window and the physical edge of the screen. See Global Agent Settings Kiosk Manager User Interface for instructions to customize this window's appearance and location.

2.19.4 Event and Audit Logs

Kiosk Manager logs agent events to the local machine's Windows Event Viewer. This functionality is enabled by default. For a list of Kiosk Manager events that you can log, see Event Log Messages.

Kiosk Manager can also log events to a Syslog server application on the local kiosk machine or a remote machine.

To configure Syslog through the Agent installer:

> **Note:** This step must be performed before installing Kiosk Manager.

1. Launch **Add-Remove Programs** from the Control Panel.

2. Click on **Oracle Enterprise Single Sign-On Logon Manager** and click **Change**.

3. Select **Modify** on the **Program Maintenance** panel.

4. On the **Custom Setup** panel, expand **Extensions**, and then expand **Event Manager**.

5. Select **Syslog** for installation.

6. Follow the prompts to complete installation of Syslog.

To configure Syslog through the Administrative Console:

1. Open the Administrative Console, expand **Global Agent Settings** > **Audit Logging** > **Syslog Server**.

2. Configure the settings for the target Syslog machine according to your environment. If logging to a remote machine, specify either a hostname or IP address of the remote machine in the **Destination Host** setting.

3. Navigate to **Global Agent Settings** > **Kiosk Manager**. Under the **Audit Logging** section, enter the **Event log name** and **Event log machine name**.

2.19.4.1 Event Log Messages

The following table lists the messages that currently are logged in the Event Viewer for applications:

Message	Notes About Message (if Applicable)
User session started: domain/username	When a user session is started.
User session ended: domain/username	When a user session ends.
User session locked: domain/username	When a session is locked.
User session unlocked: domain/username	When a session is unlocked.
Process action: action type, action name	(IE, Terminate list, notepad_close)
	This corresponds to the session actions in the repository. If the action does not have a corresponding state that triggers, you should not see the action logged in the event viewer.

Message	Notes About Message (if Applicable)
Process state: state name, event GUID	(IE, Session_locked, {6D5B7645-25A5-42f3-B641-BFE4DC4F774C})
	This corresponds to the Session States in the repository. A log entry is only generated if a state is triggered, such as a session lock. The GUID corresponds to the GUID for that state, if you viewed the state from the Administrative Console. For example, if you have a state in the repository for Transparent Lock but you do not have Transparent lock turned on, you should not see an event logged.
Transparent lock screen DISPLAYED	When transparent lock displays.
Transparent lock screen HIDDEN	When transparent lock is hidden.
Method Invocation: file path/file name, method name	Corresponds with Run List .Net API Assembly name and method.
Run list command: command name	Corresponds with Run List Script commands.
The following applications were not terminated:	This will only log applications that are specified in a terminate list and did not terminate.
Kiosk Manager STARTED	When Kiosk Manager is started.
Kiosk Manager SHUTDOWN	When Kiosk Manager is shut down.
Successfully closed: Application name	Applicable to all three closure methods in the terminate list—keystroke sequence, closure request, and process termination.
	This event is logged when the application in a terminate list is closed. Logs are not generated for applications that are closed but not specified in a terminate list.

2.19.4.2 Bypassing the Kiosk Manager Agent

If necessary, you can bypass the Kiosk Manager Agent when a kiosk starts up.

The Kiosk Manager Agent will not start if you hold the **Shift** key down when logging into the computer.

2.19.4.3 Closing the Kiosk Manager Agent

If necessary, the Kiosk Manager Agent can be closed on a kiosk by:

- Pressing **ALT + F4** on the keyboard.

- Clicking **Exit Kiosk Manager** from the **Administration** menu on the Desktop Manager.

- Clicking the **X** located on the top right of the window title bar.

The administrator is then prompted to enter his or her credentials. Only an administrator's credentials will succeed in closing the agent.

This feature is disabled by default. To enable this feature:

1. Open the Logon Manager Administrative Console, expand **Global Agent Settings** > **Kiosk Manager**.

2. Check **Allow administrator to close Kiosk Manager**.

3. Select **Yes**.

2.19.4.4 Setting Up a Trust

Kiosk Manager has the capability to allow other applications that trust Kiosk Manager authentication to retrieve the logged-on username. Kiosk Manager provides a public function in `SSOUserInfo.dll` with the following function signature:

`extern "C" BOOL _stdcall GetUserId(BSTR* bstr);`

Parameters:

`bstr`

Object into which to retrieve the username.

Return Value

Returns `TRUE` if the function succeeds and a user is currently logged in.

Returns `FALSE` if the function fails. Use `GetLastError()` for more information.

If the function succeeds, the username will be returned as: `"DomainName\UserName"`

> **Note:** Kiosk Manager can be set up to run a command line or call a
> `.NET` method after a user successfully starts a session. Utilize this
> mechanism to trigger the other application to request the logged-on
> username from Kiosk Manager.

2.19.4.5 Using the MacListener Utility to Enable Caregiver Mobility and Oracle VDI Session Support

The MacListener utility enables Kiosk Manager to interface with Caregiver Mobility and Oracle VDI environments, allowing health-care professionals to log on to kiosk systems to access location-specific information, such as patient data or other local resources pertinent to the kiosk system's location. MacListener.exe ships with Oracle Enterprise Single Sign-On Suite and is located in the "Utility" sub-folder of the "Logon Manager" folder of the suite master archive.

MacListener.exe is a command-line utility that emulates the echo server by listening on a specific TCP/IP port for incoming client connections, receiving the client's MAC address in plain-text form, and running a specified command when a client disconnects with the client's MAC address appended to the end of the specified command in the following format:

`/MACADDRESS=xx:xx:xx:xx:xx:xx`

where `xx:xx:xx:xx:xx:xx` is the client's MAC address.

The syntax for using the `MacListener.exe` utility is as follows:

Parameter	Description
`/PORT <port_number>`	Specifies the port number on which to listen for incoming client connections.
`/DEBUG`	Displays error messages.
`/E <command>`	Command to execute upon client disconnection. The MAC address received from the client will be appended to the end of the command in the format that follows.

For example, if you launch the utility as follows:

```
MacListener /PORT=8080 /E=C:\Windows\Notepad.exe
```

and a client with a MAC address of `12:AB:34:CD:56:EF` connects to the utility on port `8080`, then the utility will execute the following command when the client disconnects:

```
C:\Windows\Notepad.exe /MACADDRESS=12:AB:34:CD:56:EF
```

2.19.5 Configuring Strong Authentication Options

The Administrative Console's Global Agent Settings > Kiosk Manager: Strong authenticator options allow you to configure how Kiosk Manager integrates with strong authenticators.

See Global Agent Kiosk Manager Settings for strong authentication options, and the Universal Authentication Manager section, Integrating with Kiosk Manager, for detailed information on integrating Kiosk Manager with Universal Authentication Manager.

2.19.6 Linking to Password Reset

You can add a link to Password Reset on the Kiosk Manager Desktop Manager. This allows users to reset their own kiosk passwords (for example, Microsoft Active Directory via LDAP authentication) using Password Reset.

Clicking this banner launches the Password Reset Web interface. Users can then follow the prompts to reset their password.

A link to the Password Reset client can be installed as a DOS command, using the following command syntax:

```
msiexec /i [/q] c:\ESSO Kiosk Manager 7.000.msi programURLs
```

`/q Quiet mode`: suppress all installer user-interface messages. Refer to the description of other Windows Installer command-line options for msiexec at http://msdn.microsoft.com.

`programURLs` (required):

```
REG_RESETURL=" http://host/vgoselfservicereset/resetclient/default.aspx"
```

```
REG_STATUSURL="http://host
/vgoselfservicereset/resetclient/checkstatus.aspx"
```

where: `host` is the server name (or domain name or IP address) and path of the folder that holds the Password Reset service root folder.

2.19.7 Command Line Options

Command-line options are available to support non-kiosk environments and allow Kiosk Manager to run on a desktop machine without presenting a user interface.

```
/EVENT <EventName1> [EventName2…]
```

This option triggers the named event and Kiosk Manager performs the tasks associated with the event and terminates. The authenticator filters are ignored.

```
/RUN <ListName1> [ListName2…]
```

This option triggers Kiosk Manager to perform the tasks associated with the named list and terminate. The event and authenticator filters are ignored.

`ListName` can be either a Session State or an Action.

For example, `"SMAgent/run StartVisualSourceSafe"`

Some things to keep in mind when using the command line:

- Any `SessionAction` or `SessionState` names that have spaces in them must be enclosed in double quotes.

- Some command-line options prevent others from working. For example, multiple lists can be run with the `/RUN` command. If `/LOCK` appears on the command line, the session is locked and the rest of the command line is ignored, including any options that appeared before `/LOCK`.

- `/SHUTDOWN`, `/LOCK`, and `/TERM` are the command-line options that cause Kiosk Manager to ignore the rest of the command line.

- The `/RUN` and `/EVENT` commands trigger Kiosk Manager to treat the rest of the command line as event and list names to be run. These will be run when all of the command line options have finished processing. The type of the parameter depends on the previous command. The command-line parameter type resets with the next `/EVENT` or `/RUN` parameter received. For example:

```
SMAgent /Event "SM session start" "SM session end" /RUN termlist1
termlist2 runlistA "My SessionState"
```

This command line will run the lists associated with events `"SM session start"` `"SM session end"` and run the named lists: `termlist1`, `termlist2`, `runlistA` and `"My SessionState"`.

2.19.8 The .NET API

Externally Callable Interfaces and Methods

A class named KioskAPI is available within the SMAgent.exe that is loaded by external programs.

The object is instantiated as follows:

```
Passlogix.SM.Manager.KioskAPI kiosk = new
Passlogix.SM.Manager.KioskAPI();
```

The following methods are available:

```
void Lock();
void Term();
void Shutdown();
void Event(string eventName);
void Run(string runtaskName);
```

- **Lock.** Locks the current Kiosk Manager session.

- **Term.** Ends the user's session as if the Kiosk Manager timer expired for a user.

- **Shutdown.** Terminates the `SMAgent.exe`.

- **Event.** Simulates the named event to occur, causing Kiosk Manager to perform tasks associated with the named event without filtering by the authenticator. Event names are the `GUID` strings from `Events.xml`.

- **Run.** Starts the named task without filtering by the event or authenticator. Task names are the SessionAction and SessionState names that are displayed by the Administrative Console.

> **Note:** Any SessionAction or SessionState names that have spaces in them must be enclosed in double quotes:
>
> ```
> kiosk.Run("\"My SessionAction\"");
> ```

Example to run tasks associated with the `"SM Session End"` event:

```
Passlogix.SM.Manager.KioskAPI kiosk = new

Passlogix.SM.Manager.KioskAPI();

if (kiosk != null)

kiosk.Event("{A644ED55-6A3F-4160-A355-C713C90733DF}");
```

> **Note:** Also see the .NET API Sample Code.

2.19.8.1 .NET API Sample Code

Following is sample code for the `.NET API` using C# with properties for the "User Change" event.

```
using System;

using System.Collections.Generic;

using System.Text;

using System.Windows.Forms;

namespace ClassLibraryTest

{

public class TestClass

{

private string m_userName;

private string m_domainName;

public string UserName

{

set

{

m_userName = value;
```

```
}

get

{

return m_userName;

}

}

public string DomainName

{

set

{

m_domainName = value;

}

get

{

return m_domainName;

}

}

public void UserChange()

{

MessageBox.Show("UserChange called with user: " + DomainName + "\\" +
UserName);

}

public void SessionStart()

{

MessageBox.Show("SessionStart called");

}

public void SessionEnd()

{

MessageBox.Show("SessionEnd called");

}

public void SessionLocked()

{

MessageBox.Show("SessionLocked called");

}

public void SessionUnlocked()

{

MessageBox.Show("SessionUnlocked called");
```

```
}

public void PreSessionUnlocked()

{

MessageBox.Show("PreSessionUnlocked called");

}

public void AuthLogon()

{

MessageBox.Show("AuthLogon called");

}

public void AuthTimeout()

{

MessageBox.Show("AuthTimeout called");

}

public void DeviceIn()

{

MessageBox.Show("DeviceIn called");

}

public void DeviceOut()

{

MessageBox.Show("DeviceOut called");

}

public void GracePeriod()

{

MessageBox.Show("GracePeriod called");

}

}

}
```

2.19.9 Kiosk Manager Best Practices

These best practices are recommendations that will help you implement an optimal Kiosk Manager configuration.

2.19.9.1 Deploying Kiosk Manager Settings

The most convenient way to mass deploy Kiosk Manager settings from the Administrative Console is to create a customized MSI package and distribute it to end user kiosk workstations using a deployment tool of your choice.

> **Note:** Administrative Overrides are not available for use with Kiosk Manager settings.

2.19.9.2 SendKeys

SendKeys is not a reliable method and therefore not guaranteed to work as expected. It is recommended that you do not use SendKeys.

2.19.9.3 Disable Task Manager and Run

The Windows Task Manager and Run menu option are disabled programmatically as a function of the Kiosk Manager Registry Service. For added security, we recommend disabling these functions for any user account that you plan to use with a Kiosk Manager kiosk user account.

To remove the **Run** menu option from the **Start** menu:

1. Open the **Group Policy** editor by double clicking on `gpedit.msc` (`C:\WINNT\system32\gpedit.msc`)

2. Navigate to **User Configuration** > **Administrative Templates** > **Start Menu and Toolbar**.

3. In the right pane double-click **Remove Run** from the **Start** menu.

4. Select **Enabled** and click **Apply** and **OK**.

To disable Task Manager:

1. Open the **Group Policy** editor by double clicking on `gpedit.msc` (`C:\WINNT\system32\gpedit.msc`)

2. Navigate to **User Configuration** > **Administrative Templates** > **System** > **Ctrl+Alt+Delete Options**.

3. In the right pane double-click **Remove Task Manager**.

4. Select **Enabled** and click **Apply** and **OK**.

2.20 Provisioning Gateway Overview

Provisioning Gateway provides the ability to remotely add, modify, and delete application credentials directly within each user's Logon Manager credential store, eliminating the need for local credential capture and granting the user instant access to the target application. The Universal Authentication Manager Management Console is a standalone, browser-based application. See the separate guide, *Administering Oracle Enterprise Single Sign-On Provisioning Gateway* for instructions to configure and use this component.

You can configure provisioning in the following ways:

■ From the **Provisioning** node of the Administrative Console, define provisioning rights for each new application you create.

■ From the **Provisioning** tab of a selected application, add or remove rights, and copy rights to other applications.

To access the Provisioning Gateway Administrative Console, open a Web browser and enter this URL (replacing `serverhost` with the server where Provisioning Gateway was installed):

```
https://serverhost/Provisioning Gateway console/overview.aspx
```

2.20.1 Managing Provisioning

Use this node to manage provisioning rights for users. There are two tabs to set the rights:

- **Default Rights**

- **Admin Rights**

When you change the settings in this node, you must publish them to the repository in order for them to take effect. Right-click the node and select **Publish**.

2.20.1.1 Provisioning Default Rights Tab

Use this tab to define standard provisioning rights for each new application created. After you create an application, change the rights as needed.

Control	Function
Directory	Select the target directory server.
Access information:	
Name	Lists the groups or users who currently have access to this item.
ID	Lists the user account name.
Access	Indicates the permissions that have been granted to the user or group (Add, Modify or Delete Logon). To change a user or group's access rights, right-click the user or group and select **Add Logon**, **Modify Logon**, or **Delete Logon** from the shortcut menu.
Actions:	
Copy permissions to…	Use this button to apply the provisioning rights for the current application to multiple applications. Click to display a list of all available applications, and select those to which you want to copy these provisioning rights. Use **Ctrl+Click** or **Shift+Click** to select multiple entries. Click **OK**.
Add	Displays the **Add User or Group** dialog (for LDAP or Active Directory) to select the users or groups to grant access to the currently selected item.
Remove	Removes selected user(s) or group(s) from the list. Select a user or group to remove; use **Ctrl+Click** or **Shift+Click** to select multiple entries.
Directory	Select the target directory server.

2.20.1.2 Add User or Group Dialog

The **Add User or Group** dialog varies based on the directory server being used:

- LDAP

- Active Directory

- AD LDS (ADAM)

2.20.1.2.1 LDAP Use this dialog to select the individual users or user groups that are to be added to the access list for the current configuration item (Add Logon, Modify Logon, or Delete Logon).

Control	Function
Search Base	The base (highest-level) directory to begin searching for user/group accounts. All subdirectories of the base directory are searched. Type a location or click **Change** to browse the directory tree.

Control	Function
Change	Displays the **Select Search Base** dialog to browse for a base directory for the search. Use this dialog to browse to and select the base (highest-level) directory to search for user/group names. Click **OK** when finished.
Search	Begin searching the base directory for users and groups.
Users or Groups	Lists the search results. Select the names to be added to the access list for the current configuration item. Use **Ctrl+Click** or **Shift+Click** to select multiple entries. Click **OK** when finished to copy your selections to the access list.

2.20.1.2.2 Active Directory/AD LDS (ADAM) Use this dialog to select the individual users or user groups that are to be added to the access list for the current configuration item (Add Logon, Modify Logon, or Delete Logon).

Control	Function
List Names From	Select an Active Directory domain or server.
Names	Lists the names of users and groups for the selected domain or server. Select one or more names to add to the access list.
Add	Copies user(s) and group(s) selected in the **Names** list to the **Add Names** list. Use **Ctrl+Click** or **Shift+Click** to select multiple entries.
Members	When a group is selected in the **Names** list, displays the **Global Group Membership** dialog, which lists the members of the selected group.
Search	Displays the **Find Account** dialog for searching one or more domains for a specific user or group.
Add Names	Displays the names of the user(s) or group(s) you have selected for addition to the access list for the current configuration item. Click **OK** to finalize the addition.
	Note: You can type or edit user names in this list. However, entries are checked for invalid account names, and duplicate account selections are automatically removed when you click **OK**.

2.20.1.3 Provisioning Admin Rights Tab

Use this tab to grant the user general administrative rights to the Provisioning Gateway Administrative Console.

Control	Function
Directory	Select the target directory server.
Access information:	
Name	Lists the groups or users who currently have access to this item.
ID	Lists the user account name.
Access	Indicates the administrative rights that have been granted to the user or group (**Delete SSO User** or **Map Templates**). To change a user's or group's access rights, right-click the user or group and select **Delete SSO User** or **Map Templates** from the shortcut menu.
Actions:	

Control	Function
Copy permissions to…	Use this button to apply the provisioning rights for the current application to multiple applications. Click to display a list of all available applications, and select those to which you want to copy these provisioning rights. Use **Ctrl+Click** or **Shift+Click** to select multiple entries. Click **OK**.
Add	Displays the **Add User or Group** dialog (for LDAP or Active Directory) to select the users or groups to grant access to the currently selected item.
Remove	Removes selected user(s) or group(s) from the list. Select a user or group to remove; use **Ctrl+Click** or **Shift+Click** to select multiple entries.
Right-clicking on a server name in the list opens a context menu that allows you to perform any of the following:	
Remove	Removes the server from the **Server** list.
Publish…	Launches the **Publish to Repository** dialog, which allows you to choose from several objects and locations to publish.
Publish To	Allows you to select a single repository directly from the menu item; publishing occurs automatically after you select the repository.
Delete SSO User	Rescinds a user's access to an OPAM-enabled account.
Map Templates	Allows an administrator to map SSO templates to OPAM targets. Right-click on a user in the list, and select **Map Templates** from the context menu to grant the user mapping permissions.

2.20.2 Oracle Privileged Accounts Manager (OPAM)

The **OPAM** tab contains a root node that allows you to connect to an OPAM server and a target repository. The server contains OPAM targets, and the repository contains Logon Manager templates and the mapping object.

> **Note:** If Logon Manager is synchronizing to an Active Directory repository and is using the "local computer credentials" option, you must enable sharing credentials from the authenticator to the Active Directory synchronization extension ("ShareCredsToSyncs") in the Global Agent Settings.

To configure the Administrative Console support for OPAM:

1. Enter the **URL** of the server that contains OPAM targets. If you've previously entered URLs in this field, they will be available to select from the dropdown list.

2. Enter your **Username** and **Password**.

3. Select the target repository:

   a. Click the **Browse…** button.

   b. In the **Connect to Repository** dialog, enter the server name, select a repository type, enter the port number, your username, and password. Check the box if this is an SSL connection. Then click **Apply**.

   c. In the **Browse for Repository** dialog, expand the desired DC node under the server, and select **OU-SSO**. This is where the ESSO configuration objects (COs) and mapping objects are stored. Click **OK** when done.

> **Note:** If the mapping object does not already exist, it will be created here.

4. Click **Apply**. The plug-in initiates an attempt to connect to the OPAM server and target repository.

5. When connection is successful, a **Template Mapping** node appears in the left navigation pane under OPAM.

When you select **Template Mapping** in the left navigation, the right pane displays a list of OPAM targets and their mapped templates. To change a target map:

1. Select the target from the list and click **Edit**.

2. In the **Edit Mapping** dialog, select a different template from the Available templates list.

3. Click **OK** to close the window. The selected target now appears in the list with the new template in the **Mapped Template** column. If for some reason, the change does not appear automatically, click the **Refresh** button to update the list.

Control	Function
OPAM Server URL	Enter the URL of the OPAM server. The Administrative Console remembers previously entered URLs; they are available in the dropdown list.
Username	Enter your username.
Password	Enter your password.
Target repository	Click the **Browse…** button to launch the **Connect to Repository** dialog. Use this dialog to specify the server name and other repository information required.
Apply	Click **Apply** to save the OPAM configuration information you entered in the previous fields.

3

Configuring an Agent Deployment with Anywhere

This section describes the procedures and settings in the Anywhere Console, and how to use them to create an Agent deployment for your end-users.

In this chapter, you will learn about the following:

- Overview of Creating a Deployment Package
- The General Tab
- The Options Tab
- The Generate Tab

3.1 Overview of Creating a Deployment Package

Following is the general procedure for creating a deployment package. Use the settings in the three tabs of the Anywhere Console for your deployment configurations. See the section for each tab for an in-depth discussion of that tab's settings.

3.1.1 A Few Notes About Anywhere Prerequisites and Deployment Limitations

Consider the following when planning your deployment options:

- Anywhere is designed for compatibility with Windows Authenticator v1. It is not designed to work with Logon Manager features that require installing system services or GINAs, adding registry entries outside of `Live HKLM\Software\Passlogix`, or additions to Program Files or Windows system folders.

- The Visual C++ Runtime Library and .NET 2.0 Framework are prerequisites for running Anywhere. The installation package includes the Visual C++ Runtime Library, however you must make the .NET 2.0 Framework available to users. See the *Oracle Enterprise Single Sign-On Suite Release Notes* for a complete list of software and hardware requirements.

- The final output of the deployment package is not a `.MSI` file. You must ensure that you supply any additional requirements that your end users will need to run their Logon Manager and additional Agent software.

- Due to security restrictions in Windows Server 2008 and Windows 7, you must change group policy settings in order for end users running these clients to use the Anywhere deployment package. See the Technical Notes in the *Oracle Enterprise Single Sign-On Suite Release Notes* for more information.

- Anywhere does not support Kiosk Manager. When you install Logon Manager with the intention of using it to create a deployment. Do not select the Kiosk Manager option.

- You must be running a 32-bit operating system when creating a 32-bit deployment, and a 64-bit operating system when creating a 64-bit deployment. Moreover, a 32-bit deployment downloaded to a 64-bit operating system, or a 64-bit deployment downloaded to a 32-bit operating system, will fail.

3.1.2 Creating a Deployment Package

1. Create a certificate file to be submitted when you generate the deployment package. See Section 7.1.2, "Obtaining a Certificate for SSL Connectivity" for complete instructions.

2. Install the Administrative Console and Agent on a clean workstation.

3. Optionally, install Provisioning Gateway.

4. Configure the Oracle products as you want them for deployment.

5. Make your Logon Manager and Provisioning Gateway configuration settings available to Anywhere by one of the following methods:

   - **Live Registry.** Write the Global Agent Settings to the registry, and select **Live registry** under **Options** > **Agent** settings.

   - **Exported Registry File (.REG).** The Administrative Console .REG file is not immediately compatible with Anywhere. If you want to use this file, you must do the following:

     a. Open Microsoft Registry Editor (`regedit.exe`).

     b. Open the Administrative Console registry file from within regedit.exe.

     c. Save the Administrative Console registry file using `regedit.exe`.

     d. Browse to this file for your selection on the **Options** tab > Agent settings.

     Note: The Console produces a `.REG` file compatible only with 32-bit systems. If you are merging the `.REG` file on a 64-bit system, you must run the following command to move the merged registry data to the correct location within the registry (otherwise, Universal Authentication Manager will not function):

     ```
     reg.exe COPY HKLM\Software\Passlogix
     HKLM\Software\Wow6432Node\Passlogix /s
     ```

     Test your configuration before proceeding to create the deployment package.

     ---

6. Install the Anywhere Console. Anywhere reads the Oracle software configuration on the workstation where you installed it.

7. Verify in the **General** tab that the products and versions installed are the ones that you want to deploy.

8. From the **Options** tab, specify:

   - The deployment version and location, the installation location, and the installation type.

- ■ The update schedule preferences.

- ■ Which registry settings Anywhere will use (the settings from the live registry, or the registry file you saved using regedit.exe).

9. On the **Generate** tab:

   a. In the **Summary** window, review all settings.

   b. Enter the directory path where the deployment package will be created, or click the B**rowse…** button to navigate to the directory.

   c. Click the **Generate** button.

   d. At the prompt, enter the location for the certificate file that you created, and the password.

10. From the **File** menu, click **Save** or **Save As…** to save the deployment configuration settings.

11. Copy the deployment package to the virtual directory or file share that you specified in the **Target location** setting.

12. If deploying from a web server, customize the index.html file in the deployment directory, replacing the generic text with the information that you want end users to see.

13. If this is a first installation, notify users that the deployment package is available.

14. To create additional deployment packages, reconfigure settings on the Administrative Console, and click **New** on the Anywhere **File** menu.

Note: Users do not have the option to alter the installation. If you want different users to install different packages, create a separate deployment package for each installation.

3.2 The General Tab

The two sections of the **General** tab contain information about the Oracle products installed on the workstation where you are creating the deployment package.
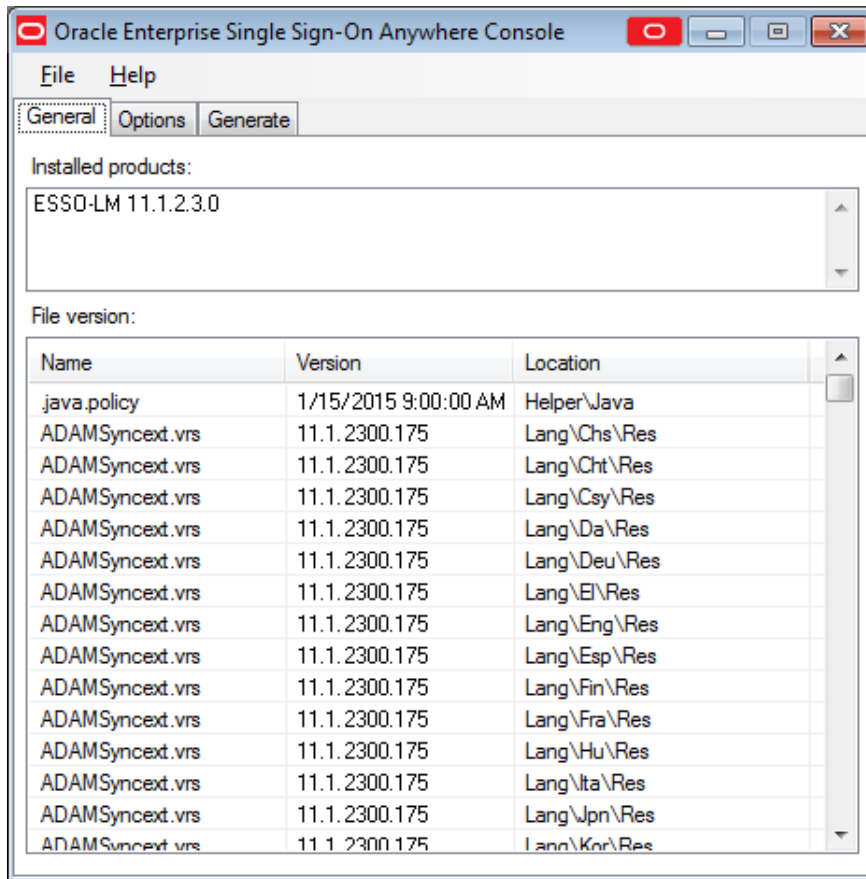
Window Region	Function
Installed products	This section lists the Oracle products in the configuration. This list must contain Logon Manager and might also include Provisioning Gateway.
File version	This section lists all components that were installed as part of the Oracle product installation, with their version numbers and installation locations. This information is the same as the information in the Logon Manager "About" box.

3.3 The Options Tab

Use the **Options** tab to configure the settings for your deployment package.
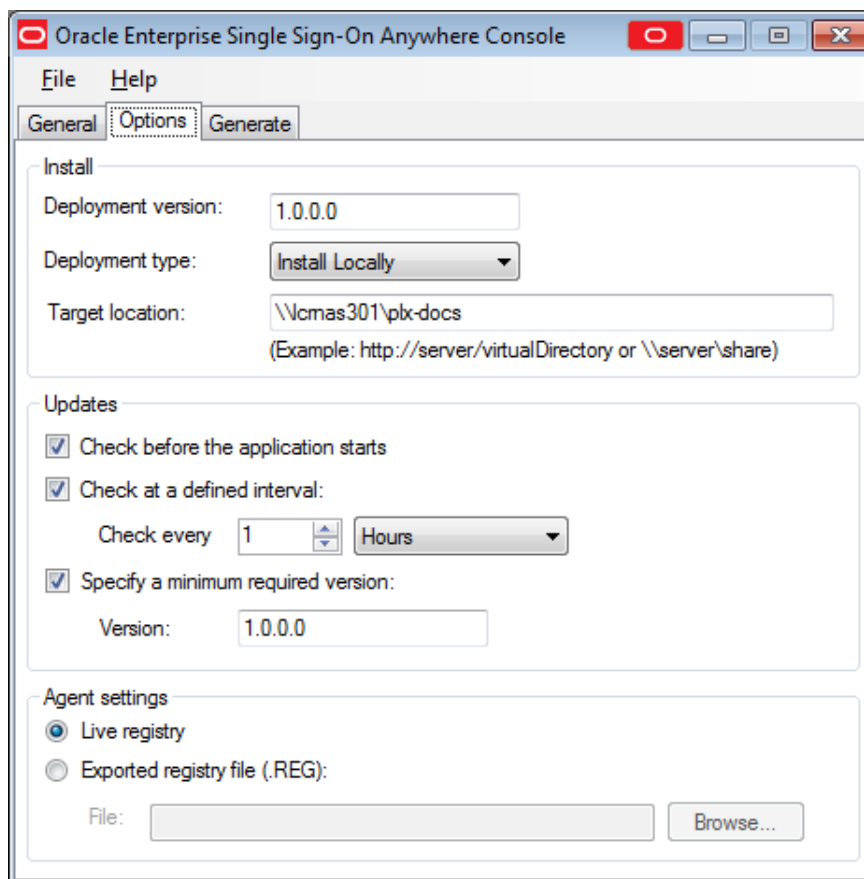
3.3.1 Install Settings

Use the settings in the **Install** group to configure the deployment version and file locations.

Setting	Function
Deployment version	Specify the four-field (x.x.x.x) version number of the deployment. It is your choice whether to match the deployment version to the version of Logon Manager that you use for the deployment.
Deployment type	Specify whether Anywhere will install on the local workstation.
	The Install Locally option creates a shortcut icon to Anywhere in the user's **Start** menu and adds an entry for Anywhere to the user's **Add or Remove Programs** applet on the Control Panel.
	The **Online** option is a per-session deployment and does not create the Start menu shortcut or add an entry to **Add or Remove Programs**. It also requires the user to have access to the web server or file share where the Anywhere deployment package is located in order to run Anywhere. The files will be cached on the user's machine, but the user cannot run the program directly.
Target location	Enter the virtual directory or file share from which Anywhere will be distributed.

3.3.2 Updates Settings

Use the settings in the **Updates** group to specify when Anywhere should check for updates, and whether the user has the option to reject them when they are available.

> **Note:** If the user declines an optional update, Anywhere does not offer that update again.

Setting	Function
Check before the application starts	Check this box to have Anywhere check for updates to any of the installed files before the application launches. Anywhere updates only files that have changed.
Specify a minimum required version	Check this box to enforce a minimum deployment version. This setting is useful for rollbacks. Anywhere rolls back only one version. If you want to roll back beyond the previous deployment, rename the desired rollback to a higher version than currently installed, and specify this new version as the minimum required. Rollbacks are available through Control Panel > Add or Remove Programs > Change > Restore.
Check at defined intervals	Check this box to specify a time interval at which Anywhere checks for updates. Configurable intervals are from one hour to one year (52 weeks).

3.3.2.1 Localized Deployments

In order for localized installers and update notifications to appear in the correct language, you must have the appropriate .NET language pack installed on the workstation. To install a .NET language pack:

1. Log on to the local workstation.

2. Install the latest Microsoft .NET Framework if it is not already present (version 2.0 or above is required).

3. Download and install the target .NET language pack for your version of the .NET Framework.

4. Restart the workstation.

5. Install Anywhere.

The installer appears in the target language.

3.3.3 Agent Settings

Use the settings in the "Agent Settings" group to specify which registry settings Anywhere should use.

Setting	Function
Live registry	Select to use the same settings as in the Anywhere live registry.
Exported registry file (.REG)	Select to use a custom registry that you created in the Administrative Console and exported. If you select this option, click the **Browse…** button to direct Anywhere to the desired registry file.

> **Note:** The Console produces a `.REG` file compatible only with 32-bit systems. If you are merging the `.REG` file on a 64-bit system, you must run the following command to move the merged registry data to the correct location within the registry (otherwise, Universal Authentication Manager will not function):
>
> ```
> reg.exe COPY HKLM\Software\Passlogix
> HKLM\Software\Wow6432Node\Passlogix /s
> ```

3.4 The Generate Tab

Use the **Generate** tab to view a summary of your configuration settings, specify a location for your deployment output, and generate your deployment package.
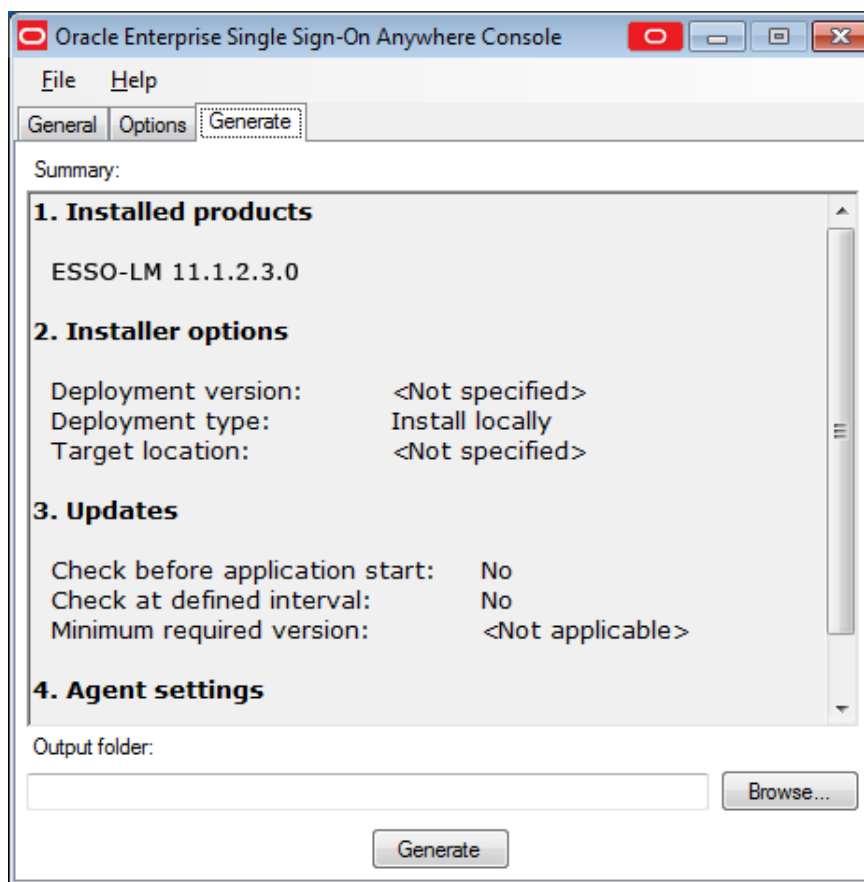
Setting	Function
Summary	Review the settings in the **General** and **Options** tabs.
Output folder	Enter the path of the directory where you want to generate the Anywhere deployment, or click the **Browse…** button to navigate to the desired directory.
Generate	After you review your settings and specify the location of the deployment package, click the **Generate** button to create the Anywhere deployment package.

> **Note:** Before distributing the deployment package, verify that it works correctly.

The Anywhere installation includes a customizable index.html file. Edit this file with the information to direct end users to the deployment package, and distribute it.

4

Using the Administrative Console to Configure Password Reset

This chapter describes the Password Reset settings in the Administrative Console, and how to use them to configure repositories, connections, and the Enrollment Interview and Reset Quiz for your end-users.

This section covers the following procedures:

- First-Time Setup
- Setting Up the Enrollment Interview
- Configuring Reset Authentication
- Password Complexity
- Alerts
- Logging
- Reporting
- Configuring the Enrollment User Interface
- Configuring the Reset User Interface
- Managing Users
- Managing Resets
- Working with External Validators

4.1 First-Time Setup

After you have installed the Password Reset server application, the first task is to configure the service for use with the directory-server or relational database and Web services. You perform this first-time configuration with the dialog pages in the **System** tab:

- Use the Reset Service tab to set the Anonymous Logon account-the user account through which Password Reset users and administrators access the service.
- Use the Storage tab to configure the directory or database to create the Password Reset repository for system questions and user data.
- Use the Reset Service tab to set the Service account-the user account that Password Reset "logs on as" to the server.

When you have completed these steps, you can begin configuring the reset service itself. These tasks include:

- Setting up the Enrollment Interview by supplying a set of system questions and associated point values

- Setting the general reset service options. These options include the pass and fail score thresholds, user-lockout parameters, and administrator.

4.1.1 Configuring Service Storage

Use the **Storage** tab (under the **System** node) to view or change connection settings for the database (SQL Server or Oracle Database) or directory service (Active Directory or AD LDS (ADAM)) that you use as the repository for Password Reset system questions and user enrollments. To do this, use the settings in the Storage Configuration group. When you have completed your changes, click **Submit** to apply your new settings to Password Reset.

You also use the **Storage** tab to have Password Reset perform the first-time setup tasks that prepare the database or directory-server repository for use with the enrollment and reset services. These tasks include:

- Extending the schema to include directory types/database tables

- Creating the main container or database

- Granting read/write access to the Web service account

- Creating required child objects or tables.

To perform these tasks, use the controls in the Initialize Storage group:

1. Select **Initialize storage for Password Reset**.

2. For **Connect as User Name**, enter the user name of an administrator of the directory server.

3. Enter the administrator password.

4. Click **Submit** to save any changes or modifications. Your changes will be lost if you do not click the **Submit** button before closing the **Storage** tab.

The following table provides information on the types of services used for storage.

Storage Configuration	
Storage type	The type of service used. The remaining settings in this group change based on this selection.
	Options are:
	■ Active Directory
	■ AD LDS (ADAM)
	■ LDAP
	■ Oracle Database
	■ SQL Server

The following table provides information about configuring connection settings for Active Directory and AD LDS (ADAM).

Active Directory and AD LDS (ADAM) Storage Settings	
Servers	Click **Add** to launch the **Add Server** dialog, and enter the information required. Click **OK** to return to the **Servers** list.
	Password Reset attempts connections in the order that they appear in the list, from top to bottom. Use the up and down arrows to arrange the servers in the order in which connections should be attempted. To delete a server from the list, select the server in the list box and click **Delete**. Note that you cannot delete a connection if it is the only connection in the list.
	In some cases, such as long server names, the entire string is not displayed in the list box. Clicking an item in the list box populates the **Server Name/IP Address** and **Port** text boxes with that item. The full string can then be viewed by scrolling in the text box and, if desired, modified and added as a new connection to the list.
Server timeout (seconds)	Enter a value (in seconds) that Password Reset should wait for a response from a server before moving on to the next server in the list.
Storage location (DN)	The distinguished name or naming context of the connection node.
Use SSL	Select to enable a secure socket layer connection.

The following table provides information about configuring connection settings for LDAP.

> **Note:** For correct functionality of the **Enrollments** and **Resets** tabs when using Oracle Internet Directory (OID) as your repository, you must use the Catalog Management Tool included with OID to index the `createTimestamp` attribute.

LDAP Storage Settings

Servers	Click **Add** to launch the **Add Server** dialog, and enter the information required. Click **OK** to return to the **Servers** list.
	Password Reset attempts connections in the order that they appear in the list, from top to bottom. Use the up and down arrows to arrange the servers in the order in which connections should be attempted. To delete a server from the list, select the server in the list box and click **Delete**. Note that you cannot delete a connection if it is the only connection in the list.
	In some cases, such as long server names, the entire string is not displayed in the list box. Clicking an item in the list box populates the **Server Name/IP Address** and **Port** text boxes with that item. The full string can then be viewed by scrolling in the text box and, if desired, modified and added as a new connection to the list.
Username (DN)	Enter a name for the account that will communicate with the LDAP server. This must be in distinguished name (DN) format.
Password	Enter a password for the Username (DN) account.
Server timeout (seconds)	Enter a value (in seconds) that Password Reset should wait for a response from a server before moving on to the next server in the list.
Storage location (DN)	The distinguished name or naming context of the connection node.
Use SSL	Select to enable a secure socket layer connection.

The following table provides information about configuring connection settings for an Oracle Database.

Oracle Database Storage Settings

Database connections	Click **Add** to launch the **Add Connection String** dialog, and enter the information required. Click **OK** to return to the Servers list.
	Then to initialize storage:
	1. From the *Password_Reset_Server_install*\WebServices directory (for example, C:\Program Files\Passlogix\v-GO SSPR\WebServices), locate the OracleTables.txt file and copy it to the Oracle DBMS workstation.
	2. On the Oracle DBMS workstation, run the OracleTables.txt file, which will create the tables in Oracle that are necessary for the Password Reset storage repository.
	Note: Running this script will delete and re-create any existing Password Reset tables in Oracle DBMS.
	In the Password Reset node of the Administrative Console, go to System > Storage. Select **Oracle** as the storage type.
	3. Enter the connection string as noted above.
	Password Reset attempts connections in the order they appear in the list, from top to bottom. Use the up and down arrows to arrange the connection strings in the order in which connections should be attempted. To delete a connection string from the list, select the string in the list box and click **Delete**. Note that you cannot delete a connection string if it is the only connection in the list.
	In some cases, such as long database connection strings, the entire string is not displayed in the list box. Clicking an item in the list box populates the **Connection String** text box with that item. The full string can then be viewed by scrolling in the text box, and if desired, modified and added as a new connection to the list.
Database timeout (seconds)	Enter a value (in seconds) that Password Reset should wait for a response from a database before moving on to the next database in the list. This value is not used in database connections if the connection string contains a Connect Timeout parameter.

The following table provides information about configuring connection settings for a SQL Server.

SQL Server Storage Settings

Connection string	The complete connection string to the database server; for example:
	Provider=SQLOLEDB.1;Integrated Security=SSPI;Initial Catalog=SSPR;Data Source=Servername;Trusted_Connection=Yes
	Click **Add** to add the connection to the **Database Connections** list. Multiple connections can be added for failover support. If more than one connection is entered, Password Reset iterates through the list in sequential order until either it has successfully connected or all connections have failed.

SQL Server Storage Settings	
Database connections	Click **Add** to launch the **Add Connection String** dialog, and enter the information required. Click **OK** to return to the Servers list.

Password Reset attempts connections in the order they appear in the list, from top to bottom. Use the up and down arrows to arrange the connection strings in the order in which connections should be attempted. To delete a connection string from the list, select the string in the list box and click **Delete**. Note that you cannot delete a connection string if it is the only connection in the list.

In some cases, such as long database connection strings, the entire string is not displayed in the list box. Clicking an item in the list box populates the **Connection String** text box with that item. The full string can then be viewed by scrolling in the text box and, if desired, modified and added as a new connection to the list. |
| Database timeout (seconds) | Enter a value (in seconds) that Password Reset should wait for a response from a database before moving on to the next database in the list. This value is not used in database connections if the connection string contains a `Connect Timeout` parameter. |

The following table provides information on preparing the database or directory-server repository for initial setup.

Initialize Storage	
Initialize storage for ESSO-PR	Activates the first-time configuration tasks. If this option is checked, Password Reset automatically iterates through the new connections in the list and attempts to initialize them sequentially. If a connection fails to initialize, initialization stops and connections further down in the list will not be initialized. If this occurs, resolve the issue and then retry initialization.

Note for Oracle Database: Because of the steps you performed in the **Database Connections** section, this setting is unnecessary and unavailable for Oracle Database. You need only enter the following two settings. |
| Connect as (User Name) | The user name of a directory or database administrator. |
| Password | The password of the administrator. |

4.1.1.1 Adding a Server

To add a server:

- Enter the name or IP address and the port number for the server that holds the password reset information (users, password reset policies, enrollment questions and answers).

- Click **OK** to return to the **Storage Configuration** tab when you are finished.
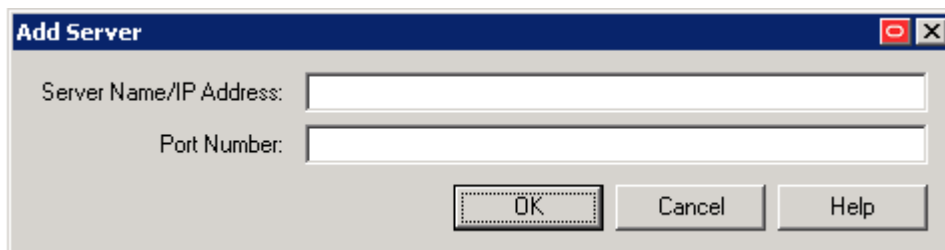
You can use multiple servers for failover support. If you enter more than one server address, Password Reset iterates through the list, in sequential order, until either it has successfully connected to a server or all connection attempts have failed.

4.1.1.2 Adding a Connection String

You must specify a connection string to the server that holds your password reset information (users, password reset policies, enrollment questions and answers). This must be the complete connection string for the database server; for example:

- For Oracle DB:

  ```
  Provider=OraOLEDB.ORACLE;Data Source=XE;User
  ID=system;Password=password
  ```

- For SQL Server:

  ```
  Provider=SQLOLEDB.1;Integrated Security=SSPI;Initial Catalog=SSPR;Data
  Source=Servername;Trusted_Connection=Yes
  ```

You can use multiple servers for failover support. If you enter more than one server address, Password Reset iterates through the list, in sequential order, until either it has successfully connected to a server or all connection attempts have failed.

To add a connection string:

1. Enter the connection string for the server that holds the password reset information (users, password reset policies, enrollment questions and answers).

2. Click **OK** to return to the **Storage Configuration** tab when you are finished.

4.1.2 Configuring the Reset Service Account

Use the **Reset Service** tab (under the **System** node) to set or change the Anonymous Logon for Internet Information Services (IIS) Web Services. This is the domain account through which all end users access the Password Reset Web interface.

The following figure shows the **Reset Service** tab with the **Status**, **Account**, **Listening Port**, and **Domain** fields populated.
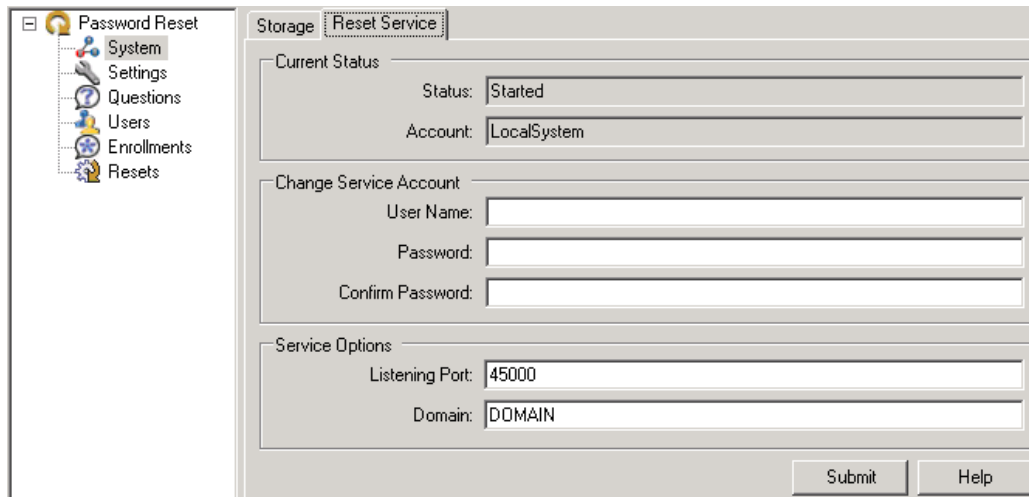
The Anonymous Logon account you specify in this dialog appears in the **Log On As** column of the Computer Management Services tool. The account should have local administrator privileges, including permission to perform the following tasks:

- Start, stop, and change services

- Read from and write to Active Directory, AD LDS (ADAM) instance, or database server

- Write to the local-machine registry (HKLM)

> **Note:** To create a new user account with administrator privileges, use the **Users and Groups** tool in the Windows Computer Management Console.

4.1.2.1 Setting or Changing the Anonymous Logon

To set or change the anonymous logon:

1. Enter the **User Name** and **Password** of the account that you want to use.

2. Enter the password again to confirm.

3. Click **Submit**.

Setting	Function
Status	Displays whether the reset service account is started. This field is informational only.
Account	Displays the current password reset account. This field is informational only.
User name	The user name you have designated for the reset service account.
Password and Confirm password	The password of the reset service account. Enter the password in both fields.
Listening port	The number of the port used to detect password reset activity (default is 45000).

Setting	Function
Domain	The trusted domain where user accounts are located. This setting is required only if the user accounts are in a domain other than that of the Password Reset machine's domain.
	Note: Changes to this setting take effect immediately and do not require a restart of the IIS or Password Reset Service.

4.2 Setting Up the Enrollment Interview

When the user starts the enrollment process, Password Reset displays the Enrollment Interview.

The Enrollment Interview comprises a series of questions in two groups:

- Required questions

- Optional questions

The required and optional questions are called system questions. System questions are predefined and managed by the administrator using the **Questions** tab of the Administrative Console. See Editing System Questions and Question Examples for more information.

When the end user has answered enough questions to meet the defined enrollment level, the Enrollment Interview ends.

If the user skips any optional questions, they may not meet the enrollment level threshold. If this scenario occurs, Password Reset begins the optional question set again, prompting the user to answer any questions they may have skipped.

4.2.1 Enrollment Level Settings

The Enrollment Level is specified on the **Settings** tab. This feature allows the administrator to set the total points value that end users must accumulate in order to complete the enrollment interview process, called the authentication threshold. This threshold removes the previous requirement that the administrator had to configure required questions with enough total value in points to meet the Authentication Success Level (**Settings** > **Authentication thresholds**).

Password Reset allows administrators to configure questions with enough points to meet the Enrollment Level by counting both the required and optional questions. The Enrollment Level must be at least equal to the Authentication Success Level. With both the Enrollment Level and Authentication Success Level thresholds, users have the flexibility to select questions they want to answer out of a pool of questions.

During the enrollment interview, starting questions can be optional or required. A progress bar shows the user's progress (in percentage) in satisfying the enrollment level threshold.

If users reach the end of the question set without enough points to meet the enrollment level, Password Reset displays the message, "You have not answered enough optional questions to satisfy the enrollment requirement. In order to complete the enrollment process, you must continue to answer questions until the progress bar reaches 100%." Password Reset will then begin the optional question set prompting users to answer questions they previously skipped.

4.2.2 National Language Support

The initial enrollment dialog can be presented in the preferred language for each business unit as required by National Language Support (NLS). NLS is required for all languages supported by Password Reset.

The welcome text that appears on the initial page of the English enrollment interview is stored in an XML file called `UserText.xml`. The XML file names for the localized welcome pages take the form: `UserText.language_code.xml`, where `language_code` is replaced with the language code as denoted in the RFC 1766 format used by .NET. For example, the German XML file is named `UserText.de.xml`, the French XML file is named `UserText.fr-ca.xml`, and so forth. The files are stored in the `\WebServices` folder. Password Reset loads all the files with the above naming pattern and uses the appropriate version to display the 'Welcome' screen of the enrollment page.

On the client side, the Windows interface passes the language the user installed within the URL to tell Password Reset to show the enrollment page in that language.

For a complete list of language codes, see Section 7.3.4, "Password Reset Client-Side Registry Settings".

4.2.3 Questions Tab

Use the **Questions** tab to review and modify the current set of system questions. You can create new questions, set their language, set their point-values, set Required/Optional status, set answer sources and validity checks on the end user's answers, and select Users and Groups to allow or deny access.

You can modify the text, language, and weights of existing questions. You can also disable system questions—that is, remove them from the Enrollment Interview. Questions that you disable from the Enrollment Interview will still appear in the Reset Quiz to end users who have already provided answers to the disabled question, but they will no longer be presented to users who subsequently enroll or re-enroll.

See Creating System Questions, Editing System Questions, and Setting Up the Enrollment Interview for more information.

4.2.4 Creating System Questions

Use the **System Questions** tab (under the **Questions** node) to create system questions for the Enrollment Interview. For instructions to edit questions, including enabling/disabling and changing question weights, see Editing System Questions. For suggested text and settings, also see Question Examples.

> **Note:** Password Reset stores the answers to the Enrollment Interview in encrypted form in the repository using the one-way SHA-1 hash algorithm. Additionally, 16 random bytes of entropy are added to enrollment answers before hashing.

To create a new system question:

1. In the **System Questions** tab, select the **Language** in which to enter the question. The default language is always available. Password Reset offers the following language options.

- English (default)
- Brazilian Portuguese
- Czech
- Danish
- Dutch
- Finnish
- French/Canadian French
- German
- Greek

- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese
- Romanian

- Russian
- Simplified Chinese
- Slovak
- Spanish
- Swedish
- Thai
- Traditional Chinese
- Turkish

You can enter and configure the same questions in multiple languages. When you navigate to this tab and select a language from the drop-down list, your questions display in whichever language you select.

As you add questions to this list, the line directly below the window keeps a running tally of the potential points a user can accumulate with correct and incorrect answers. The line appears in red type until you add questions with enough points for a user to reach the authentication threshold that you specified on the **Settings** tab.

2. Click **Add** to launch the **Edit Question** dialog and begin entering and configuring questions.

4.2.4.1 Assigning Point Values to Questions

Secure implementation of self-service reset depends on the selection and weighting of the individual system questions. Here are some primary considerations for each question:

- **How secret the answer is**. How few people (ideally, none) are likely to know or be able to guess any given user's answer. The more secret the answer, the higher a point-value that can be assigned to the question if answered correctly in the Reset Quiz.

- **How personal the answer is**. How much a wrong answer ensures that the person taking the Reset Quiz is not the authorized user; for example, "Are you left-handed, right-handed, or ambidextrous?" Questions that call for personal answers can serve as "eliminators" in the Reset Quiz: few or zero points are awarded for a correct response, and more points deducted for an incorrect response.

- **How memorable and static the answer is**. This ensures that the user will recall the exact answer that he or she provided at enrollment. Questions that involve preferences (such as "what is your favorite ice cream") should have lower point-values for both correct and incorrect answers and are better suited as Optional questions. By comparison, questions that are based on unchanging and easily-recalled facts ("What is the name of the last high school you attended?") can have higher point-values for correct or incorrect responses; they are better candidates for Required questions.

- **The minimum number of questions** that must be answered in order to pass (or explicitly fail) the Reset Quiz. This is derived from the Success/Failure score thresholds and the point values you assign to each question for correct and incorrect responses.

See Question Examples for more information.

4.2.5 Editing System Questions

After creating system questions, you can edit them and adjust their configurations in the **Edit Question** tab. Access this tab by clicking the **Edit** button on the **System Questions** tab.

Using this tab, you can:

- Create new questions (in multiple languages, if desired)

- Assign point values

- Set Required/Optional status

- Specify answer sources

- Perform validity checks on the end user's answers

- Select Users and Groups to allow or deny access to any question

- Disable system questions; that is, remove them from the Enrollment Interview.

  Questions that you disable from the Enrollment Interview will still appear in the Reset Quiz to end users who have already provided answers to the disabled question, but they will no longer be presented to users who subsequently enroll or re-enroll.

See Setting Up the Enrollment Interview for more information. For suggested text and settings, also see Question Examples.

The following table provides information about Question Text settings.

Question Text	Description
Question text	The text of the question, in the default language, as it is displayed to the end user.
	If you specify case-sensitivity, the answer given in the Reset Quiz must have exactly the same spelling, punctuation, capital-letter use, and white space, as the answer in the Enrollment Interview. Therefore, it is advisable to include formatting instructions or examples.
	For instance, if asking for a telephone number, provide an example, such as "(333) 555-1234" to insure consistency between the Enrollment Interview and the Reset Quiz. If the question is "What is your Social Security number?" note whether or not the response should include dashes between number segments.
<Language> text	If you are using Password Reset in more than one language, enter the translated question text in this field.

The following table provides information about Question Properties settings.

Question Properties	
Correct response weight	Specify the number of points to add to the end user's score if the question is answered correctly. If modifying this field, see Changing Question Weights.
Wrong response weight	Specify a negative number to indicate the number of points to deduct from the end user's score if the question is answered incorrectly. If modifying this field, see Changing Question Weights.
Enabled	**If checked**: This question is used in the Enrollment Interview and in the Reset Quiz.
	If unchecked: This question is not used in the Enrollment Interview. It is used in a Reset Quiz only if: 1) it has previously been enabled and 2) if the end user has answered the question in an Enrollment Interview.
Required	**If checked**: This is a Required question. The end user must provide an answer to the question in order to complete enrollment. A Required question is always used in the Reset Quiz.
	If unchecked: This is an Optional question. The end user can skip this question in the Enrollment Interview, in which case the question will not be used in this end user's Reset Quiz.
	If the end user supplies an answer to an Optional question, the question is used in the Reset Quiz only after all Required questions have been asked.

The following table provides information about Answer Constraints settings.

Answer Constraints	
Answer source	Specify the source from which the answer to this question should come. Select the default, **User supplied**, if the user will supply the correct answer during the Enrollment Interview.
	If the source is not supplied by the user, select the external validator location from the drop-down list. See Working with External Validators for more information.
Minimum answer length	Specify the minimum number of characters the end user must enter for a valid answer.
Answer format	Specify the format and punctuation for the answer using a regular expression. For example, you can specify the date format "12/1/1983" with the expression
	`\d*\d/*\d\d/\d{4}`
	(allowing the entry of single or double-digit month and day and requiring a four-digit year). If you want to require the end user to type a Social Security number with dashes, use the expression
	`\d{3}-\d{2}-\d{4}`
	This setting is optional.
	Note: For more information about regular expressions, refer to http://msdn.microsoft.com/
Case sensitive	**If checked.** The end user's answer is checked for consistent use of upper- and lower-case characters.
	If unchecked. The end user's answer is not checked for consistent use of upper- and lower-case characters.

The following table provides information about Access Control settings.

Access Control	
Allow	Click the **Add** button to launch a window from which to select users and groups that will receive this question. See Selecting Users and Groups for Question Assignment.
Deny	Click the **Add** button to launch a window from which to select users and groups that will not receive this question.
	Note: By default, if any user or group is denied access, all users and groups are denied access except those specified in the Allow list.

4.2.5.1 Selecting Users and Groups for Question Assignment

Clicking the **Add** button in the **Access Control** settings displays the **Edit Users and Groups** dialog.
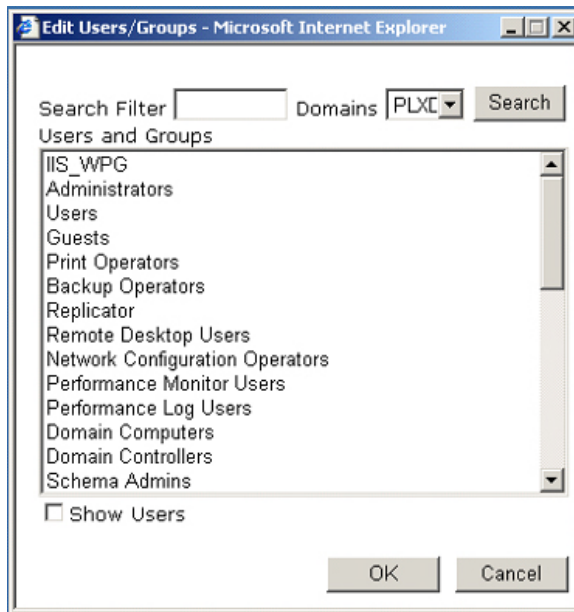
To use this dialog:

- Enter a search filter, if desired, and select a domain from the drop-down list.

- Check the **Show Users** box at the bottom of the screen if you want the list to include individual users as well as groups (this could create a very long list). You can check this box before or after performing the search.

- Click the **Search** button.

- Scroll through the **Users and Groups** list on the left to locate the groups (and users if you checked the box below) to specify who receives the question you are configuring.

- Do one of the following:

  - Double-click an item in one list to move it to the other list.

  - Click the right-facing double arrows (**>>)** to move a user or group to the Selected list on the right. Remove an entry by clicking the left-facing double arrows (**<<**).

- Click **OK** to save your selections and return to the **Edit Question** dialog.

For more information about how system questions are assigned to users and groups, see Role/Group Support.

4.2.5.2 Modifying or Disabling a System Question

You can change the text or point value of a question, assign or unassign it to users and groups, or remove it from the enrollment interview entirely. To perform any of these tasks:

1. In the **Questions** tab, select the Language in which to modify the question.

2. Do one of the following:

   - Double-click a question.

   - Select a question and click **Edit**.

3. In the **Edit Question** dialog, do any or all of the following:

- Edit the text and then click **OK**.

- Edit the weights and then click **OK**.

> **Note:** If you change the values in the **Correct Response Weight** or **Wrong Response Weight** fields, a **Response Weights Changed** dialog appears. See Changing Question Weights.

- Clear **Enabled** to remove the question from the Enrollment Interview.

> **Note:** After you create a question, you cannot change whether to require it or the answer constraints settings.

- Select or deselect the **Users and Groups** that you want to assign this question to.

> **Note:** You cannot assign questions to users or groups when using a database (such as Microsoft SQL Server or Oracle Database) for your repository. The settings are available for editing, but the assignments will not be written to the database.

4. Click **OK** to save your changes, or click **Cancel** to abandon your changes, and return to the **System Questions** tab.

4.2.5.3 Changing Question Weights

The weight of a question may be modified if it is determined to be more or less effective in the reset test. A possible ramification of modifying a correct response weight after a question has been created is that enrolled users might not be able to pass the reset test due to an insufficient score, even if they answer all the questions correctly. To avoid such an occurrence, if a correct response weight is changed, a dialog appears, presenting the option to:

- **Modify this question**: When this option is selected, the change will be made to this question. Note that users who answered this question during enrollment may not be able to reset their password if the correct response weight is set too low.

  or

- **Disable this question and create a new question**: Disables this question and creates a new question with the changes. The benefit is that currently enrolled users will not be affected by the changes. Note that disabled questions are shown as "disabled" (dimmed) in the **System Questions** list.

4.2.6 Question Examples

The following tables provide some examples of system questions, recommended as Required, Eliminator, or Optional, with suggested point values based on the default score thresholds of -100 to 100 points.

4.2.6.1 Required Questions

These questions are good prospects for Required questions. Note that all of these questions have answers that are facts on record. Oracle strongly recommends that

your selection of Required questions have answers that come from as many *different sources* as possible. For example, in some states, a driver's license may display the Social Security number and date of birth.

Question	Required?	Points if Correct	Points if Incorrect
What is your Social Security number (numbers only, no spaces)?	Y	10	-75
What is your date of birth (mmddyy)?	Y	25	-50
In which city were you born?	Y	25	-50
What is your mother's maiden name?	Y	25	-75
What was the name of the first school you attended? (or "...that you remember attending)?"	Y	25	-25
What is the name of the last high school that you attended?	Y	25	-25

4.2.6.2 Eliminators

These questions are Eliminators because the authorized end user is very unlikely to answer them incorrectly. The answers are personal, and therefore have low or no point-value for correct answers and high negative point-value if answered incorrectly.

Question	Required?	Points if Correct	Points if Incorrect
What is your eye color?	Y	0	-75
Are you left/right handed, or ambidextrous (l, r, or a)	Y	5	-75
What is your gender (male or female)?	Y	0	-75

4.2.6.3 Optional Questions

These questions are acceptable as Optional questions only, because they may not apply to all enrollees.

Question	Required?	Points if Correct	Points if Incorrect
What was the name of your first or favorite pet?	N	25	-25
What color was your first car?	N	25	-25
What is your wife's maiden name?	N	25	-25
How many siblings do you have?	N	25	-25
What is your spouse's date of birth? (mmddyy)	N	25	-25

4.2.7 Excluding Users from Forced Enrollment

> **Note:** The use of the Windows Integrated authentication method in this procedure requires that the Password Reset server URL be added to the Internet Explorer Local Intranet zone for all end users. In the absence of this URL, pass-through authentication will fail and the user will not be prompted for forced enrollment, despite having permissions to the `checkenrollment.aspx` page.

To exclude users from forced enrollment, do the following:

1. Open the **Internet Information Services (IIS) Manager** tool.

2. Locate the `vGOSelfServiceReset` virtual Web directory, and expand it.

3. Locate the `CheckEnrollment.aspx` file beneath the `vGOSelfServiceResetReset Client` virtual directory.

4. Right-click **CheckEnrollment.aspx**, and select **Properties**.
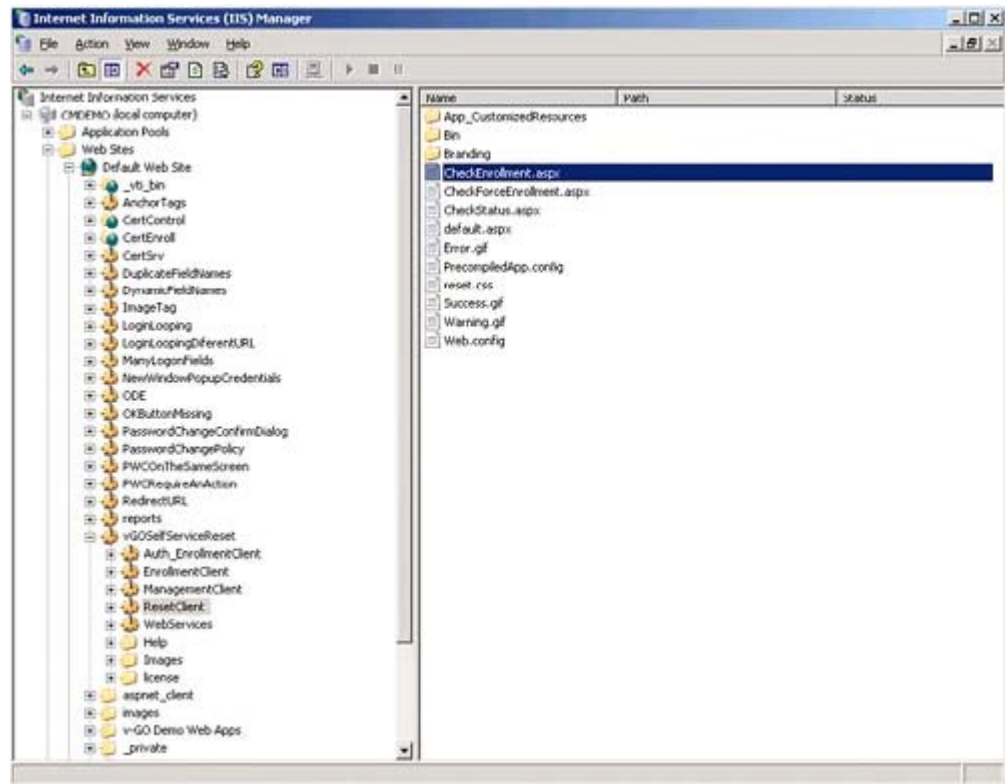
5. In the properties of **CheckEnrollmentStatus.aspx**, click the **File Security** tab, then click **Edit** in the **Authentication and access control** section.
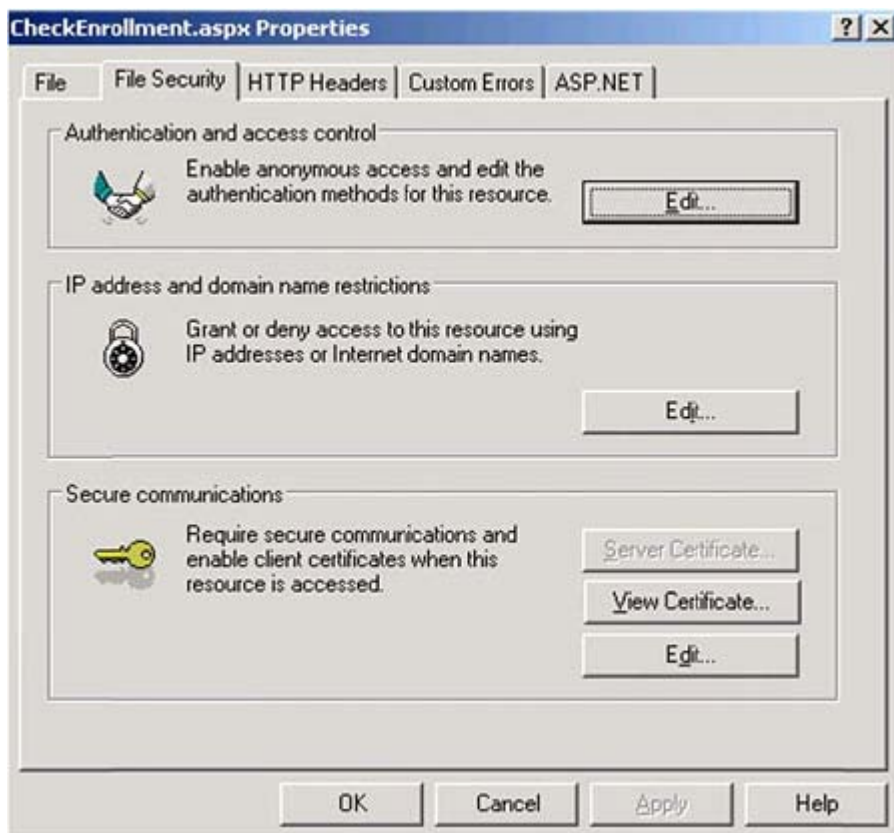
6. In the **Authentication Methods** dialog, uncheck **Anonymous Access** so that only **Integrated Authentication** is selected.
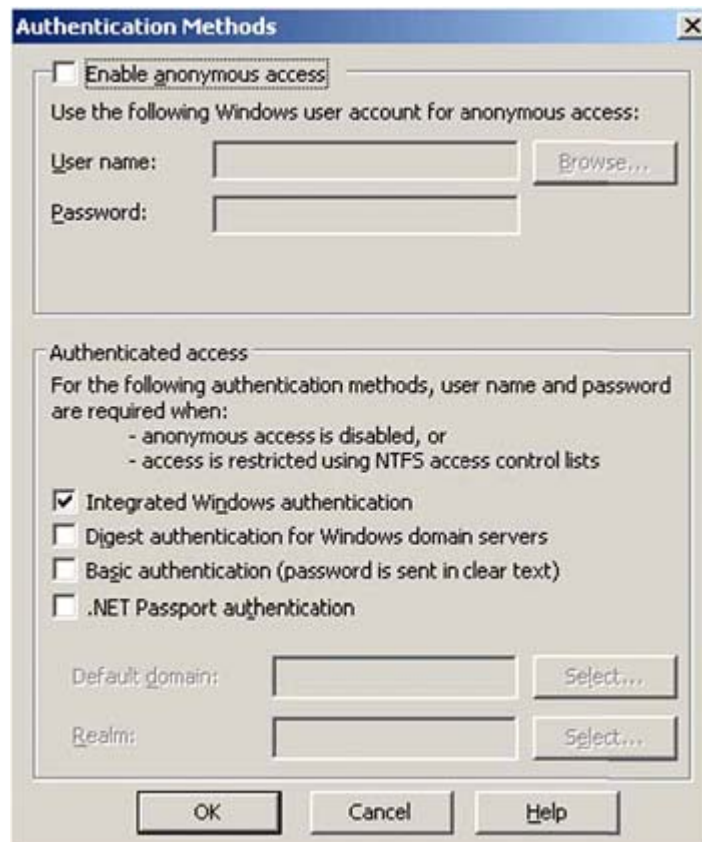
7. Navigate to `C:\Program Files\Passlogix\v-GO SSPR\ResetClient`, and set permissions on the `CheckEnrollment.aspx` file. Add the Exclusion Group(s) with **Deny** permissions checked. In the example below, the Exclusion Group is `Universal_Group_SSPR`.
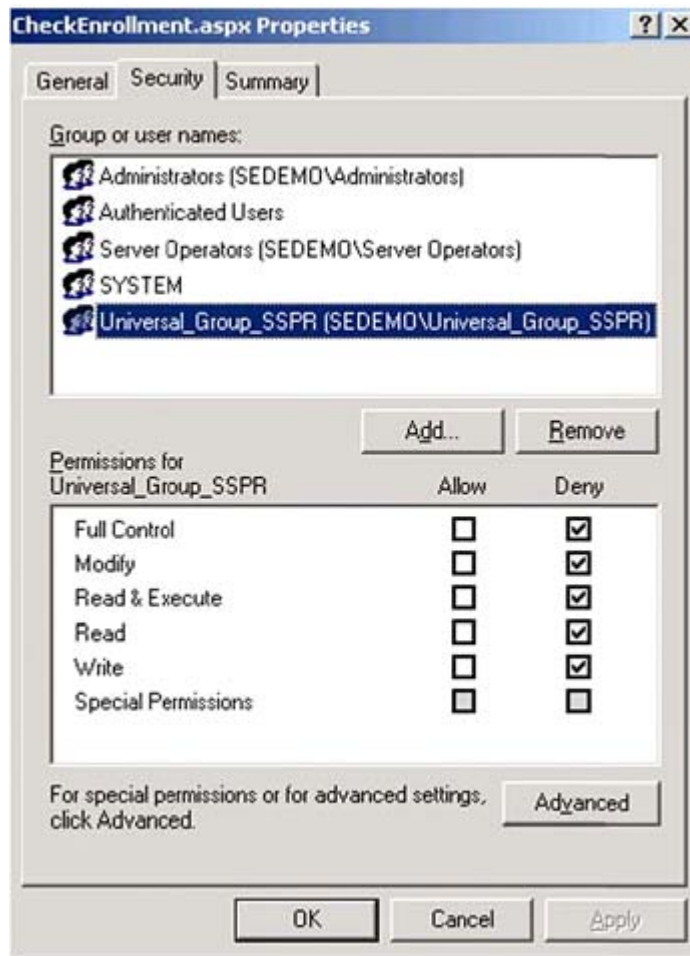
4.3 Configuring Reset Authentication

When an end user requests a password reset, Password Reset displays the Reset Quiz.

The Reset Quiz is a series of questions drawn from the system questions that the end user answered in the Enrollment Interview. The Reset Quiz presents all of the required questions one at a time, in random order, for the end user to enter a response. If there are no required questions set up, the Reset Quiz presents the optional questions only. With each response, the preset point-value for correct answers is added to the total score, or the point-value for incorrect answers is deducted.

After all of the required questions have been presented, the Reset Quiz continues until either:

■ All Optional questions have been presented.

■ The end user answers a sufficient number of questions to meet either of two score thresholds.

   – If the end user's score equals or exceeds a preset Success score threshold, the **New Password** dialog appears. The end user then enters and confirms a new password, and returns to the initial logon dialog.

   – If the end user's score equals or falls below a preset Failure score threshold, the Reset Quiz ends with no password reset, and the end user returns to the initial

logon dialog. Password Reset records the quiz session as an explicit failure, indicating that the end-user failed the quiz by incorrectly answering questions.

–   If the end user answers all of the questions without achieving either score threshold, the Reset Quiz ends with no password reset, and the end user returns to the initial logon dialog. Password Reset records the quiz session as an implicit failure indicating that the end-user failed the quiz with an insufficient score to pass or explicitly fail.

The Success and Failure score thresholds are set by the administrator in the **Settings** page of the Password Reset node of the Administrative Console. The text and point-values for individual system questions are set in the **System Questions** page.

Also see Reset Service Settings for more information.

4.3.1 Score Thresholds

The score thresholds are the point-values that determine whether the end user passes or fails the Reset Quiz.

■   The Success value determines the score (the point-value total achieved for the quiz) that end users must achieve in order to reset their passwords.

■   The Failure value determines the minimum (that is, a negative) score that end users can accrue by answering Reset Quiz questions incorrectly. If the end user's score falls below this setting, the Reset Quiz ends without a password reset.

See Enrollment Level Settings for more information.

4.3.2 Editing Reset Service Settings

Use the **Settings** tab (under the Settings node) to modify general settings for the Reset Quiz. When you have completed your changes, click **Submit** to apply your new settings to Password Reset.

The following table provides information about Authentication Threshold settings (shown below).

Authentication Thresholds	
Authentication success level	The score (the point-value total achieved for the quiz) that end users must achieve in order to reset their passwords. The default value is 100.
Authentication failure level	The minimum (negative) score that end users can accrue. If the end user's score falls below this setting, the Reset Quiz ends without a password reset. The default value is -100.
Enrollment level	The score (the point-value total achieved for the enrollment interview) that end users must achieve in order to complete the enrollment interview. The default value is 100. The **Enrollment Level** must be at least equal to or greater than the **Authentication Success Level**.

The following table provides information about Reset Lockout settings (shown below).

Reset Lockout

Lockout threshold (attempts)	The number of consecutive unsuccessful reset attempts permitted. If an end user fails the Reset Quiz this number of times in a row, no further Reset Quiz attempts are permitted for the Lockout Duration interval.
Lockout duration (hours)	The time period, in hours, that an end user is not permitted to take the Reset Quiz. The Lockout Duration begins when the end user consecutively fails the Reset Quiz the number of times given for Lockout Thresholds. **Note:** To override lockout for individual end users, click the **Users** tab, select the end user from the list, then click **Unlock**.

The following table provides information about Forced Enrollment settings (shown below).

Forced Enrollment

Deferrals allowed	The maximum number of times a user can defer Password Reset enrollment. When the user exceeds the maximum number of deferrals, he must complete the enrollment process in order to be allowed to log on. **Note:** If you wish, you can exclude certain users from forced enrollment. See Excluding Users from Forced Enrollment for detailed instructions.

The following table provides information about User E-mails settings (shown below).

User E-mails	Function
Required during enrollment	Controls whether or not users are required to enter an e-mail address during the enrollment process.
E-mail format (regular expression)	Controls the valid format of the user e-mail address. The default setting allows for most acceptable e-mail formats.

The following table provides information about Reset Experience settings (shown below).

Reset Experience	Function
Show "Unlock account only" option	Controls whether or not a user is given the option to unlock his or her account rather than reset the password. This option is presented after a user passes the Reset Quiz.
Enable "Display temporary password" mode	Controls whether or not Password Reset should allow the end user to reset the password regardless of the Active Directory password policy. With this checkbox enabled, Password Reset overrides any Active Directory restrictions that are in place and provides the user with a temporary password. The user can then log on with that temporary password and change it through Windows.

Also see Configuring Reset Authentication for more information.

4.3.3 Multi-Domain Support

You can configure Password Reset to reset Windows passwords and unlock Windows accounts in its own domain or any domain you designate as trusted.

Multi-domain support requires the following conditions:

- There must be valid two-way trusts between the Password Reset domain and other domains.

- The Password Reset reset service user account must be a member of the local administrators group of the trusted domain.

- All the domains must share the same settings as the Password Reset server, such as password complexity, alerts, questions, and so forth.

To set up multi-domain support, in the Administrative Console, select the domain you want to designate as trusted from any of the following screens:

- The drop-down menu in the **Edit Users/Groups** dialog.

- The **Questions** tab, when you edit existing questions or create a new one.

- The **Users** tab.

When you make a domain selection on any one of these screens, that change is reflected in all the other screens. The domain that you select is saved in the registry value, HKLM\SOFTWARE\Passlogix\SSPR\SSPRService\DisplayDomain.

> **Note:** When performing queries against a trusted domain, you may receive the error message: "The server is not operational." This can occur if the guest account on the trusted domain is turned on, because that account does not have the rights to enumerate users
>
> To eliminate this error, do one of the following:
>
> - Turn off the guest account in the trusted domain.
>
> - Create the same trusted domain user account in the trusted domain.

4.4 Password Complexity

Use the **Password Complexity** tab (under the **Settings** node) only to adjust the password constraints to make certain that they match or are within the constraints of the Group Policy of the Windows domain. This setting does not apply to end-user passwords (see note, below). In typical usage (that is for typical group policies), these settings need not be changed.
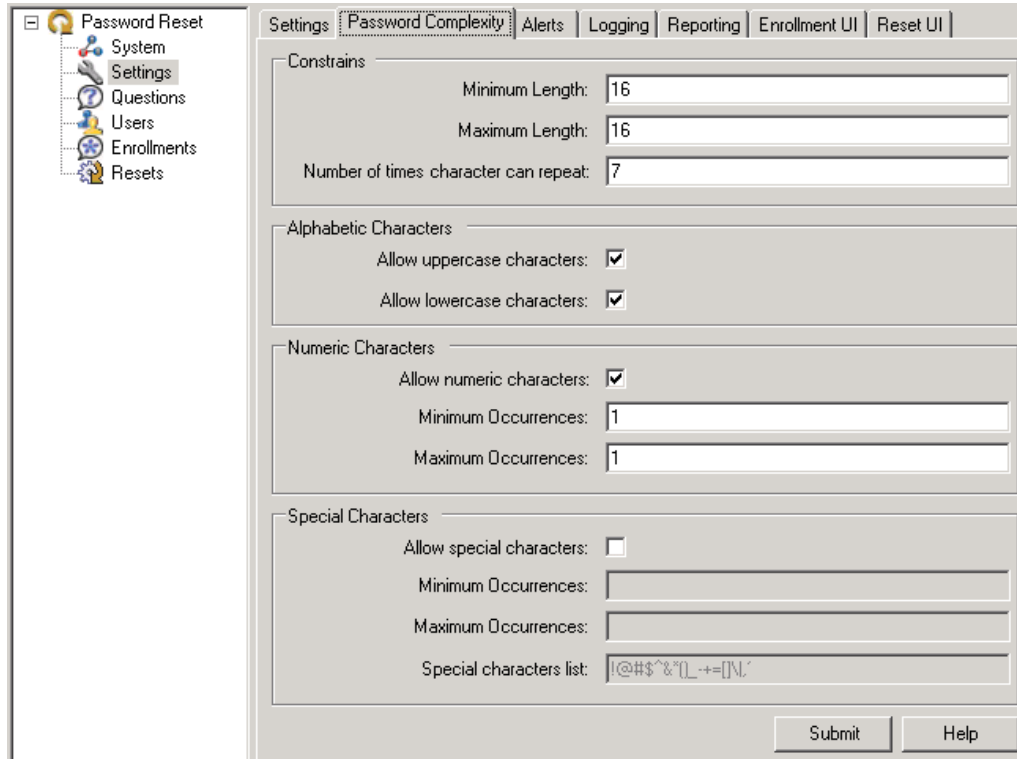
The following tables explain the options for the **Password Complexity** settings. When you have completed your changes, click **Submit** to apply your new settings to Password Reset.

> **Note:** In order for Password Reset to reset end-user passwords, the Reset Service account performs an intermediate password reset as a proxy for the user. The Reset Service account generates a password internally that must conform to the domain's group policy, but is not subject to the domain's minimum password age policy. The password complexity settings in this dialog apply only to that intermediate password, not to end-user passwords.
>
> Resetting a password adds two entries to the user's password history in Active Directory.

Constraints	
Minimum length	Minimum internal password length: 1-63 (default: 16)
Maximum length	Maximum internal password length: 1-63 (default: 16)
Number of times characters can repeat	0-62, default: 7

Alphabetic Characters

Allow uppercase characters	Select to allow uppercase characters (default: allowed)
Allow lowercase characters	Select to allow lowercase characters (default: allowed)

Numeric Characters

Allow numeric characters	Select to allow numeric characters (0-9), (default: allowed)
Minimum occurrences	1-63, default: 1
Maximum occurrences	1-63, default: 1

Special Characters

Allow special characters	Select to allow special characters (non-alphabetical, non-numeric) (default: not allowed)
Minimum occurrences	1-63, default: 1
Maximum occurrences	1-63, default: 1
Special characters list	Characters that may be used (default: !@#$%^&*()_-=+[]|.?)

4.5 Alerts

Use the **Alerts** tab (under the **Settings** node) to configure Password Reset to email administrators and/or users with notification of significant user-generated events. You configure this alert with the `UserText.xml` template included with the product in the directory: `C:\program files\Passlogix\v-GO SSPR\WebServices`.

The following table lists the variables in the `UserText.xml` file.

E-Mail Template Variable	Description
$USER	The user's "display name" (full name) as defined in Active Directory
$ACCOUNT	The user's username in the format: `domain\username`.

E-Mail Template Variable	Description
$ADMIN	The administrator's name (as entered in the **Alerts** tab of the Administrative Console)
$DATETIME	The date and time when the event occurred; for example: `7/23/2012 3:24 PM`
$ATTEMPTS	The number of times the user has failed the reset quiz
$PRODUCT	ESSO-PR
$FULLPRODUCT	Oracle Enterprise Single Sign-On Password Reset

You can see a sample alert by clicking **Send Test E-mail to Admin**. When you are satisfied with the results, click **Submit** to apply your new settings to Password Reset.

The following table provides information on E-mail Template variables.

E-Mail Settings	Description
Enable e-mail alerts	Select to activate e-mail alerts
"From" e-mail address	The e-mail address that originates the alert. This can be any valid email address for the SMTP mail server specified below.
Admin e-mail address	The e-mail address of the administrator to whom the alerts will be sent.
Admin name (displayed in e-mails)	The name of the administrator to whom alerts will be sent. This name will be displayed in the e-mails.
SMTP mail server	The name of the outbound mail server.

The following table provides information on Alert Conditions.

Alert Conditions	Description
User fails a reset attempt	Select who should receive e-mail alerts if a user fails a reset attempt: the Admin, the User, or both. This field is only active if **Enable e-mail alerts** is selected. Also see Reset Service Settings for the lockout controls.
User successfully resets password	Select who should receive e-mail alerts if a user successfully resets his password: the Admin, the User, or both. This field is only active if **Enable e-mail alerts** is selected.
User is locked out of Reset Quiz	Select who should receive e-mail alerts if a user fails the Reset Quiz more times than the threshold permits: the Admin, the User, or both. This field is only active if **Enable e-mail alerts** is selected.

4.6 Logging

Use the **Logging** tab (under the **Settings** node) to enable logging, specify the syslog server and port, and select the types of events that should generate syslog messages. Password Reset sends these messages to a syslog listener, which in turn generates notifications to apprise the administrator of user enrollment and reset events.

Enter the following information and click **Submit** to apply your new settings to Password Reset.

SysLog Setting	Function
Enable	If checked, syslog logging will be enabled.
Server name/IP address	The name or IP address of the syslog server.
Server port	The port where the syslog server is listening for Syslog messages (default port is 514).

Event Filters	Function
Start	Check to have Password Reset send a message when the user begins an enrollment or reset session.
Cancel	Check to have Password Reset send a message when the user cancels an enrollment or reset session.
Success	Check to have Password Reset send a message when the user successfully completes an enrollment or reset session.
Fail	Check to have Password Reset send a message when the user fails the reset session.
Locked out	Check to have Password Reset send a message when the user gets locked out of the Password Reset system (by failing too many reset quizzes).

4.7 Reporting

Use the **Reporting** tab (under the **Settings** node) to configure generation of reports on user activities. Refer to the Reporting section of this guide for more information on using this tool.
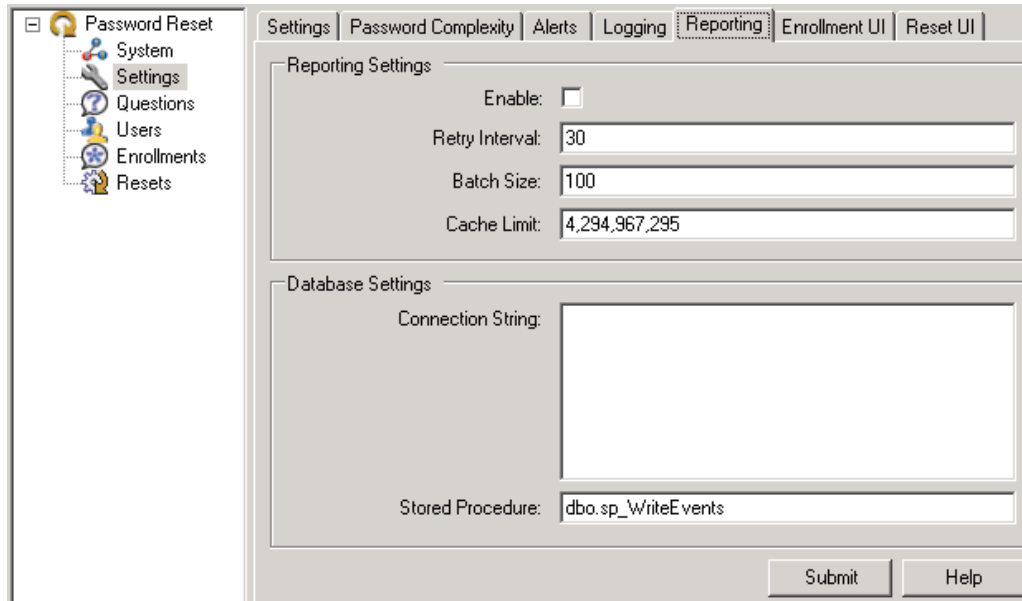
The settings on this tab configure the Reporting tool and database. Click **Submit** to apply your new settings.

The following table provides information on Reporting settings.

Reporting Setting	Function
Enable	Check this box to enable Reporting.
Retry interval	Defines timeout in minutes between sequential operations of the Reporting Service Cache offloading events to the database. Default is 30. An interval is necessary to reduce database connection load.
Batch size	Defines the group size of events to be sent to the database Stored Procedure at one time. Default is 100. For example, if you have 1000 events in the Reporting Service cache and the Batch Size = 100, you will have 10 database Stored Procedure calls.
Cache limit	Number of reporting events to be cached. Once this number is reached, the oldest events are discarded. Default is 4,294,967,295. For example, if the batch size is 100, and an end users system cannot connect to the reporting service, it will keep logging events. Once it gets to 4,294,967,295, the oldest events will be discarded.

The following table provides information on database settings.

Database Setting	Function

Connection string	Database connection string in the OLE DB format:
	
	`"Provider=sqloledb; Data Source=myServerName; Initial Catalog=myDatabaseName; User Id=myUsername; Password=myPassword"`
	
	or
	
	`Provider=SQLOLEDB.1;Integrated Security=SSPI;Persist Security Info=False;Initial Catalog=<Database>;Data Source=<DBServer>`

Database Setting	Function
Stored procedure	The name of the stored procedure in the database. When encoded events are sent to the database, the stored procedure is called to decode the XML file and store the events in the database.

4.8 Configuring the Enrollment User Interface

Use the **Enrollment UI** tab (under the **Settings** node) to customize the Enrollment Interview User Interface.

You can edit the look and feel of all Password Reset Client pages (the Enrollment and Reset interviews, not the Administrative Console). This page allows you to adjust colors, fonts, and logos on the Enrollment user interface.

The choices you make on this tab become the Default style settings. You can create additional styles by performing the following steps:

1. Shut down the Administrative Console.

2. In `C:\Program Files\Passlogix\v-GO SSPR\WebServices\Templates`, select the `default.xml` and copy it.

3. Paste the copy into the same directory.

4. Select the copied file and rename it. The new style will be available in the drop-down when you relaunch the Administrative Console. You can select it to create and save an entirely different look and feel while still retaining the Default style.

Enter the following information and click **Submit** to apply your new settings to Password Reset.

Status Panel	Function
Text color	Select the color for the text in the status panel.
	1. Click the ellipsis ("**…**") button to launch the color picker, and select a standard color swatch.
	or
	1. Click the ellipsis ("**…**") button to launch the color picker, then click **Define Custom Colors>>** to mix a color of your choosing.
	2. Use the slider or enter a color's HSL or RGB values, and click **Add to Custom Colors**.
	3. Select the new color in the custom color swatches and click **OK**.
Background	From the drop-down list, select to use either a solid color or background image.
	▪ Choosing **Select solid color…** launches the color picker. Follow the same procedure as above to choose a color.
	▪ Choosing **Select image…** launches a dialog that lets you choose from all images in the `%SSPR%\Images` folder on the server.
	Note: There is no size requirement for this image. For reference, the Oracle status panel background image is 408x28.

Side Panel	Function
Normal text color	Select the text color for the unhighlighted category text in the side panel. Follow the same procedure as above to choose a color.
Current step text color	Select the text color for the current step text in the side panel. Follow the same procedure as above to choose a color.
Background	From the drop-down list, select to use either a solid color or background image. Follow the same procedure as above. **Note:** There is no size requirement for this image.

Page	Function
Background	From the drop-down list, select to use either a solid color or background image. Follow the same procedure as above. **Note:** There is no size requirement for this image.
Border color	Select the border color for the page. Follow the same procedure as above to choose a color.
Text font	Select the font to be used for the Enrollment UI. Click the ellipsis ("**…**") button to launch the **Font** window. Highlight the desired font and click **OK**. **Note:** The font list is generated from fonts installed on the server. To add a font to the list, install it on the server.

Buttons	Function
Enable style	Check this box to activate the button style you create in this section.
Normal color	Select the normal color for buttons in the Enrollment UI. Follow the same procedure as above to choose a color.
Hover color	Select the hover color for buttons in the Enrollment UI. Follow the same procedure as above to choose a color.
Text color	Select the text color for buttons in the Enrolment UI. Follow the same procedure as above to choose a color.

Top Panel	Function
Text Color	Select the text color to be displayed for the text in the top panel of the Enrollment UI. Follow the same procedure as above to choose a color.
Background	From the drop-down list, select to use either a solid color or background image. Follow the same procedure as above. **Note:** There is no size requirement for this image. For reference, the Oracle status panel background image is 408x47.

Logo	Function
Image	Select the logo image to appear in the top left area of the Enrollment UI. Follow the same procedure for selecting a background image above. For images to appear in this list, they must exist in the `%SSPR%\Images` folder. **Note:** There is no size requirement for this image. For reference, the Oracle enrollment logo is 146x47.

Main Panel	Function
Text Color	Select the color for the text in the main panel. Follow the same procedure as above to choose a color.
Background	From the drop-down list, select to use either a solid color or background image. Follow the same procedure as above. **Note:** There is no size requirement for this image. For reference, the Oracle main panel background image is 408x273.

4.9 Configuring the Reset User Interface

Use the **Reset UI** dialog (under the **Settings** tab) to customize the Reset User Interface.

You can edit the look and feel of all Password Reset Client pages (the Enrollment and Reset interviews, not the Administrative Console). This page allows you to adjust colors, fonts, and logos on the Reset User Interface.
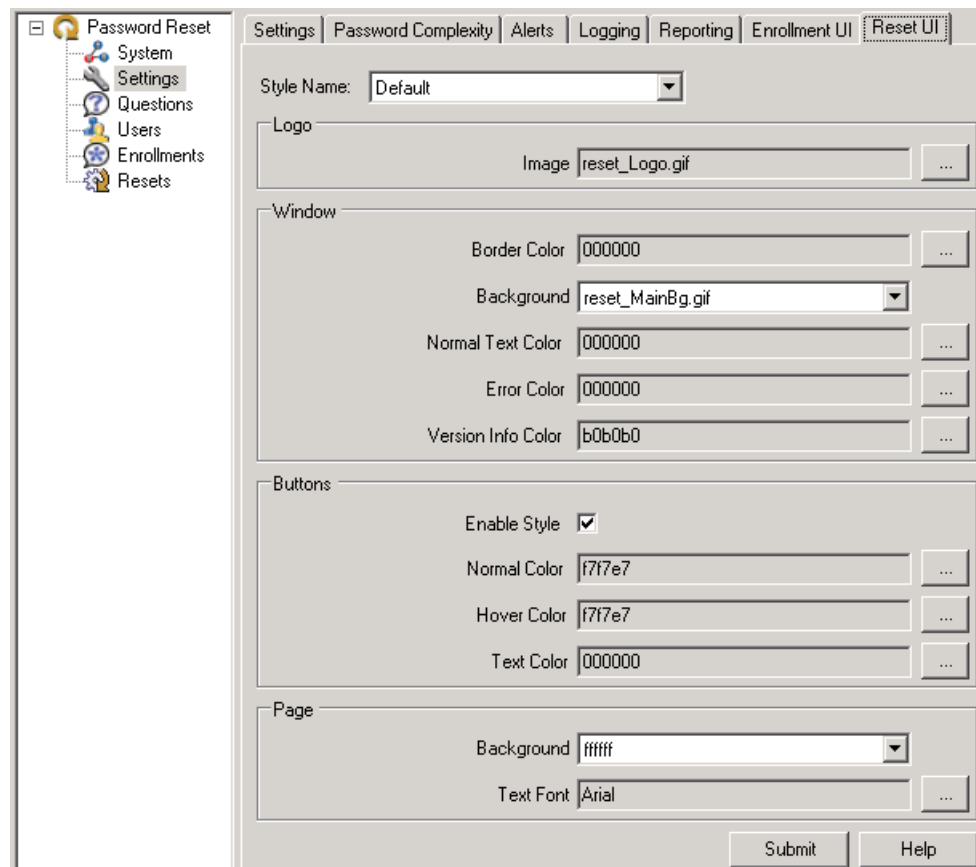
Configure the following settings as you want them and click **Submit** to apply your changes to Password Reset.

Logo	Function
Image	Select the logo image to appear in the reset window. Click the ellipsis ("**…**") button to launch a window that lets you choose from all images in the `%SSPR%\Images` folder on the server. **Note:** The maximum size for this image is 448x45. For reference, the Oracle reset logo is 342x24.

Window	Function
Border Color	Select the border color for the reset box: 1. Click the ellipsis "**…**" button to launch the color picker and select a standard color swatch. Then either: or 1. Click the ellipsis "**…**" button, then click **Define Custom Colors>>** to mix a color of your choosing. 2. Use the slider or enter a color's HSL or RGB values, and click **Add to Custom Colors**. 3. Select the new color in the custom color swatches and click **OK**.
Background	From the drop-down list, select to use either a solid color or background image. ■ Choosing **Select solid color…** launches the color picker. Follow the same procedure as above to choose a color. ■ Choosing **Select image…** launches a dialog that lets you choose from all images in the `%SSPR%\Images` folder on the server. **Note:** There is no size requirement for this image. For reference, the Oracle reset window background image is 450x350.
Normal text color	Select the text color for error messages that appear during the reset process. Follow the same procedure as above to choose a color.
Error color	Select the text color for the unhighlighted category text in the side panel. Follow the same procedure as above to choose a color.
Version info color	Select the text color for version information shown on the reset window. Follow the same procedure as above to choose a color.

Buttons	Function
Enable style	Check this box to activate the button style you create in this section.
Normal color	Select the normal color for buttons in the Enrollment UI. Follow the same procedure as above to choose a color.
Hover color	Select the hover color for buttons in the Enrollment UI. Follow the same procedure as above to choose a color.
Text color	Select the text color for buttons in the Enrolment UI. Follow the same procedure as above to choose a color.

Page	Function
Background	From the drop-down list, select to use either a solid color or background image. Follow the same procedure as above. **Note:** There is no size requirement for this image.
Text font	Select the font to be used for the Reset UI. Click the ellipsis ("**...**") button to launch the **Font** window. Highlight the desired font and click **OK**. **Note:** The font list is generated from fonts installed on the server. To add a font to the list, install it on the server.

4.9.1 Changing the Reset User Interface Through the Registry

Some user interface settings are configurable through registry settings only. For instance:

- The Reset User Interface, by default, has fields pre-populated with the username and domain of the last Windows account to log on to the workstation. You can set the message above these fields to display a prompt that reads, "To reset your network password, please type in your user name, choose the domain, and click **OK** to continue."

- The title bar for the enrollment and reset windows, by default, reads, "Oracle ESSO-PR." You can change this window title to suit your company's needs.

- The password reset link message, by default, reads, "Forgot your password? Click here to reset it." You can change the message in this link (registry settings for this configuration apply only to Windows 7).

   > **Note:** To learn more about customizing error messages, continue to Customizing Reset Messages.

- You can eliminate the "Forgot your password?" link under the user's default Windows 7 logon tile, and create a separate password reset tile and text, on the logon screen. This setting is useful in some Windows 7 environments where attaching the reset user interface to the Microsoft password credential provider causes the appearance of duplicate tiles.

   See Section 7.3.4, "Password Reset Client-Side Registry Settings" for the specific registry settings to configure the above options.

4.9.2 Customizing Reset Messages

When the user attempts to change a password and cannot, due to either an account or password policy restriction that you have set, the user receives an error message explaining why the attempt was unsuccessful. The Administrator has the ability to customize the most common of these error messages through the Administrative Console to help the user to correct the error.

Following are the customizable error messages and the instances that would prompt their display:

Message	Message Code	Description
Password has been successfully reset.	Text_ResetSuccess	The password reset attempt was successful.

Message	Message Code	Description
Your account has been successfully unlocked.	Text_UnlockSuccess	The attempt to unlock the account was successful.
Your temporary password is "{0}".	Text_TempPassword	Provides the user with a temporary password after completion of the reset quiz. **Note:** Be certain to include the {0} syntax in this message. Password Reset replaces this string with the temporary password.
Thank you for using $PRODUCT. You may not be able to log on immediately because it takes time for account updates to propagate throughout the network.	Text_Success	Informational message that follows each of the success messages above. **Note:** Password Reset replaces the $PRODUCT string with the product name.
Access Denied	Error_AccessDenied	There is a configuration error that the Administrator needs to rectify in order for the user to continue.
Bad Password	Error_BadPassword	The user entered a password that does not fulfill the password policy requirements.
Click here to reset the enrollment session.	Text_ResetSession	This text instructs the user to click to be directed to a URL that links to the reset session.
Session is invalid.	Error_SessionInvalid	The user has exceeded the permissible interval of inactivity while taking the reset quiz.
The answers provided failed to satisfy the requirements necessary to continue with the reset.	Error_FailQuiz	The user provided enough incorrect answers to reach the failure threshold.
The reset service is currently not available. Please contact your administrator for more information.	Error_ServiceNotRunning	The SSPRChangePasswordSvc service is not running on the Password Reset server.
Error retrieving user data. Please make sure the specified user is enrolled.	Error_UnknownUser	The user who is attempting to log on has not enrolled in Password Reset.
User Cannot Change	Error_UserCannotChange	The user is attempting to change a password in a time frame or manner contrary to the policy that the Administrator has defined.
User Not Found	Error_UserNotFound	The user's account has been deleted from Active Directory between the time of enrollment and the current attempt to access the account.
Your account has been locked out.	Error_LockedOut	The user has exceeded the permissible number of failures taking the reset quiz and has been locked out of Password Reset. The user must wait until the Administrator unlocks the account or the lockout interval elapses.

> **Note:** To use these settings, add them to the Server registry. See
> Section 7.3.5, "Password Reset Server-Side Registry Settings" for more
> information.

Example

In the following example, you will change the "Bad Password" error message. If the
user enters a password that does not comply with the password policy, the user
receives the standard error message, "The password did not meet password policy
requirements."

Perhaps you want to inform the user how to select a policy-compliant password, and
so you want to add more information to this message. To change this message:

1. From the **Start** menu, select **Run…**

2. Open the registry by entering `regedit`.

3. Select the registry key: `HKLM > SOFTWARE > Passlogix > SSPR > SSPRService`.

4. Create a new `DWORD` value by right-clicking the **SSPRService** folder and clicking
   New > DWORD value.

5. Name the registry setting `Reset_CustomizedErrorMsg` and assign a value of `1` to
   activate it. This setting specifies the directory from which the Server retrieves the
   error message: `C:\Program Files|Passlogix\v-GO SSPR\ResetClient\App_
   CustomizedResources`.

6. Select the `.ini` file that you want to edit and open it in a text editor.

> **Note:** The Server retrieves the error message in the language that the
> user selected during enrollment. If the user selected English, the
> Server uses the `ResetErrorStrings.ini` file. Otherwise it uses the
> corresponding language's .ini file. The messages available for editing
> are contained in this `.ini` file.

7. Open the `.ini` file in Notepad or another text editor.

8. Change the message to read as you want it to display to the end user.

> **Note:** Be certain to enter the message as one continuous line. If you
> want to display the message to the end user as separate paragraphs,
> use the `<br>` tag.

9. Save your changes and close the file. The next time a user enters an unacceptable
   password, he will see your edited message. For example, "The password did not
   meet password policy requirements. Please enter a password at least seven
   characters long."

4.9.3 Role/Group Support

System questions can be assigned to particular roles or user groups. Role/Group
assignment determines the questions a user will be asked during the enrollment
interview.

> **Note:** You cannot assign questions to users or groups when using a database (such as Microsoft SQL Server or Oracle Database) for your repository. The settings are available for editing, but the assignments will not be written to the database.

The **Access Control** panel makes users and groups available so that you can assign question rights to them. The **Users and Groups** list is unpopulated until you check the **Show Users** box. Domain users and groups are not initially assigned Allow or Deny access for a given question.
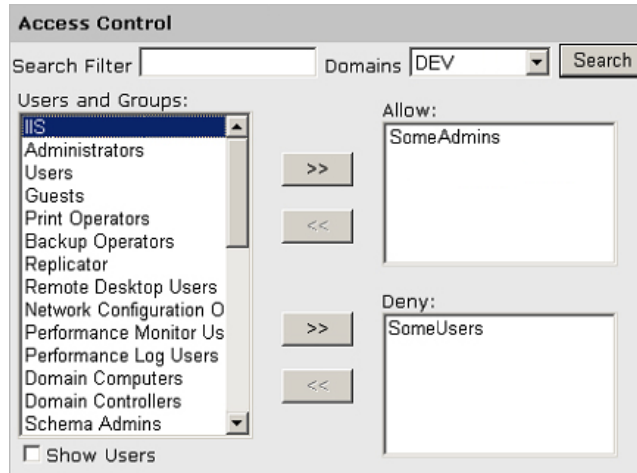
When a user or group is selected, the arrow buttons (**<<** and **>>**) become enabled. You move users back and forth between the **Users and Groups** list and the **Allow** and **Deny** lists by clicking the arrow buttons. When you click **Create** or **Modify**, the Role/Group access rights are written to the back-end storage for the system question.

The rules for Access Control are as follows:

- **Allow/Deny lists empty**: All users and groups receive the question.

- **Allow list empty, Deny list populated**: All users and groups in the Deny list do not receive the question. All other users and groups receive the question; Allow is implicit.

- **Deny list empty, Allow list populated**: All users and groups in the Allow list receive the question. All other users/groups do not. Deny is implicit.

- **Both lists populated**: Users and groups in the Allow list that are not in the Deny list receive the question. If a user or group in the Allow list is also in the Deny list, or belongs to a group in the Deny list, that user or group does not receive the question. Deny overrides Allow.

A user's or group's presence in the **Deny** list always supersedes its presence in the **Allow** list.

The following table provides information about user and group permissions.

Scenario Number	Description	Allow	Deny	Outcome
1	No user or group specified in Allow and Deny lists	Ø	Ø	Everyone receives the question.

Scenario Number	Description	Allow	Deny	Outcome
2	Dr. Baxter specified in Allow list; no one specified in Deny list	Dr. Baxter	Ø	Only Dr. Baxter receives the question. All others users are denied.
3	Dr. Baxter specified in Deny list; no one specified in Allow list	Ø	Dr. Baxter	Everyone receives the question except Dr. Baxter.
4	Doctors group specified in Allow list; Dr. Loomis, a member of Doctors group, specified in Deny list	Doctors	Dr. Loomis	All members-and only members-of Doctors group receive the question, except Dr. Loomis, who is denied the question.
5	Doctors group specified in Deny list, Dr. Loomis specified in Allow list	Dr. Loomis	Doctors	Everyone, including Dr. Loomis, is denied the question. The Deny list supersedes the Allow list.

The scenarios below demonstrate how to apply these rules.

You have set up a group, Doctors, which includes members Dr. Baxter and Dr. Loomis.

- **Scenario 1**: If the Allow and Deny lists are unpopulated, all users and groups receive the question.

- **Scenario 2**: If the Deny list is unpopulated and the Allow list is populated, only users and groups in the Allow list receive the question.

- **Scenario 3**: If any user or group is in the Deny list, and the Allow list is unpopulated, only the user or group in the Deny list does not receive the question.

- **Scenario 4**: If a group is in the Allow list but a member of that group is in the Deny list, all members of that group receive the question except the member in the Deny list.

- **Scenario 5**: If a group is in the Deny list but a member of that group is in the Allow list, that member will not receive the question.

4.10 Managing Users

Use the **Manage Users** tab (under the **Users** node) to generate reports on the enrollment status of end users. This report indicates whether or not users have completed the Enrollment Interview, the date and time of enrollment, and whether or not the user is currently locked out.
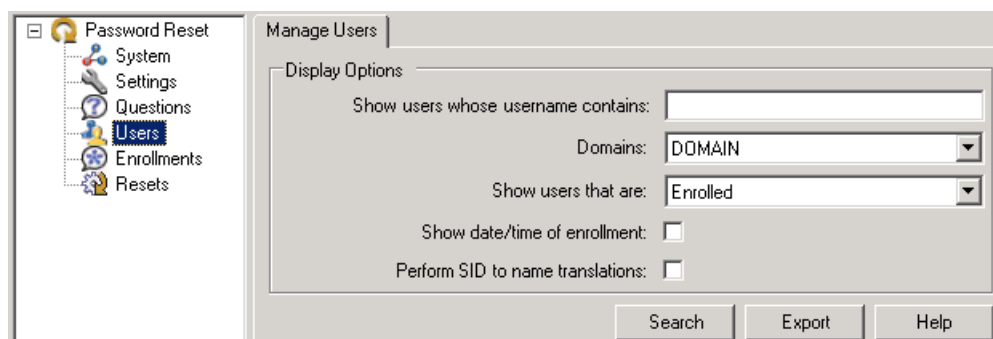
To generate a report, select the appropriate display options. Click **Search** to generate and display the report on your screen, or click **Export** to save the report as a CSV file.
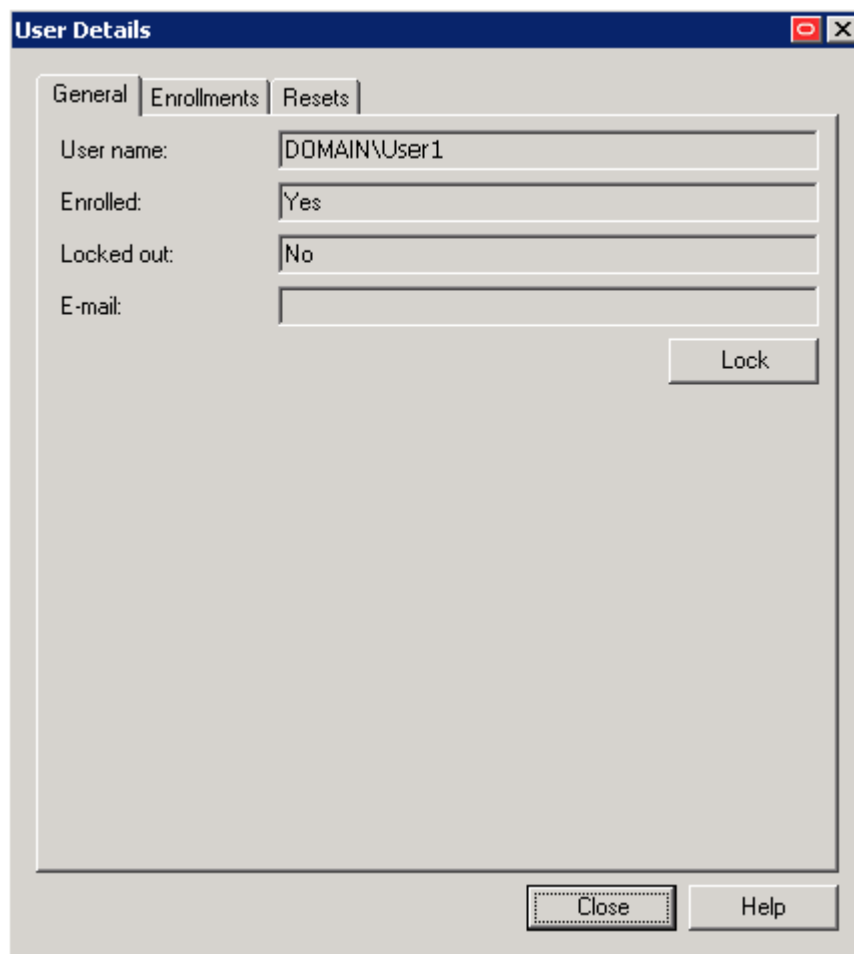
Field	Options
Show users whose username contains	Enter text for the report search to match.
Domains	Select from the available domains.
Show users that are:	Select the user enrollment status to generate a report on: ■ Enrolled ■ Not Enrolled ■ Both
Show date/time of enrollment	Select to display the date and time of enrollment. (Enabling this may increase report generation time.)
Perform SID to name translations	Check the box if you want to use Active Directory to retrieve users' usernames based on their SIDs, rather than retrieving them from the repository cache. Enabling this setting slows performance, but is useful in instances where users have changed their usernames since their initial enrollment.

4.10.1 User Details General Tab

This tab displays the following information about a user account:

- **User Name.** The name associated with this account.

- **Enrolled.** The current enrollment status of this account.

- **Locked Out.** Whether the end user has been locked out of the reset service for having repeatedly failed the Reset Quiz; the number of permitted consecutive failures and the duration of the lockout are specified on the **Settings** tab (under the **Settings** node).

- **E-mail.** The end user's e-mail address.
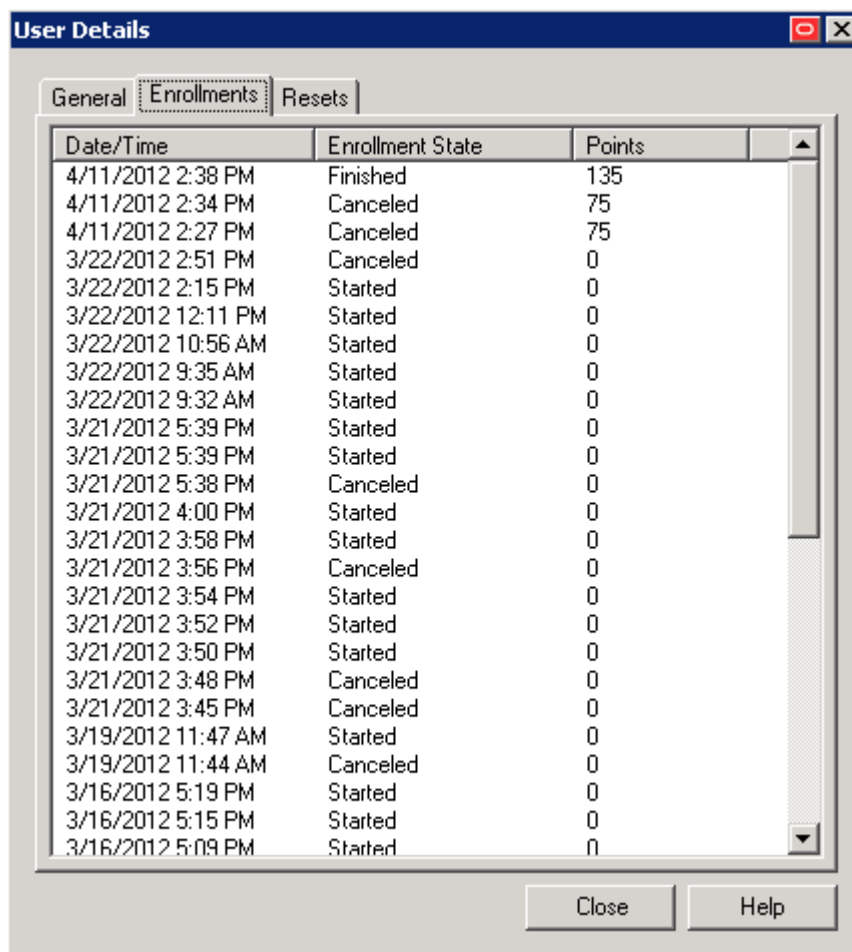
A user whose account is unlocked will have a **Lock** button beneath the information fields, and a user whose account is locked will have an **Unlock** button beneath the information fields. You can change the lockout status of a user by clicking **Lock** or **Unlock** as appropriate.

4.10.2 User Details Enrollments Tab

This tab provides information about the enrollment status of the specified user:

■   The date and time of each enrollment attempt.

■   The current status of the enrollment. There are three possible statuses:

–   **Started.** The user has begun to take the Enrollment Interview but has not completed it.

–   **Finished.** The user has completed the Enrollment Interview.

–   **Canceled.** The user began to take the Enrollment Interview but canceled before answering enough questions to reach the authentication threshold.

■   The total number of points that the user accumulated with the questions he answered.

4.10.3 User Details Resets Tab

This tab provides information about the reset status of the specified user:

- The date and time of each reset attempt

- The current status of the reset; that is, whether it was successful

- The score the user achieved on the Reset Quiz

- The IP address of the workstation at which the user took the Reset Quiz
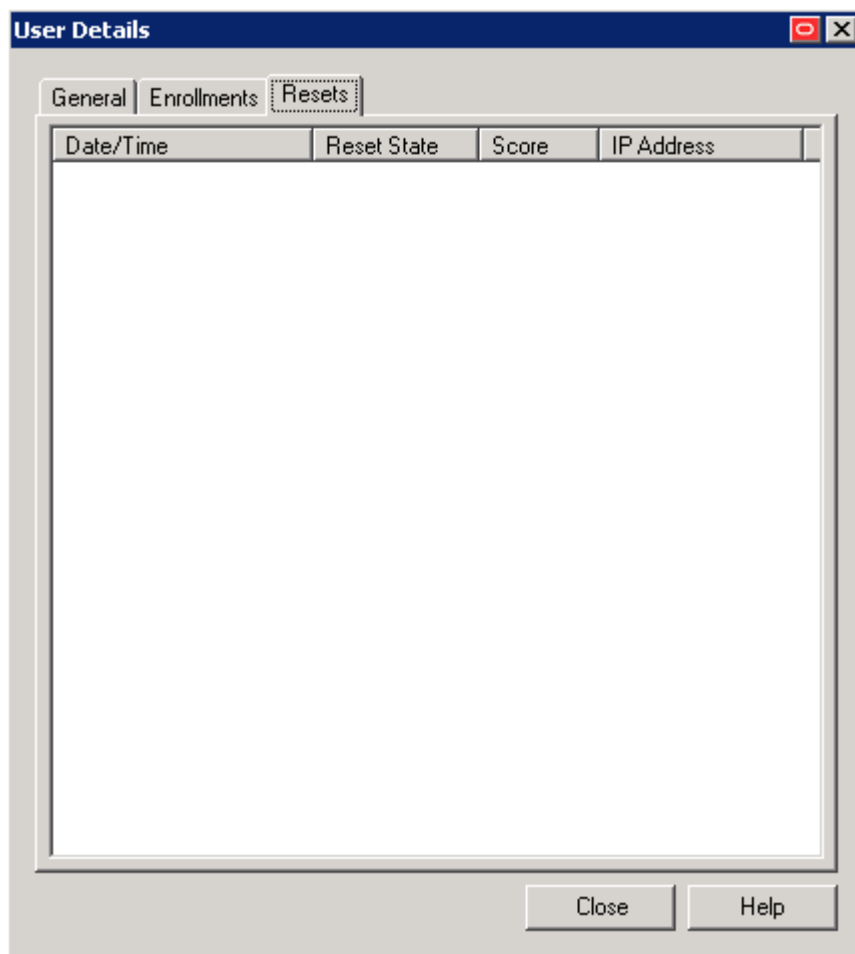
4.10.4 Managing Enrollments

Use the **Manage Enrollments** tab (under the **Enrollments** node) to view, export, or delete enrollment log entries within a specified date range.
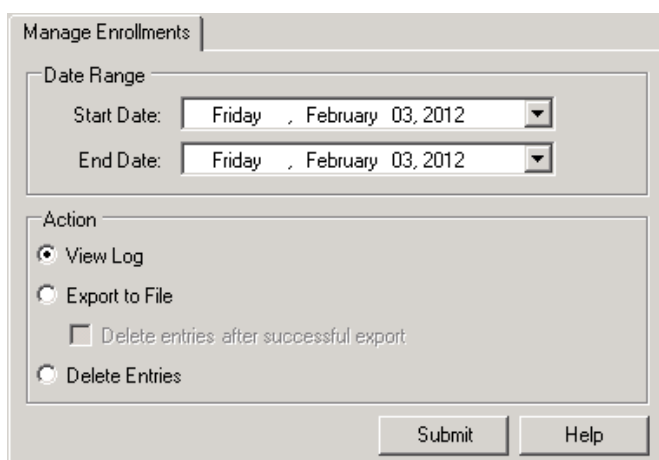
1. Select a **Start Date** and an **End Date** for the date range from the pop-up calendars).

2. Select an **Action**:

- **View log** opens the **Search Results** window where you can review users, their status, scores, and the time of their activity.

- **Export to file** saves all log entries within the specified date range to a file in comma-separated-value format. Select the **Delete entries after successful export** checkbox if you want to remove the exported log entries after saving them to a file.

- **Delete entries** removes all log entries within the specified date range, without saving them.

3. Click **Submit**. If you have selected **Export to file**, in the **Save As** dialog, enter a file name and click **OK**.

See Setting Up the Enrollment Interview for more information.

4.10.4.1 Viewing Enrollment Search Results

Use the **Search Results** screen (from the **Manage Enrollments** tab) to view the enrollment log.
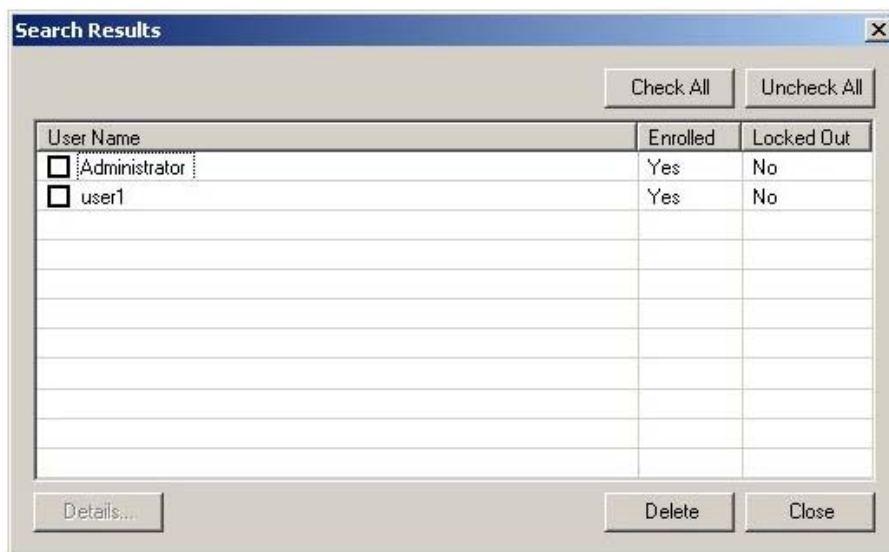
This log records enrollment activity for all users who have taken (or at least started) the Enrollment Interview within the time span you specify:

- The names of all users who began the Enrollment Interview.

- The current enrollment status of each user.

- The total point values of all system questions (Required and Optional) that the end user answered during enrollment.

- The date and time of each enrollment activity.

See Setting Up the Enrollment Interview and Managing Enrollments for more information.

4.11 Managing Resets

Use the **Manage Resets** tab (under the **Resets** node) to view, export, or delete reset log entries within a specified date range.

1. Select a **Start Date** and an **End Date** for the date range for the date range from the pop-up calendars).

2. Select an Action:

    ■   **View Log** opens the **Search Results** window where you can review users, their status, scores, and the time of their activity.

    ■   **Export to File** saves all log entries within the specified date range to a file in comma-separated-value format. Select the **Delete entries after successful export** checkbox if you want to remove the exported log entries after saving them to a file.

    ■   **Delete** removes all log entries within the specified date range, without saving them.

3. Click **Submit**. If you have selected **Export to File**, in the Save As dialog, enter a file name and click **OK**.

See Configuring Reset Authentication for more information.

4.11.1 Viewing Resets

Use the **View Resets** dialog (under the **Resets** tab) to view the reset log. The record for each Reset Quiz given shows the username, the date and time of the quiz, the quiz score, the current reset status, and the IP address of the workstation used to take the quiz.

To view log entries within a specific date range, enter a **Start Date** and an **End Date** (or click **Choose** to select a date from a pop-up calendar), then click **Submit**.

See Configuring Reset Authentication for more information.

4.11.1.1 Viewing Reset Search Results

Use the **Search Results** window (under the **Manage Resets** tab) to view the reset log. This log records reset activity for all users who have taken (or at least started) the Reset Quiz within the time span you specify:

- The names of all users who began the Reset Quiz

- The current reset status of each user

- The score the user achieved during the Reset Quiz

- The date and time the user attempted to reset his password

- The IP address of the workstation from which the user took the Reset Quiz

See Creating System Questions and Managing Enrollments for more information.

4.11.1.2 Viewing User Search Results

This table contains a list of the users who met the search criteria you defined on the Manage Users tab, with their enrollment and lockout status. From this list you also can:

- Unenroll a user by checking the box next to the **User Name** and clicking **Unenroll**. Use the **Check All** and **Uncheck All** boxes to select or deselect all names in the list quickly.

- Learn more about a user's history by highlighting the **User Name** (not the checkbox) and clicking the **Details** button at the bottom of the page to launch the **User Details** screen.

    Note: The **Details** button is only available if the user account contains information other than the User Name.

4.12 Working with External Validators

By default, Password Reset requires the administrator to create and configure all the questions and weights used for reset, and the user to answer these questions upon enrollment. Password Reset can also work with external validator sources to simplify this process. External validators allow organizations to write an interface, which can be accepted by Password Reset, to their back end. This validator can call data from various sources (for example, the HR database) that contain pre-defined answers.

For example, suppose one of the reset questions is "What is your Social Security Number?" By default, when a user enrolls, the enrollment interview asks him to supply his social security number. Then when a user resets his password, he is asked to enter his social security number. With an external validator in place, an administrator can direct Password Reset to an external data source which contains a pre-defined list of social security numbers. The validator supplies the answer to that question upon user enrollment so that the user does not even have to see that question. A user will only have to enter the answer to that question when attempting to reset his password. If all system questions are answered by an external validator, users can be automatically enrolled.

The basic steps to implement the use of external validators are:

1. Writing the External Validator Interface

2. Installing the External Validator

3. Directing Password Reset to the External Validator

4.12.1 Writing the External Validator Interface

The external validator must be written in .NET 4.0. To write an implementation, add a reference to the library `Passlogix.PasswordReset.dll`. Within your assembly, a class

implementing the interface, ISSPRValidator, must be written. The interface has the following five methods:

- Initialize

- Cleanup

- IsValidQuestion

- IsValidAnswer

- FriendlyName

> **Note:** Validators that do not implement the ISSPRValidator interface or fail on startup will be ignored.

The validator interface definition is as follows:

```
public interface ISSPRValidator
{
// Called by ESSO-PR on first use of validator.
void Initialize();

// Called once by ESSO-PR when the service shuts down.
void Cleanup();

// Returns true/false if question is valid for a given user
bool IsValidQuestion(ISSPRQuery iquery);

// Returns true/false if question/answer pair is correct
bool IsValidAnswer(ISSPRQuery iquery, string strAnswer);

// The friendly name for SSPR to display
string FriendlyName { get; }
}
```

The ISSPRQuery interface is supplied by the SSPR service and contains the following properties:

```
interface ISSPRQuery
{
// The guid of the question
Guid QuestionGuid { get; }

// The user's identity (in SID format)
string UserIdentity { get; }
}
```

After this interface has been implemented, the following attribute must be declared referencing the implementation:

```
[assembly: ISSPRValidatorType("<Validator class>")]
```

Replace the string <Validator class> with the full name of the class (including namespace) that implements this interface.

4.12.2 Installing the External Validator

After the validator.dll is written, follow these steps:

1. Create a directory called `Validators` under `INSTALL_
   DIR\VgoSelfServiceReset\WebServices`.The actual validator directory is defined in `web.config` and can be changed if a different folder for discovery is preferred.

2. Copy the validators into this directory.

3. Restart the Password Reset Web Service.

4.12.3 Directing Password Reset to the External Validator

After the validators are installed, do the following:

1. Open the **Password Reset** node of the Administrative Console.

2. Click **Questions** from the top menu and then select **System Questions**. Select an existing question or create a New Question.

3. The **Answer Source** drop-down field lists the available external validators that can be used. The default is **User Supplied**, which indicates that the user must answer that question during enrollment. If a validator is installed and detected, its friendly name will now be listed here. Select the appropriate validator and save the question settings.

4.12.3.1 User Enrollment with External Validators

Enrollment can contain a mix of User Supplied and Validator Supplied questions. Questions that require external validation will be checked against `IsValidQuestion` and `allowed/discarded` based on the result. A user will be prompted for answers only on questions that are user supplied. In a pure external validation case, the user will be automatically enrolled.

4.12.3.2 Password Reset with External Validators

During a password reset, questions with answers supplied by an external validator will be sent to `IsValidAnswer` to determine a pass or fail for a particular question.

4.12.4 Deleting the External Validator

To delete an external validator:

1. Remove the `.dll` from the directory in which you placed it.

2. Return to the Administrative Console, and individually select for editing the questions that relied on the external validator.

   You will be presented with the error message, "The validator <validator details> cannot be found. Answer Source will default to User Supplied."

3. Click the **Modify** button.

> **Note:** Deleting an external validator results in users' failing the reset quiz, but does not force them to re-enroll. In order to force their re-enrollment, you must delete users whose enrollment was dependent on the external validator.

5

Configuring Strong Authenticators with 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.

In this chapter, you will learn the following:

- Overview of Universal Authentication Manager
- Deploying Universal Authentication Manager
- Working with Universal Authentication Manager Policies

5.1 Overview of Universal Authentication Manager

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.

5.1.1 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 takes place only 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 Universal Authentication Manager for Synchronization with Microsoft Active Directory and Configuring

Universal Authentication Manager for Synchronization with Microsoft AD LDS (ADAM).

5.1.1.1 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 Section 7.5, "Universal Authentication Manager Registry Settings"

5.1.1.2 Repository Functions

- Stores Universal Authentication Manager policies and enrollment data.

- Leverages existing repository schemas used by other Oracle Enterprise Single Sign-On Suite products.

- Enrollment data is secure and access to it is restricted.

5.1.1.3 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.

5.1.2 Administration of Universal Authentication Manager

Universal Authentication Manager administrators can configure and apply Universal Authentication Manager policy settings from a central location using the Administrative Console. The 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 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 Microsoft AD LDS (ADAM) in *Oracle Enterprise Single Sign-On Suite Installation Guide* for information on performing this procedure.

5.1.3 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 v1.12 (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.

5.1.4 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 Section 7.5, "Universal Authentication Manager Registry Settings"

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)

5.1.4.1 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.

> **Note:** 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.

5.1.5 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.

5.1.5.1 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.

> **Note:** To have Universal Authentication Manager generate a key pair, you must configure it to do so via Section 7.5, "Universal Authentication Manager Registry Settings" Universal Authentication Manager does not generate digital certificates and one is not required in such a 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.

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.

5.1.6 Challenge Questions

The **Challenge Questions method** 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.

> **WARNING:** If you are 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 as described in Integrating with Password Reset.

- 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.

> **Note:** 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.

5.2 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 Microsoft Active Directory
- Configuring Universal Authentication Manager for Synchronization with Microsoft AD LDS (ADAM)
- Integrating with Logon Manager
- Integrating with Password Reset
- Integrating with Kiosk Manager

5.2.1 Selecting the Client Mode

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

5.2.1.1 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 cannot 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.

5.2.1.2 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.

> **WARNING:** If you are 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.

5.2.1.3 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 Prepare the Universal Authentication Manager Repository in *Oracle Enterprise Single Sign-On Suite Installation Guide*.

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.

> **WARNING:** 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.**

5.2.2 Configuring Universal Authentication Manager for Synchronization with Microsoft Active Directory

> **Note:** 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 and Microsoft AD LDS (ADAM) are supported as repositories.

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:

- Creating a Universal Authentication Manager Service Account

- Extending the Schema

- Enabling Data Storage Under User Objects

- Initializing Universal Authentication Manager Storage

- Configuring the Universal Authentication Manager Synchronizer

- Configuring Universal Authentication Manager Synchronization for Administrative Users

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.

5.2.2.1 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.

5.2.2.2 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.
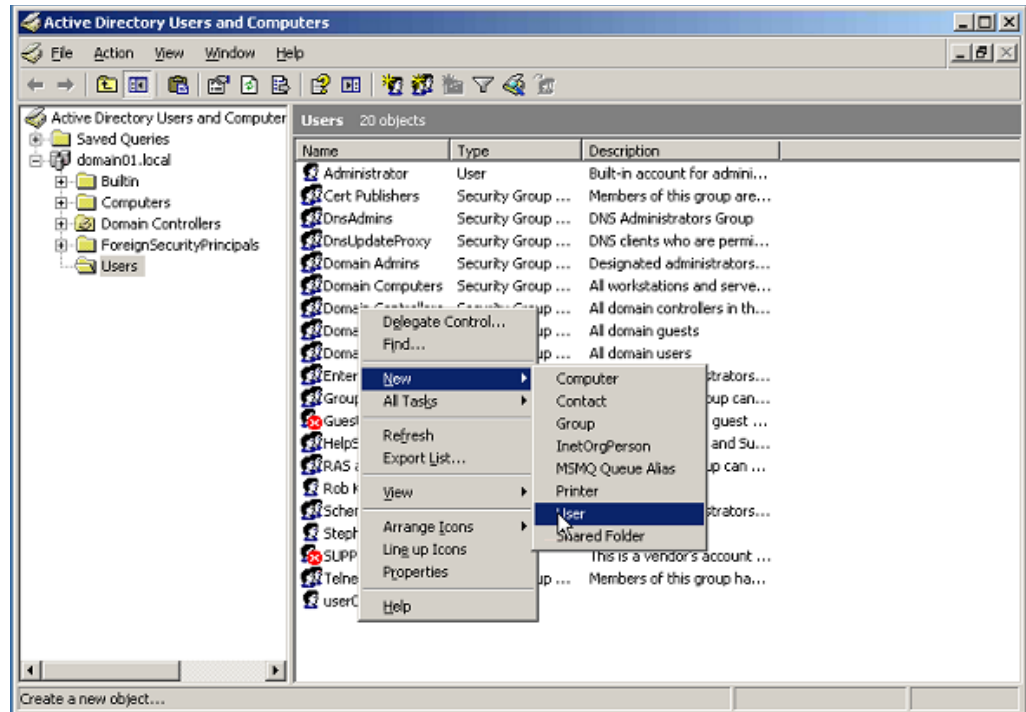
3. Enter a name for the user or group account (for this example, the name is `uamservice`) and click **Next>**.
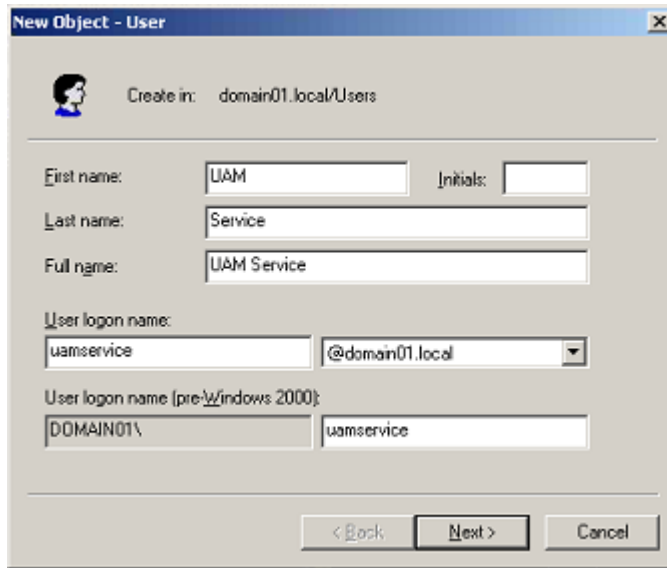
4. Enter a password, select the **Password never expires** box, and deselect the **User must change password at next logon** box.

5.2.2.3 Extending the Schema

> **Note:** 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 Administrative Console.

2. From the **Repository** menu, select **Extend Schema**.

3. In the Connect to Repository dialog 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.

5.2.2.4 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:

> **Note:** 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 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.
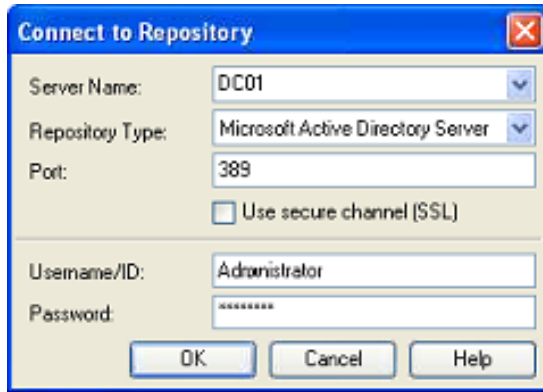
3. From the **Repository** menu, select **Enable Storing Credentials Under User Object**.

4. In the prompt that appears, click **OK**.

5. In the confirmation dialog that appears, click **OK** to dismiss it.

5.2.2.5 Initializing Universal Authentication Manager Storage

Perform these steps after successfully extending the schema.

1. Return to the **Repository** menu and select **Initialize UAM Storage**.
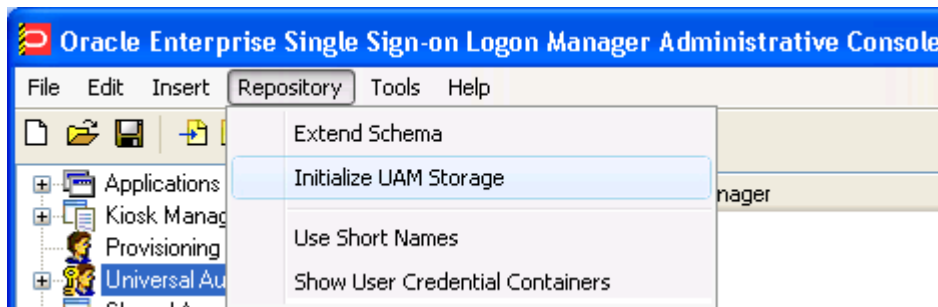
2. From the drop-down menu, select the server that you just created. The other fields are filled in automatically.
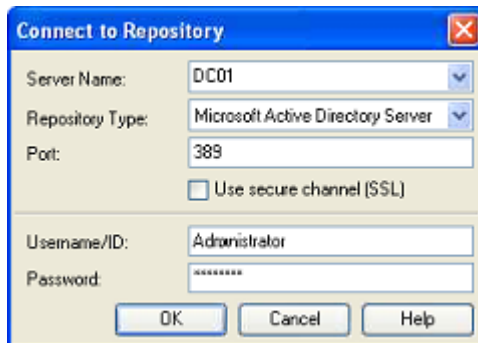
3. Click **OK**.

4. In the **Select User or Group** dialog, start typing the name of your service account, then click **Check Names**. The service account name is filled in automatically.
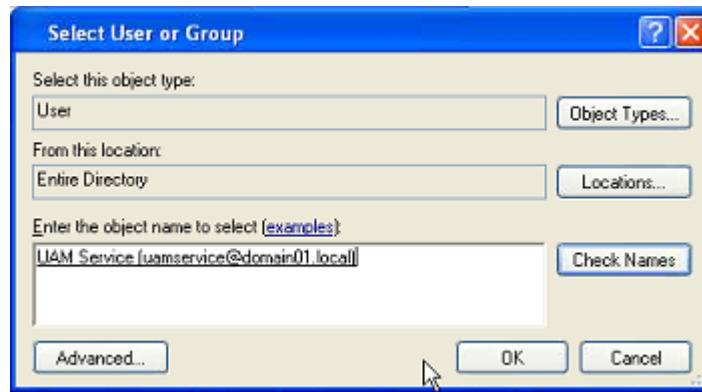
5. Click **OK** and wait for the success message.
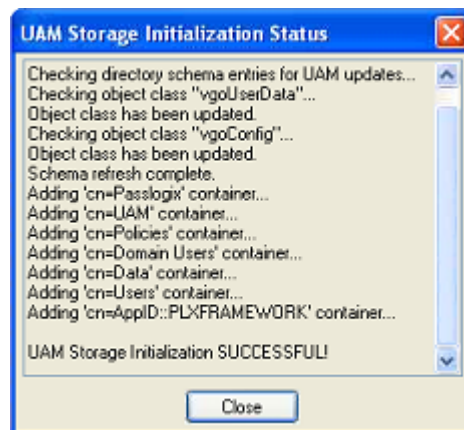
The data structures have now been created and the required permissions set. For more information on what's done in the repository during this step, see the next section.

5.2.2.5.1 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:

■ Modifies the schema to ensure that `vgoUser` and `vgoConfig` classes may be placed inside Container objects.

■ Builds the default container structure `Program Data/Passlogix/UAM` with subcontainers `Policies` and `Index` as shown below:

> **Note:** 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.

- 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.

- 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.

- 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.)

- 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.

5.2.2.6 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 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:

      Select the check box.

      Click the ellipsis ("**…**") button.

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

      Click **OK**.

5. In the **Base location(s) for UAM storage index** field, select the check box, click the ellipsis ("**…**") 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 Administrative 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**.

   Note: The Console produces a .REG file compatible only with 32-bit systems. If you are merging the .REG file on a 64-bit system, you must include the /reg:32 switch in your import command to merge the registry data into the correct location within the registry; otherwise, Universal Authentication Manager will not function.

   For example: reg.exe import MyRegistryFile.reg /reg:32

   ---

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

5.2.2.7 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 necessary to create and delete `vGOUserData` and `vGOSecret` objects.

> **Note:** 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 administrative 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. For more information about this issue, see Microsoft Knowledge Base Article 817433 available at the Microsoft Help and Support site: 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 on 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:
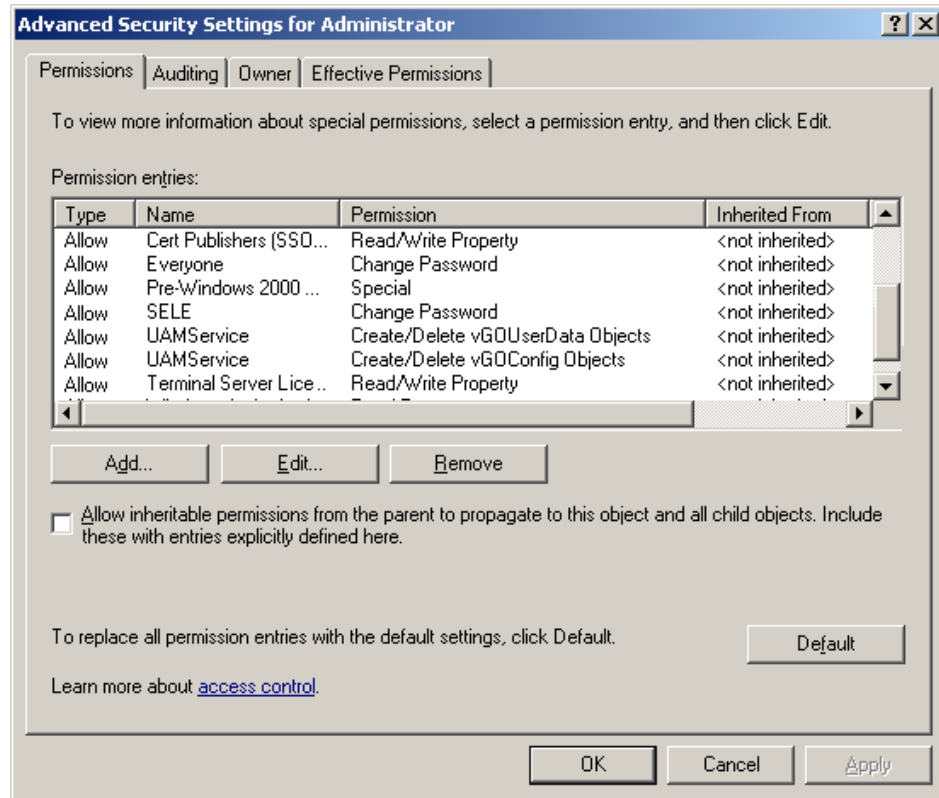
7. In the dialog, check whether:

   - 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.
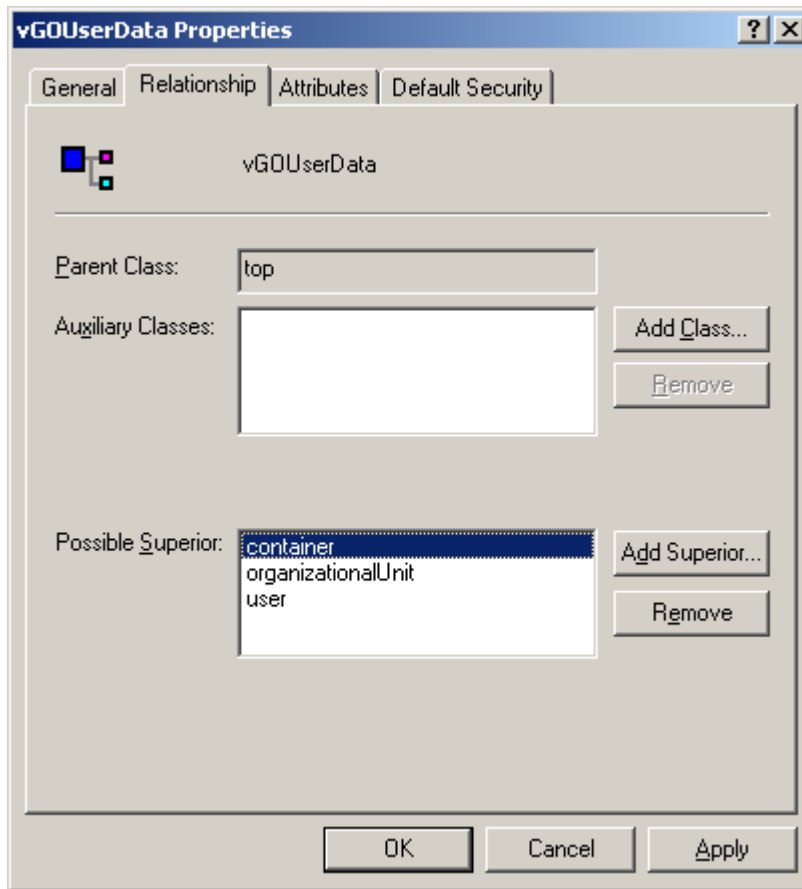
8. In the Microsoft Management Console, open the **Active Directory Users and Computers** snap-in.

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 Manager service 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**.

    > **Note:** If the create and delete permissions for vGOUserData objects do not appear in the permissions list, select **User** objects from the **Apply on to:** 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:
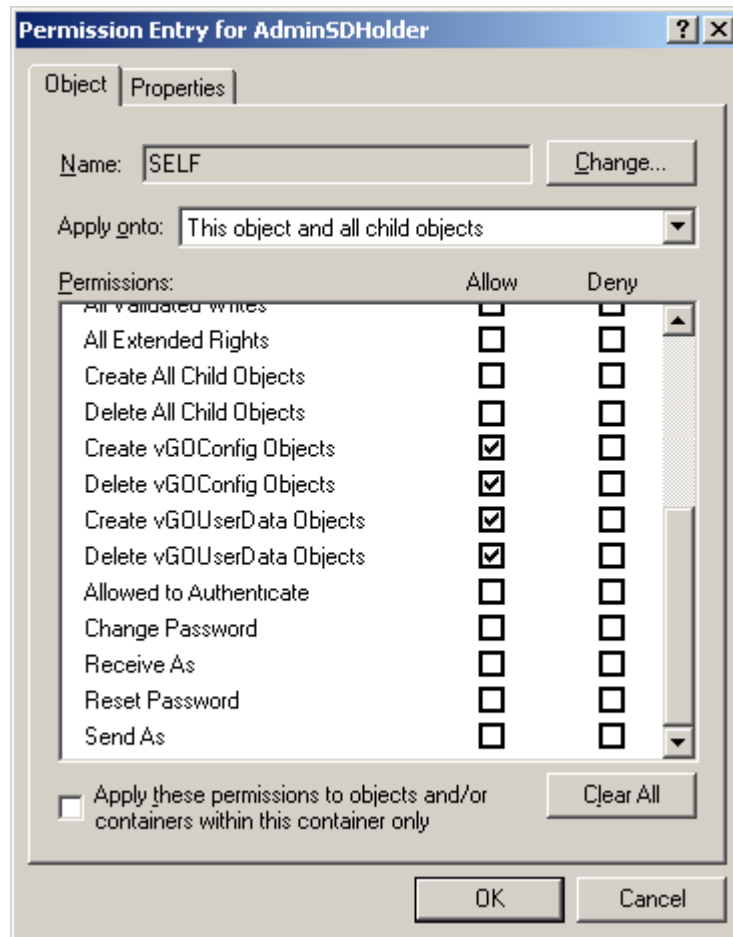
c. Click **OK**.

16. Trigger the SD propagator (SDPROP) process to immediately propagate the changes throughout the network. For instructions for launching the SD propagator process, see Microsoft Knowledge Base Article 251343 available at the Microsoft Help and Support site: http://support.microsoft.com/kb/251343.

Note: 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.

Deploying Universal Authentication Manager

5.2.3 Configuring Universal Authentication Manager for Synchronization with Microsoft AD LDS (ADAM)

> **Note:** 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 and Microsoft AD LDS (ADAM) are supported as repositories.

In order to allow Universal Authentication Manager to centrally store and manage policies and enrollment data in Microsoft AD LDS (ADAM), you must prepare a Microsoft AD LDS (ADAM) instance and configure Universal Authentication Manager for synchronization with that repository by performing the following tasks:

- Create the AD LDS (ADAM) Instance and Partition
- Configure the AD LDS (ADAM) Default Naming Context
- Create a Universal Authentication Manager Service Account
- Extend the Schema
- Create the `People` Container
- 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.

5.2.3.1 Preparing the Repository when Logon Manager Is Already Deployed

If Logon Manager is already installed and synchronizing with your AD LDS (ADAM)-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 create the `People` container. Instead, complete the following steps:

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

Universal Authentication Manager requires that the `People` container is located in its default location. If you have configured Logon Manager to use a `People` container located elsewhere (e.g. not in the root of the AD LDS (ADAM) partition), Universal Authentication Manager will not be able to share that container with Logon Manager; you will need to create a separate `People` container at the root of the AD LDS (ADAM) partition for Universal Authentication Manager.

5.2.3.2 Creating the AD LDS (ADAM) Instance and Partition

If you have not already done so, create an AD LDS (ADAM) instance and partition by following the steps in the "Creating an AD LDS (ADAM) Instance" section of the guide *Deploying Logon Manager with a Directory-Based Repository*.

5.2.3.3 Configuring the AD LDS (ADAM) Default Naming Context

After you have created your AD LDS (ADAM) instance and partition, you must point the instance's default naming context to the target partition so that Universal Authentication Manager is able to locate its data within the repository.

1. Launch the `ADSIEdit` tool (available from the Microsoft website) and connect to the "Configuration" context of the target AD LDS (ADAM) instance.

2. In the left-hand tree, navigate to **Configuration** > **CN=Sites** > **CN=SiteName** > **CN=InstanceName** .

3. Under the instance node, double-click the **CN=NTDS Settings** child node.

4. In the properties dialog that appears, select the **msDS-DefaultNamingContext** attribute and click **Edit**.

5. In the editor dialog that appears, enter the fully qualified distinguished name of the target AD LDS (ADAM) partition, then click **OK** to save your changes.
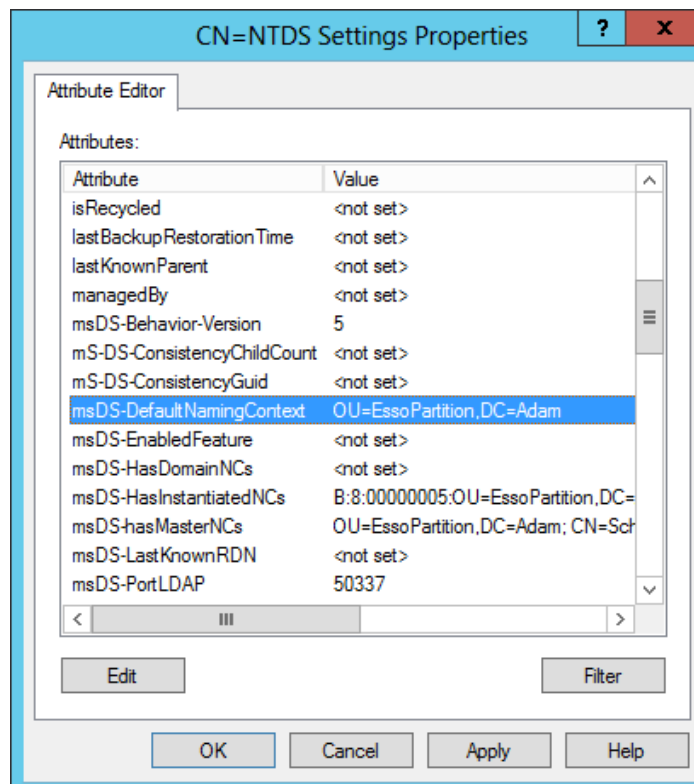
6. Click **OK** to save your changes and dismiss the properties dialog.

7. Restart the affected AD LDS (ADAM) instance by restarting the corresponding service in the Windows Services Manager.

5.2.3.4 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. However, you must add the account to the target AD LDS (ADAM) instance's "Readers" group.

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, select the **Password never expires** box, and deselect the **User must change password at next logon** box.

5. Add the Universal Authentication Manager service account to the AD LDS (ADAM) instance's "Readers" group:

    a. Start the ADSIEdit tool (available from the Microsoft website) and connect to the data partition of the target AD LDS (ADAM) instance.

    b. In the left-hand tree, expand the target partition and select the **CN=Roles** node.

    c. In the right-hand pane, double-click the **CN=Readers** role.

    d. In the properties dialog that appears, do the following:

    Select the member attribute and click **Edit**.

    In the attribute editor dialog that appears, click **Add Windows Account**.

    In the dialog that appears, enter the name of the Universal Authentication Manager service account and click **Check Names**.

    Once the name validates successfully, click **OK** to dismiss the account selection dialog.

    Click **OK** to save your changes and dismiss the attribute editor dialog.
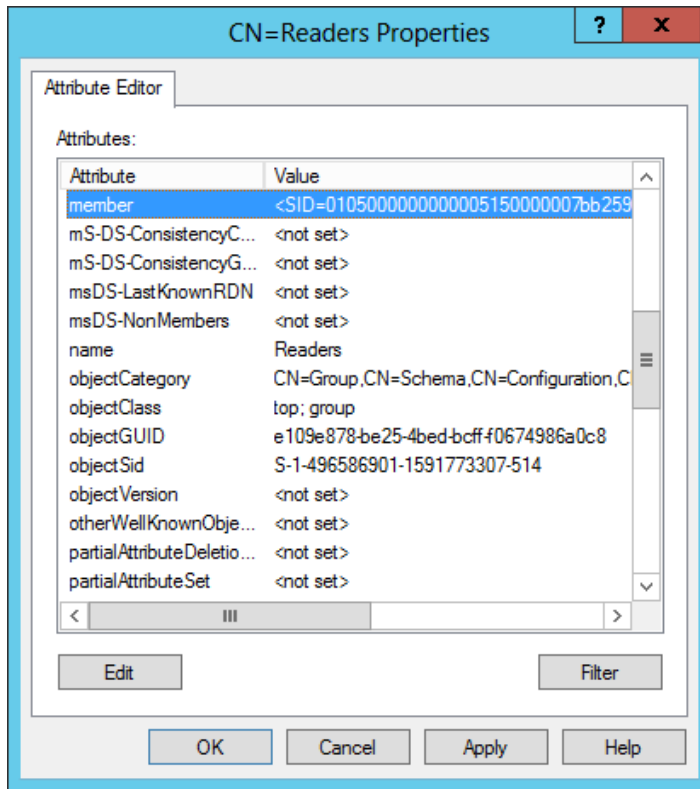
e. Click **OK** to save your changes and dismiss the properties dialog.

5.2.3.5 Extending the Schema

> **Note:** 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 Administrative Console.

2. From the **Repository** menu, select **Extend Schema**.
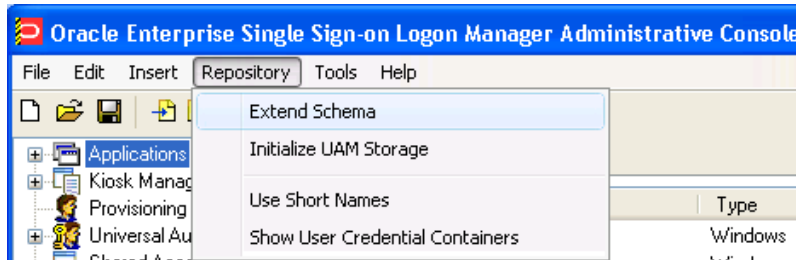
3. In the **Connect to Repository** dialog that appears, enter a Server Name, select **Microsoft AD LDS (ADAM)** from the drop-down menu, select the **Use secure channel (SSL)** check box if your environment is configured for SSL connectivity, enter the Port number, and the Username/ID and Password of an administrative account with Domain and Schema Administrator permissions. Click **OK** when finished.

5.2.3.6 Creating the People Container

In order to allow Universal Authentication Manager to store enrollment data in AD LDS (ADAM), you must create an `OU` named `People` at the root of your AD LDS (ADAM) partition. You must not rename or move this container or Universal Authentication Manager synchronization will not function.

If Logon Manager is already installed and synchronizing with the repository and it is using a custom `People` container location, you must still create the `People` container for Universal Authentication Manager at the root of the AD LDS (ADAM) partition.

Oracle recommends that you maintain separate `People` containers for Logon Manager and Universal Authentication Manager when sharing an AD LDS (ADAM) instance.

1. In the Administrative Console, select the **Repository** node in the tree.

2. Click the **Click here to connect link** in the right-hand pane. The Console displays the Connect to Repository dialog. Fill in the fields as explained in step 3 in the previous section and click **OK** to connect.

3. In the tree, right-click the root of the target AD LDS (ADAM) instance, and select **Create People Container** from the context menu.
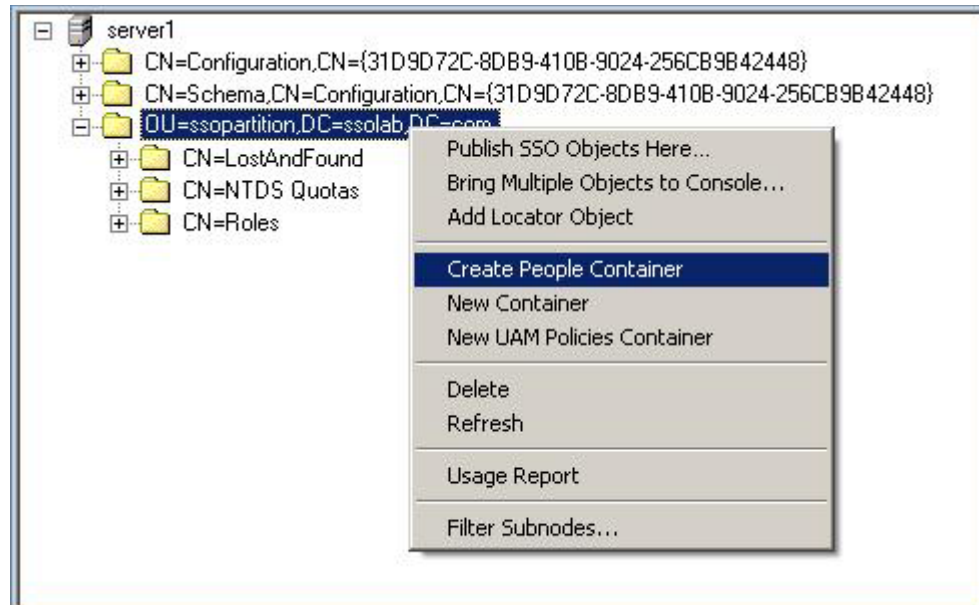
4. Verify that the `People` container now exists at the root of the AD LDS (ADAM) instance's sub-tree.

5.2.3.7 Initializing Universal Authentication Manager Storage

Perform these steps after you have successfully extended the schema.

1. Return to the **Repository** menu and select **Initialize UAM Storage**.
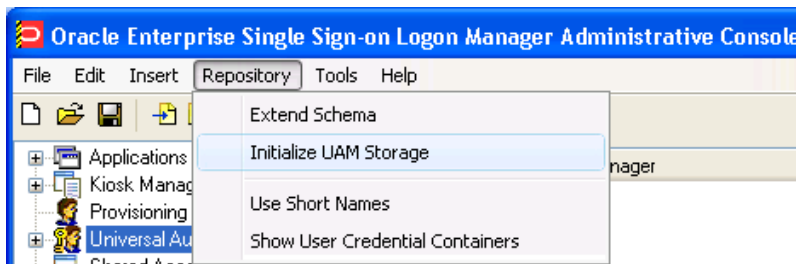
2. From the drop-down menu, select the server that you just created and click **OK**. (The other fields are filled in automatically.)

3. In the **Select User or Group** dialog, start typing the name of your service account, then click **Check Names**. The service account name is filled in automatically.
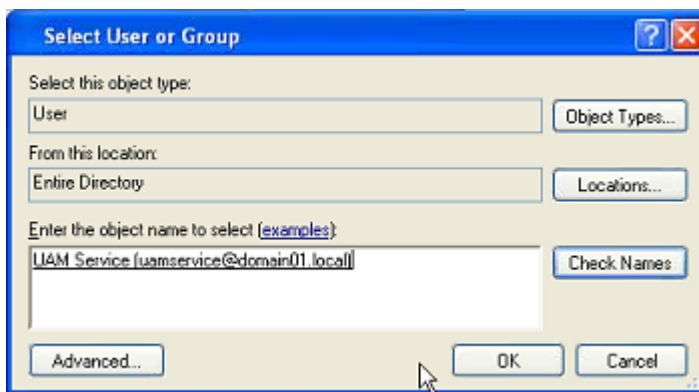
4. Click **OK** and wait for the success message.
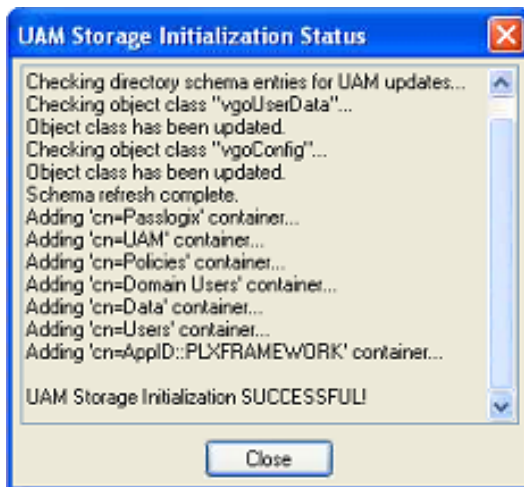
The data structures have now been created and the required permissions set. For more information on what's done in the repository during this step, see the next section.

5.2.3.7.1 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:

- Modifies the schema to ensure that `vgoUser` and `vgoConfig` classes may be placed inside Container objects.

- Builds the default container structure "`Program Data/Passlogix/UAM`" with subcontainers "`Policies`" and "`Index`" as shown below:

ADSI Edit
  ◢ ▤ Default naming context [localhost:50000]
    ◢ 📁 OU=esso-partition,DC=domain,DC=local
        📁 CN=ForeignSecurityPrincipals
        📁 CN=LostAndFound
        📁 CN=NTDS Quotas
        📁 OU=People
      ◢ 📁 CN=Program Data
        ◢ 📁 CN=Passlogix
          ◢ 📁 CN=UAM
              📁 CN=Index
              📁 CN=Policies
        📁 CN=Roles

> **Note:** 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.

- 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.

- 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.

- Updates the root `DSE` object of the AD LDS (ADAM) partition to grant the Universal Authentication Manager service account permissions to create and delete `vgoConfig` and `vGoUser` objects under `User` objects across the entire AD LDS (ADAM) partition. (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.)

- Updates the root `DSE` object of the AD LDS (ADAM) partition to grant the Universal Authentication Manager service account generic read permissions to all `vgoConfig` objects across the AD LDS (ADAM) partition so that the Universal Authentication Manager service can read all `vgoConfig` objects regardless of their location in the repository.

5.2.3.8 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 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 AD LDS (ADAM) 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 **Microsoft AD LDS (ADAM)**, enter `ADAMSyncExt` as the name, and click **OK**.

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

4. If Logon Manager is installed and synchronizing with the repository, do not modify the value of the **Servers**, **SSL**, or **Base location(s) for configuration objects** fields; instead, skip to the next step.

    If Logon Manager is not installed and synchronizing with the repository, do the following:

    a. In the **Servers** field, select the check box.

    b. Click the ellipsis ("**…**") button.

    c. In the window that appears, enter the full address(es) and port(s) of your AD LDS (ADAM) instances, one per line, in the format *server:port*.

    d. Click **OK**.

    e. In the **Base location(s) for configuration objects** field, select the check box.

    f. Click the ellipsis ("**…**") button.

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

    h. Click **OK**.

    i. If your environment is not using SSL, select the check box next to the **SSL** field and select **No** from the drop-down field. Oracle highly recommends enabling SSL in your environment for maximum security.

5. In the **Base location(s) for UAM storage index** field, select the check box, click the ellipsis ("**…**") button, and enter the fully-qualified `DN` of the `Index` container, then click **OK**.

6. In the **Prepend Domain** field, select the check box and select **Yes** from the drop-down menu.

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**.

> **Note:** The Console produces a `.REG` file compatible only with 32-bit systems. If you are merging the `.REG` file on a 64-bit system, you must include the `/reg:32` switch in your import command to merge the registry data into the correct location within the registry; otherwise, Universal Authentication Manager will not function.
>
> For example: `reg.exe import MyRegistryFile.reg /reg:32`

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

5.2.4 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. For details on installation, see the *Oracle Enterprise Single Sign-On Suite Installation Guide*.

5.2.5 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 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 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
    ```

    > **Note:**   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**.

    > **Note:**   The Console produces a `.REG` file compatible only with 32-bit systems. If you are merging the `.REG` file on a 64-bit system, you must run the following command to move the merged registry data to the correct location within the registry (otherwise, Universal Authentication Manager will not function):
    >
    > ```
    > reg.exe COPY HKLM\Software\Passlogix
    > HKLM\Software\Wow6432Node\Passlogix /s
    > ```

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

5.2.6 Integrating with Kiosk Manager

Universal Authentication Manager can be used as an authentication mechanism for locking and unlocking Kiosk Manager sessions in kiosk environments.

The steps in this procedure outline only the minimal configuration required to integrate Universal Authentication Manager with Kiosk Manager; your environment might require a more comprehensive configuration of Kiosk Manager.

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 Installation Guide*. When configuring Kiosk Manager, you must follow instructions for strong authentication environments, as Universal Authentication Manager is a strong authentication application.

2. Install Universal Authentication Manager as described in the *Oracle Enterprise Single Sign-On Suite Installation Guide*.

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 Microsoft Active Directory.

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 Administrative Console.

  b. Navigate to **Global Agent Settings** > *[TargetSettingsSet]* > **Kiosk Manager**.

  c. In the Cached Credentials section, select the check box next to the **Use Cached Credentials** option and select **No** from the drop-down menu.

  d. 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.

  e. Select the check box next to the **Prepopulate on Startup** option and select **Always** from the drop-down menu.

  f. (Optional) If you do not 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 Manager to 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. In the left hand tree, expand the **Kiosk Manager** (top level, not under **Global Agent Settings**) node.

Configure the action and session state for the "KM Session Locked" event:

  a. Select the **Session States** sub-node.

  b. Click **Add** and enter KMS_Locked as the name.

  c. Select the **Events** tab.

  d. Uncheck the **Session End** event.

  e. Check the **Session Locked** event.

  f. Select the **Authenticators** tab.

  g. Check the **Universal Authentication Manager authenticator** and all its individual adapters.

    h. Select the **Actions** tab.

    i. Click **Add**.

    j. Enter KMA_Locked as the name, select the **Run List** option, and click **OK**.

    k. 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

5. Configure the action and session state for the KM Before Session Unlocked event:

    a. Select the **Session States** sub-node.

    b. Click **Add** and enter KMS_IsUnlocking as the name.

    c. Select the **Events** tab.

    d. Uncheck the **Session End** event.

    e. Check the **Before Session Unlocked** event.

    f. Select the **Authenticators** tab.

    g. Check the **Universal Authentication Manager authenticator** and all its individual adapters.

    h. Select the **Actions** tab.

    i. Click **Add**.

    j. Enter KMA_IsUnlocking as the name, select the **Run List** option, and click **OK**.

    k. 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

6. Publish your changes to the repository.

5.3 Working with Universal Authentication Manager Policies

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

- Creating a Policy
- Configuring a Policy
- Publishing a Policy
- Modifying an Existing Policy
- Deleting a Policy

5.3.1 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 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.

5.3.1.1 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**.

5.3.1.1.1 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 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.

5.3.1.1.2 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.

5.3.2 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 Administrative Console. The 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.

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 a Proximity Card Policy

- Configuring a Smart Card Policy

- Configuring a Challenge Questions Policy

- Configuring a Windows Password Policy

> **Note:** 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.

5.3.2.1 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.

5.3.2.1.1   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.
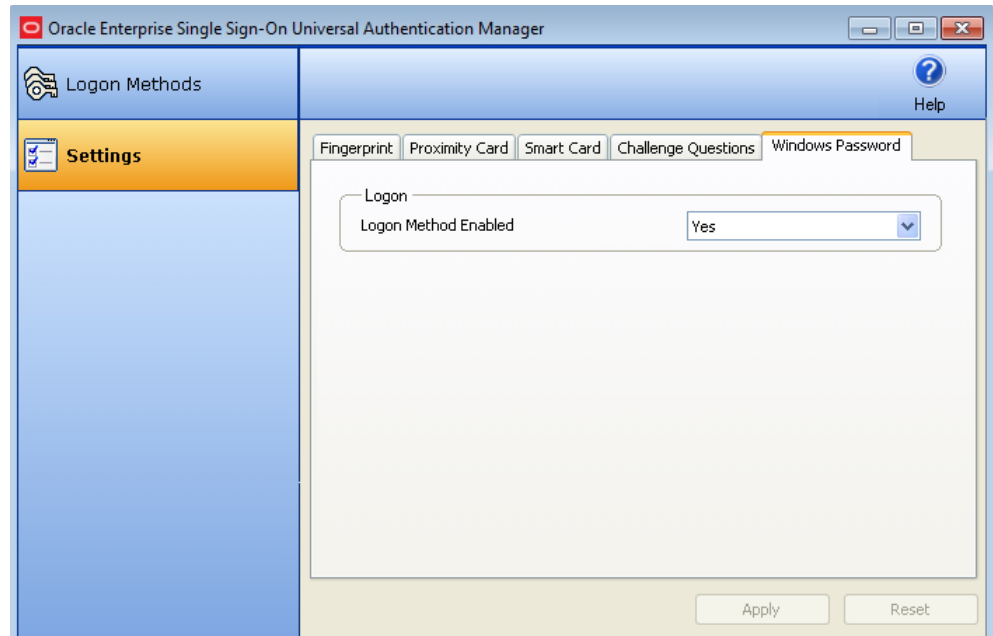
5.3.2.1.2   Windows Password Exception Universal Authentication Manager automatically enables Windows Password authentication if no other logon methods are enrolled.

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.

> **WARNING:**   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 Administrative Console.

5.3.2.1.3   Logon Method Enabled Policy Prerequisites Before you publish the Logon Method Enabled policy:

■   You must install the 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 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.

5.3.2.1.4 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.

5.3.2.2 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.

> **Note:** 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 Administrative Console.

> **Note:** 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.

5.3.2.2.1 Configuring the Enrollment Prompt Policy Before you publish the Enrollment Prompt policy:

- You must install the 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 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.

   Universal Authentication Manager applies the policy during the next synchronization with the repository.

5.3.2.3 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 Administrative Console.

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

> **Note:** 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.

5.3.2.3.1 Configuring the Grace Period Policy Before you publish the Grace Period policy:

- You must install the 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 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.

   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.
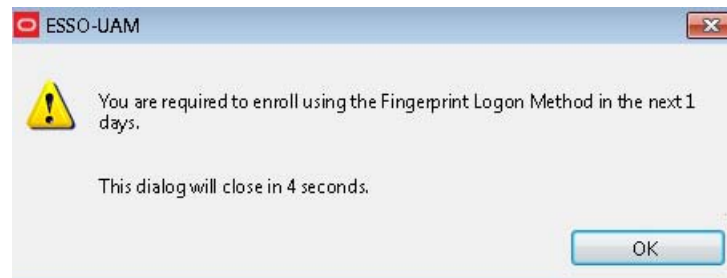
5.3.2.3.2 Conditions that Disable the Grace Period Policy The Enrollment Grace Period will not be in effect (that is, it will be disabled) if either of the following conditions exist:

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

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

5.3.2.4 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:

Control	Function
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).

Control	Function
PIN Allowed Characters	Restricts the character type(s) you can use in your PIN. Options are numeric only, alphanumeric, or any characters (default setting).

5.3.2.5 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:

Control	Function
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. Note: 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

Control	Function
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 either 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

5.3.2.6 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:

Control	Function
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.
	Note: 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

Control	Function
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 either 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).

5.3.2.7 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.

> **Note:** 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:

Control	Function
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 either 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.

5.3.2.8 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.

Control	Function
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.

5.3.3 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:

■ Assign the desired users and/or groups to the target policy.

■ Publish the policy to the repository.

5.3.4 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.

> **WARNING:** 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.**
>
> ■ **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 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.
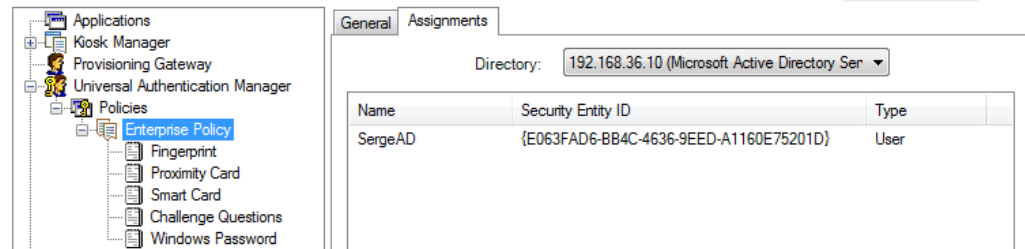
6. Repeat step 5 for any additional users or groups you want to assign to the policy.

7. Publish the policy to the repository.

5.3.5 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 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**.
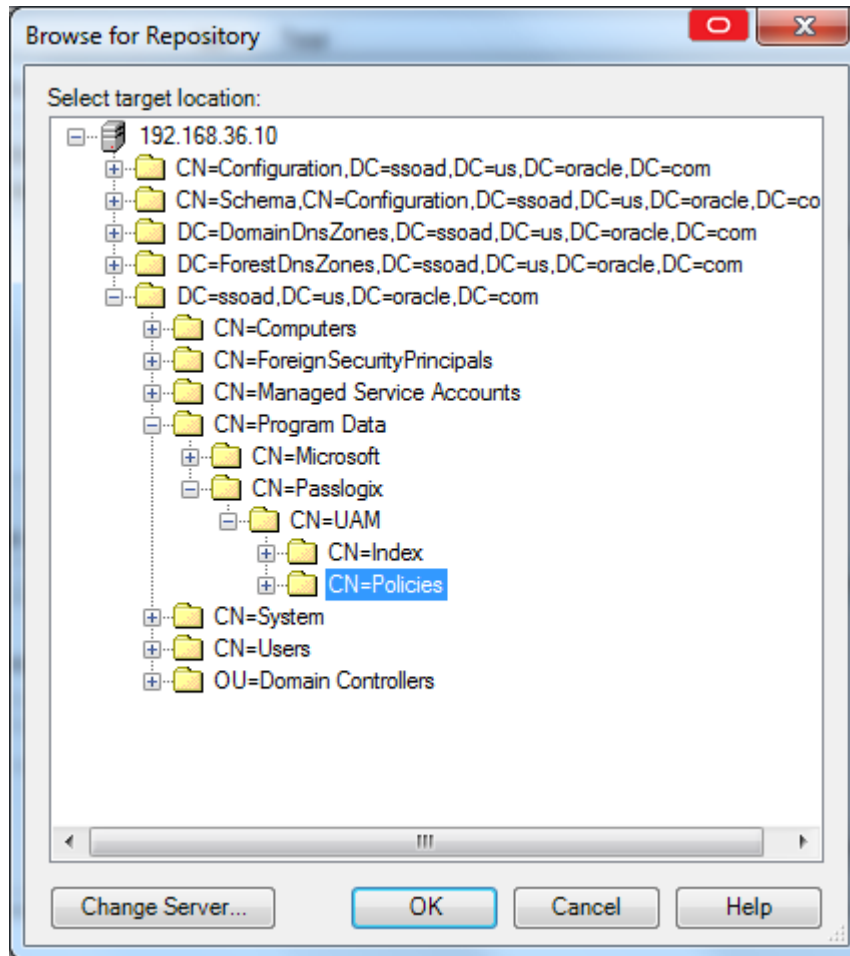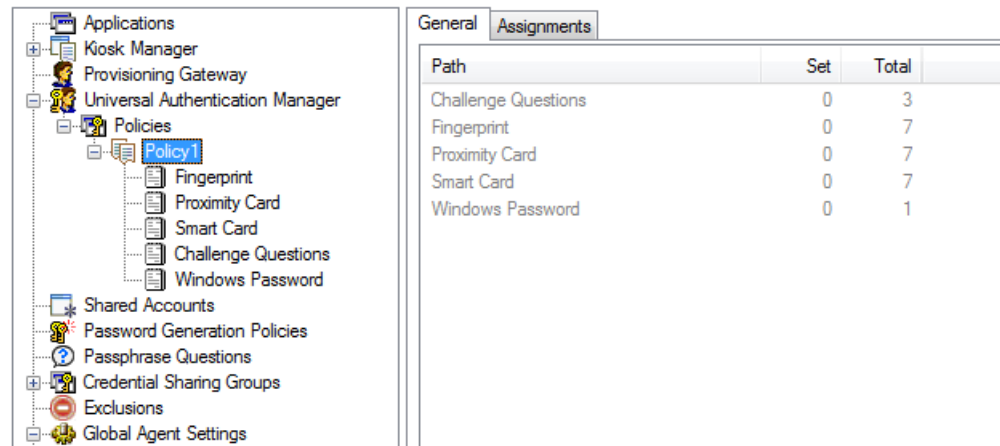
e. Click **Publish**.

5.3.6 Modifying an Existing Policy

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

1. Launch the 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 publish the updated policy object to the repository in place of the old one as described in Publishing a Policy.

5.3.7 Deleting a Policy

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

1. Launch the 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.

6

Using the Administrative Console to Configure the Reporting Client

Using the Administrative Console, you can configure the Reporting client to generate reports for every type of event that might occur in the course of regular business operation. Using Oracle Business Intelligence (BI) Publisher, you can output reports, with a selection of a variety of formats to suit your needs. This section describes the steps to install and configure the Reporting client and database, and to leverage BI Publisher to create reports for enterprise single sign-on events.

This section covers the following:

- Installing the Administrative Console and Reporting Client
- Installing the Reporting Extension
- Setting Up the Reporting Service as a Domain User
- Oracle Database Configuration Overview
- Setting Up the Oracle Database for Reporting
- Microsoft SQL Server Configuration Overview
- Using Oracle Business Intelligence Publisher for Deployment with Reporting

For complete instructions to install and configure Oracle Enterprise Single Sign-On Suite, refer to the *Oracle Enterprise Single Sign-On Suite Installation Guide*.

Also see the Reference section of this guide for Chapter 7.4.1, "Reporting Event Definition Table,".

6.1 Installing the Administrative Console and Reporting Client

If you have not already done so, download and install the Administrative Console and Logon Manager Agent. The Reporting Extension is installed as an option during the Agent installation and configured within the Administrative Console.

6.2 Installing the Reporting Extension

You install the Reporting extension on Client workstations during the Logon Manager Agent installation. After starting the InstallShield Wizard:

1. On the Setup Type panel, select a **Custom Setup**.

2. On the Custom Setup panel, expand **Audit Logging Methods**.

3. Select **Reporting Server** and set it to install.

4. Follow the on-screen instructions to complete the installation.
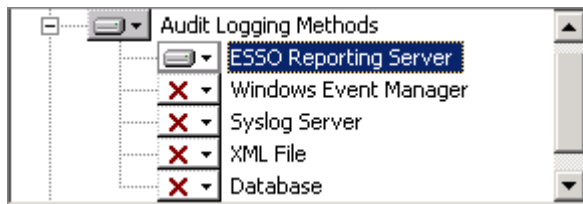
> **Note:** Refer to the *Oracle Enterprise Single Sign-On Suite Installation Guide* for specific instructions.

6.2.1 Configuring Reporting Settings

To configure Logon Manager to begin capturing events, you must adjust some settings in the Administrative Console.

1. Open the Administrative Console by pointing to **Start** > **Programs** > **Oracle** > **ESSO-LM Administrative Console**.

2. Select a set of Global Agent Settings (or right-click **Global Agent Settings**, point to **Import**, click **From Live HKLM**, expand **Live**).

3. Expand **Audit Logging** and select **Reporting Server**. Configure the following settings:

- **Connection string**: Enter the database connection string in OLE DB format. The machine must be within the domain. For example:

  ```
  Provider=SQLOLEDB.1;Integrated Security=SSPI;PersistSecurity
  Info=False;Initial Catalog=Database_Name;Data Source=database_server
  ```

- **Stored procedure**: The name of the stored procedure in the database. When encoded events are sent to the database, the stored procedure is called to decode the XML file and store the events in the database. Set this to `dbo.sp_WriteEvents`.

- **Batch size**: Defines the group size of events to be sent to the database Stored Procedure at one time. For example, if you have 1000 events in the Reporting Service cache and the Batch Size is 100, you will have 10 database Stored Procedure calls. (Default is `100`.)

- **Cache limit**: Maximum number of reporting events to be cached. Once this number is reached, the oldest events are discarded. For example, if the batch

size is 100, and an end-user's system cannot connect to the reporting service, it will keep logging events. Once it gets to 1000, the oldest events will be discarded. (Default is `1000`.)

- **Retry interval**: Defines timeout in minutes between sequential operations of the Reporting Service Cache offloading events to the database. An interval is necessary to reduce database connection load. (Default is `30`.) Retry Interval should be set to `0` when Reporting is used.

4. Export the settings to the Logon Manager Agent. For information on exporting Global Agent Settings, refer to the Logon Manager documentation.

6.3 Setting Up the Reporting Service as a Domain User

You can make the Reporting Server a domain user by assigning it the same privileges as the Domain Computers group. This eliminates having the Domain Computers group connect to the database and, when using an Oracle Database, also eliminates the need to specify a clear text username and password.

Note: It is strongly recommended that you select **Password never expires** for user accounts that are used to log on as a service.

6.3.1 Overview of the Process to Set Up Reporting as a Domain User

This process consists of the following steps:

1. Creating the domain user account:

   - For Oracle, create the account that connects to the Oracle Database.

     or

   - For Microsoft SQL, create a domain user with the same rights to the SQL database as you would give the Domain Computers group.

2. Granting the Reporting Service domain user the "Log on as a service" privilege.

3. Running the Reporting Service as the domain user account you created. (For instance, run the `sc config` command on all workstations.)

For detailed instructions to set up your database for Windows integrated authentication, refer to the following sections:

- Setting Up Oracle Database to Use Reporting with Windows Integrated Authentication

- Setting Up Microsoft SQL Server to Use Reporting with Windows Integrated Authentication

Next Steps

After you configure Logon Manager to capture events and store them in the database, do one of the following:

- For Oracle Database, continue to Oracle Database Configuration Overview.

- For SQL databases, continue to Microsoft SQL Server Configuration Overview.

6.4 Oracle Database Configuration Overview

The following is a brief overview of the procedures that you must follow in order to successfully configure the Oracle Database to work with Reporting.

- Creating the Oracle Database User
- Creating the Database Table and Setting Up Stored Procedures
- Creating a Connection String
- Configuring Oracle Database on Client Machines
- Setting Up Oracle Database to Use Reporting with Windows Integrated Authentication
- Next Steps

6.4.1 Creating the Oracle Database User

You must create one user and grant the appropriate privileges to the account. This user will be the SSO Database table owner.

Launch the database in which you want to create the user and enter the following command in the SQL*Plus tool:

```
SQL> CREATE USER username IDENTIFIED BY password DEFAULT TABLESPACE user_
tablespace TEMPORARY TABLESPACE temp_tablespace;
```

where *user_tablespace* is the default tablespace identified by the database administrator to store user objects, and *temp_tablespace* is identified to store temporary objects.

For example:

1. Start SQL*Plus (the Oracle SQL command line tool), and enter the following commands to log in:

   ```
   $ sqlplus
   ```

2. Press **Enter**.

3. Enter user-name:

   ```
   username/password@dbname
   ```

   where *username* is an existing administrative user in the database. For example, `system/password` will log the administrative user `system` with a password of `password` into the default database.

4. Create the user, grant these two default roles and their corresponding default privileges to the user that you created, and log out of the SQL command line tool:

   ```
   SQL> CREATE USER orauser IDENTIFIED BY oracle DEFAULT TABLESPACE USERS
   TEMPORARY TABLESPACE TEMP;
   SQL> GRANT CONNECT, RESOURCE, CREATE ANY DIRECTORY, CREATE PROCEDURE TO
   orauser;
   SQL> EXIT
   ```

6.4.2 Creating the Database Table and Setting Up Stored Procedures

After you create the Oracle Database User, run the provided script, `Oracle_Setup.sql`, to:

- Upgrade an existing or create a new database table.

- Upgrade existing or set up new stored procedures.

The script might require some modification with respect to the location of the `StoredProcedures.java` file, which is initially set to `D:\orcl_scripts`. If you plan to use a different location, refer to the script's comment header for the exact line number where you can make this change.

When you have updated the `StoredProcedures.java` location (if necessary), you are ready to execute the following script using SQL*Plus (the Oracle SQL command line tool) to accomplish the remaining tasks:

```
$ sqlplus username/user_password < path_to_file\Oracle_Setup.sql
```

where *username* is `orauser`, *user_password* is `oracle`, and *path_to_file* is the path to the SQL script file.

For example:

```
$ sqlplus orauser/oracle < Oracle_Setup.sql
```

or:

```
C:\>sqlplus orauser/oracle < C:\oracle_setup\Oracle_Setup.sql
```

6.4.3 Creating a Connection String

In this section, you will create a connection string that will be used in the following section, Configuring the Oracle Database on Client Machines.

1. Open Windows Explorer and navigate to the folder in which you want to store the `.udl` file.

2. From the File menu, click **New** and then click **Text Document**. A new file named `New Text Document.txt` appears in the directory.

3. Rename this file, removing all spaces and changing the file extension to `.udl`, for Universal Data Link.

4. Double-click the Universal Data Link (`.udl`) file. The Data Link Properties dialog opens.

5. On the **Provider** tab, select **Oracle Provider for OLE DB** and then click **Next**.
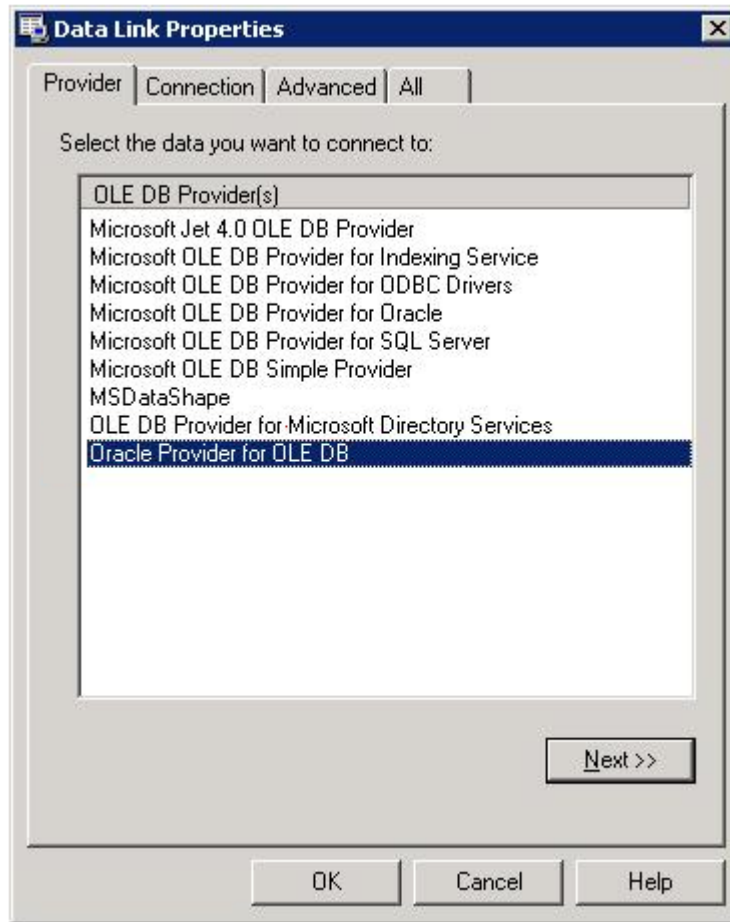
6. On the **Connection** tab, enter the Data Source, User name, and Password. Check the **Allow saving password** check box and click **Test Connection**. For example: Data Source: `ORCL`, User name: `orauser`, Password: `oracle`.
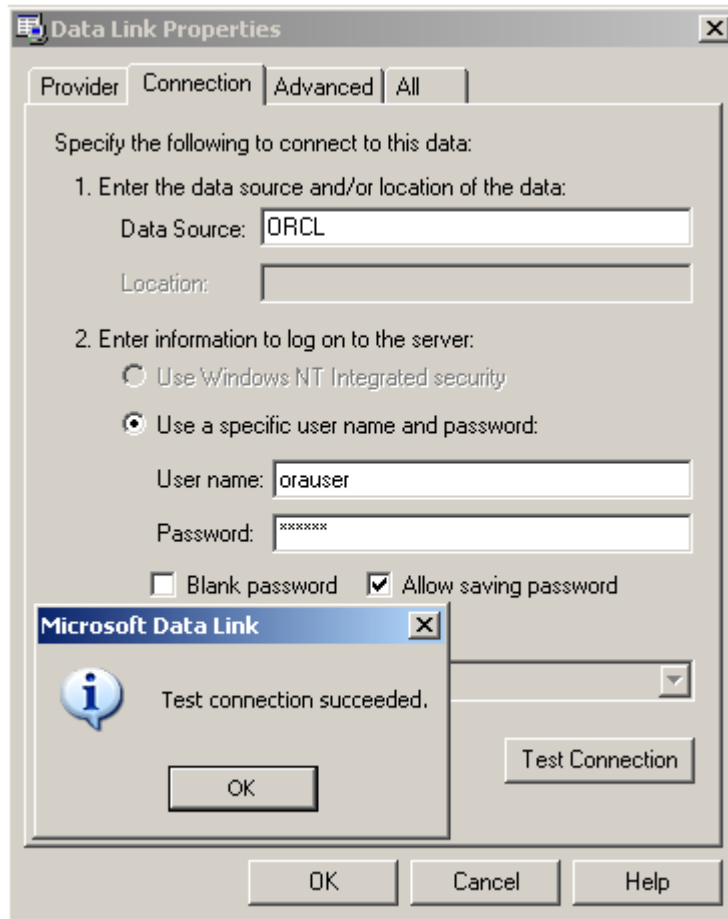
7. A message will appear indicating that the test connection succeeded. Click **OK**.

8. Click **OK** to save the connection string to the Universal Data Link (`.udl`) file.

9. Open the `.udl` file in Notepad. In the next section of this guide you will be instructed to enter a connection string. Copy and paste this string and enter it into the **Connection string** field.
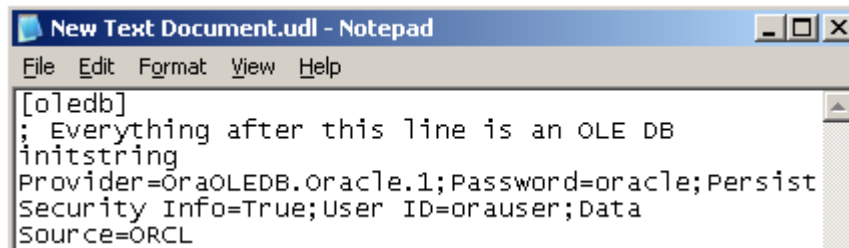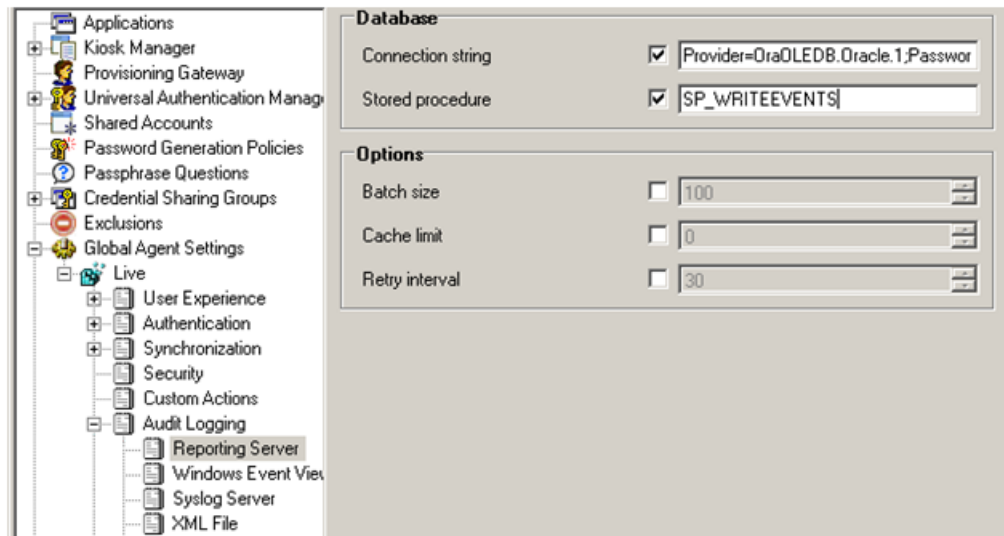
The full connection string above reads as follows:

6.4.4 Configuring Oracle Database on Client Machines

> **Note:** If you are installing Logon Manager on a 64-bit system and plan to configure the Reporting Service to store event data in an Oracle Database, you must install the 32-bit version of the Oracle Database client on the target end-user machine; otherwise, the Reporting Service will not be able to connect to the Oracle Database.

1. Install either Oracle Client with Oracle Provider for OLE DB or Oracle Data Access Components for Oracle Client.

or
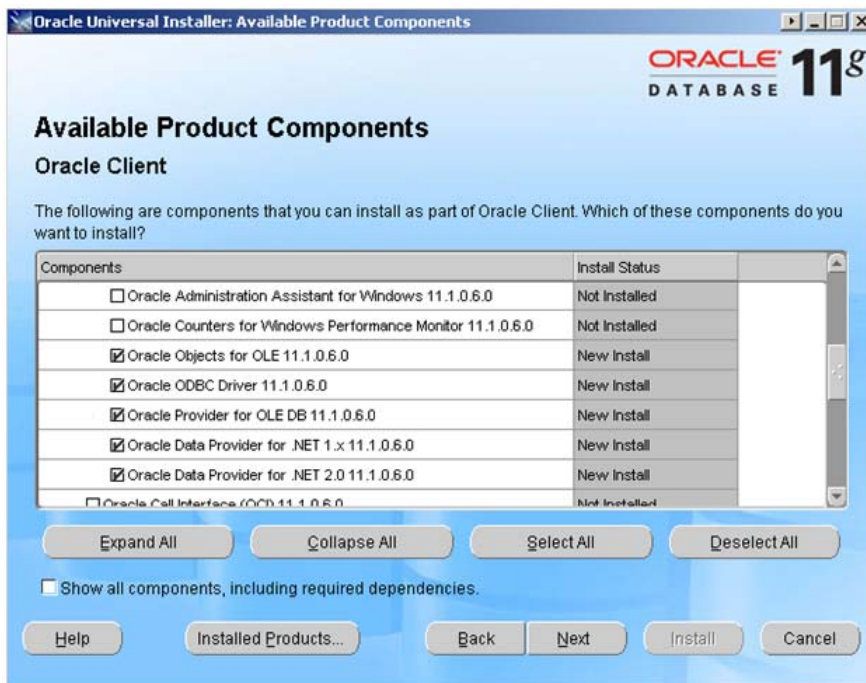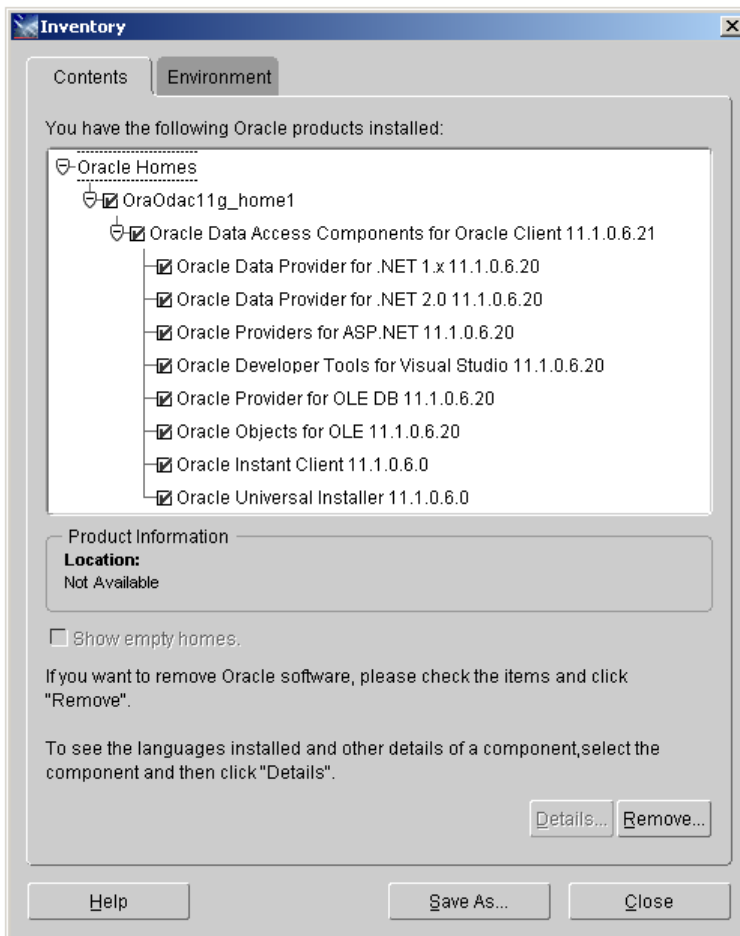
2. Next, configure the Oracle Client for connection to the Oracle Server. Edit or create the following file:

```
<Oracle_Home\client_1\Network\Admin\tnsnames.ora:
"# tnsnames.ora: Network Configuration File:
C:\oracle\product\11.1.0\client_1\NETWORK\ADMIN\tnsnames.ora
# Generated by Oracle configuration tools.

ORCL =
(DESCRIPTION =
 (ADDRESS_LIST =
 (ADDRESS = (PROTOCOL = TCP)(HOST = oracle_host_server_name)(PORT = 1521))
 )
 (CONNECT_DATA =(SERVICE_NAME = ORCL)))
```
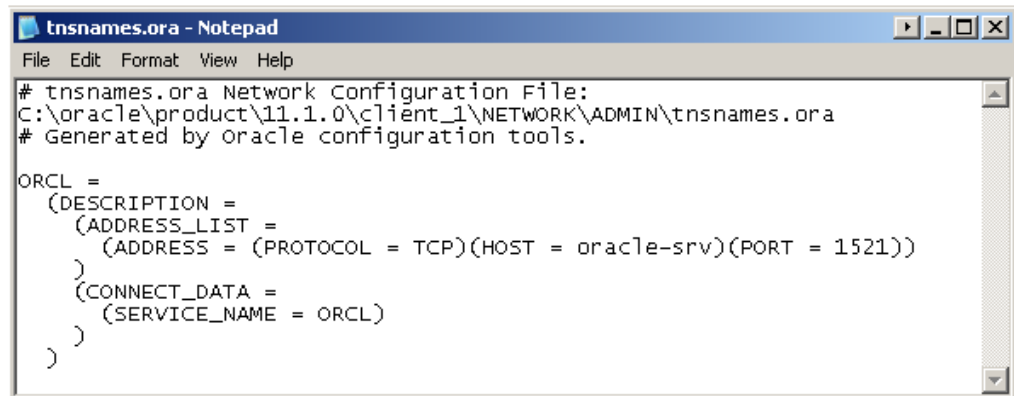

3. Launch the Administrative Console by clicking **Start** > **Programs** > **Oracle** > **Administrative Console**.

4. In the tree, right-click **Global Agent Settings**, click **Import**, then click **From live HKLM**.

5. Under **Global Agent Settings** > **Live**, expand **Audit Logging** > **Reporting Server**.

6. Copy and paste the string you created in the previous section, Creating a Connection String. For example:

```
"Provider=OraOLEDB.Oracle.1;Password=password;Persist Security Info=True;User
ID=user_name;Data Source=ORCL"
```

7. Set the Stored Procedure setting to:

```
"SP_WRITEEVENTS"
```
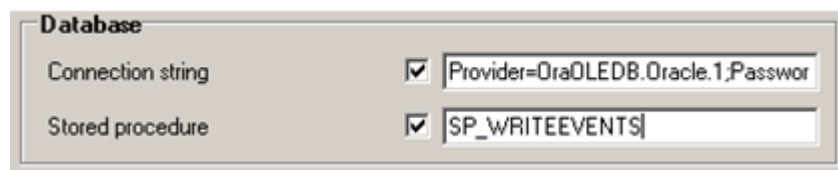

8. Right-click **Live** and click **Write to Live HKLM**.

9. Close the Administrative Console.

6.4.5 Setting Up Oracle Database to Use Reporting with Windows Integrated Authentication

To use Windows integrated authentication with Reporting, the ESSO Reporting Service must run as a domain user with permissions to write to the Reporting database (either Microsoft SQL Server or Oracle). To run the service as domain user on a workstation, the user must have "Log on as Service" permissions.

You can modify this setting (as detailed below) on your domain controller so that the setting is published to all client computers.

6.4.5.1 Creating an Active Directory domain user that will write events to the database

Create a user in Active Directory (henceforth referred to as the "Reporting Domain User"). You will grant this user permissions to write Reporting events to the database.

6.4.5.2 Modifying the Default domain policy to allow the Reporting Domain User to Log on as a service

Modify the Default domain policy on your domain controller so that all client computers connected to the domain have this setting defined.

> **Note:**   Oracle recommends that you create a backup of the current Group Policy before editing the default domain policy. To create a backup, in the console tree, open `Domains/Current Domain Name/Group Policy` objects. Right-click **Default Domain Policy**, and select **Back Up** from the context menu.
>
> The Group Policy is domain-wide and overwrites the local policy. If you need to configure any local accounts to log on as a service, refer to the documentation for the Group Policy Management Console for this procedure.

---

1. On your domain controller, click **Start**, click **Run**, enter `gpmc.msc`, and then click **OK**.

2. In the console tree, open **Domains** > **Current Domain Name** > **Group Policy Objects**. Right-click **Default Domain Policy**, and select **Edit** from the context menu.

3. In the Group Policy Management Editor's console tree, go to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Local Policies** > **User Rights Assignment**.

4. In the details pane, double-click **Log on as a service**.

5. Verify that the **Define this policy setting** check box is selected, and click **Add User or Group**. Enter the new Reporting Domain User in the **User and group names** field.

6. Click **OK** when finished.

To apply the Group Policy change immediately:

- Restart the domain controller.

  or

- Open a command prompt, and type: `gpupdate /force`. Then press **Enter**.

6.4.5.3 Verifying Publication of the Active Directory Permission on the Client Machine

---

Note: Also see Microsoft's technical note about modifying permissions on an Active Directory domain or local computer to allow a domain user to log on as a service.

---

1. Ensure that the client is updated by opening a command prompt and entering the `gpupdate /force` command. For a discussion of this procedure, see the Microsoft Technical Library article at
   http://technet.microsoft.com/en-us/library/cc778890%28v=ws.10%29.aspx

2. Go to **Administrator Tools** > **Local Security Policy**.

3. In Local Security Policy go to **Security Settings** > **Local Policies** > **User Rights Assignment** (as shown in the following figure).

4. In the Detail Panel check for the updated "Log on as a service" policy. It should include the Reporting Domain User among the users who have this permission.
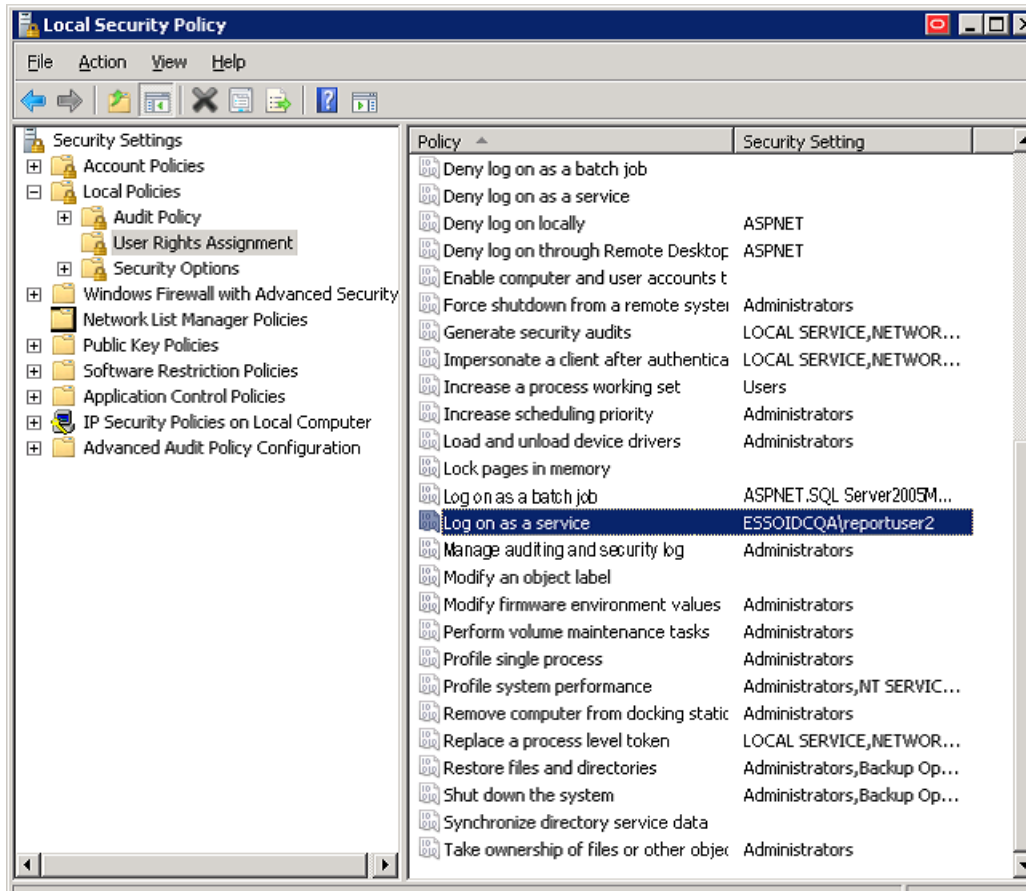
6.4.5.4 Configuring the ESSO Reporting Service on the Client Machine to run as this domain user

Perform these steps on all client computers where the ESSO Reporting Service is running.

To configure the ESSO Reporting Service to run under the Reporting Domain User account:

1. Open a command prompt and enter the following command:

   ```
   sc config "SSO Reporting Service" obj= "Domain\User" password= "password"
   ```

2. Press **Enter**.

   This command should return the following output:

   ```
   [SC] ChangeServiceConfig SUCCESS
   ```

3. Restart the ESSO Reporting Service:

   a. Open a command prompt and enter the following command:

   ```
   net stop "SSO Reporting Service" && net start "SSO Reporting Service"
   ```

   b. Press **Enter**.

   This command should return the following output:

   ```
   The ESSO Reporting Service service is stopping.
   The ESSO Reporting Service service was stopped successfully.
   The ESSO Reporting Service service is starting.
   ```

```
The ESSO Reporting Service service was started successfully.
```

> **Note:** You can achieve the same results through the user interface by accessing the "Services" console on any client computer.

6.4.6 Setting Up the Server for Integrated Authentication

Perform the following tasks to set up the server for integrated authentication.

6.4.6.1 Verify the Windows Authentication Protocol

Ensure that the `SQLNET.AUTHENTICATION_SERVICES` entry in the `sqlnet.ora` file reads `NTS`. This setting must be modified on both the client and database server. You must edit or create the `sqlnet.ora` file. The file is located at:

`ORACLE_BASE\ORACLE_HOME\network\admin\sqlnet.ora`

> **Note:** Refer to the *Oracle Database Platform Guide* on Windows Authentication Protocols, User Authentication and more information.

6.4.6.2 Create the External Oracle User for the Domain User

You must create the new "Reporting Domain User" as "identified externally" on the Oracle Database and grant appropriate privileges to the account.

> **Note:** Refer to the *Oracle Database Platform Guide* for Manually Creating an External Operating System User, External user Authentication Task on the Oracle Database Server, External User Authentication Task on the Client Computer and more information.
>
> Set `OSAUTH_PREFIX_DOMAIN` to `true` in `HKEY_LOCAL_ MACHINE\SOFTWARE\ORACLE\HOMEID`, to enable authentication at domain level, where *ID* is the Oracle home directory you want to edit. For more information, refer to the External User Authentication task on the Oracle Database Server in the *Oracle Database Platform Guide*.

1. Grant Administrative privileges to the New "Reporting Domain User" (for example, `domainname\username`) on the workstation where the Oracle Database is installed or will be installed.

2. Log on to this workstation as the New Report Domain User.

3. Launch SQLPLUS and log on as `SYSDBA` at the prompt.

4. Create the "Reporting Domain User" identified externally (refer to the SQL syntax below). Grant required privileges to the user that you created, and log out of the SQL command line tool.

   Create the User with the following syntax:

   ```
   SQL> CREATE USER username IDENTIFIED EXTERNALLY DEFAULT TABLESPACE user_
   tablespace TEMPORARY TABLESPACE temp_tablespace;
   ```

   Where *user_tablespace* is the default tablespace identified by the database administrator to store user objects, and *temp_tablespace* is the location to store temporary objects.

The username would take the form OPS$DOMAINNAME/USERNAME, where:

- OPS$ is the value of OS_AUTHENT_PREFIX set for your database

- DOMAINNAME is the name of the domain

  and

- USERNAME is the Reporting User with whose permissions the Reporting service would be running.

Example

The following examples were created using Oracle Database 11g.

```
SQL> CREATE USER "OPS$ESSOIDCQA\REPORTUSER1" IDENTIFIED EXTERNALLY DEFAULT
TABLESPACE USERS TEMPORARY TABLESPACE TEMP;
User created.
SQL> GRANT CONNECT, RESOURCE, CREATE ANY DIRECTORY, CREATE PROCEDURE TO
"OPS$ESSOIDCQA\REPORTUSER1";
Grant succeeded.
SQL> EXIT
Disconnected from Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 -
Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options
C:\Users\reportuser1>
```

In the above example OPS$ is the OS_AUTHENT_PREFIX prefix value and REPORTUSER1 is the username defined on the ESSOIDCQA domain.

Grant the User CONNECT, RESOURCE, CREATE ANY DIRECTORY and CREATE PROCEDURE permissions.

The Windows Domain user ESSOIDCQA\REPORTUSER1 (that is, the Reporting Domain User) will now be able to log on to Oracle Database if this domain user is logged on to the machine and if the Windows Authentication Protocol has been set.

Perform the following steps to verify these conditions:

1. Make sure you log on to the system with the new user (here, ESSOIDCQA\REPORTUSER1).

2. Make sure you have Windows Authentication Protocol set correctly. That is, the SQLNET.AUTHENTICATION_SERVICES entry in the sqlnet.ora file reads NTS.

3. Open a command prompt and enter sqlplus /@ORCL, where ORCL is the net_ service_name defined in the tnsnames.ora file on the system.

   If configured properly, sqlplus will log the user on without prompting for a username and password. Once logged on, enter SHOW USER at the sqlplus prompt. This displays the current logged-on user.

Example

```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\reportuser1>SQLPLUS/@ORCL
SQL*Plus: Release 11.2.0.1.0 Production on Fri May 11 07:43:12 2012
Copyright (c) 1982, 2010, Oracle. All rights reserved.
Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options
SQL> SHOW USER
USER is "OPS$ESSOIDCQA\REPORTUSER1"
```

```
SQL>
```

> **Note:** You can verify the value of `OS_AUTHENT_PREFIX` set on your database with the `SHOW PARAMETER OS_AUTHENT_PREFIX` command as shown in the following example. By default it is set to `OPS$`. You can modify this value to any string you wish. For more information, refer to the *Oracle Database Platform Guide*.

```
C:\Users\reportuser1>SQLPLUS /NOLOG
SQL*Plus: Release 11.2.0.1.0 Production on Thu May 10 10:33:49 2012
Copyright (c) 1982, 2010, Oracle. All rights reserved.
SQL> CONNECT SYS AS SYSDBA
Enter password:
Connected.
SQL> SHOW PARAMETER OS_AUTHENT_PREFIX
NAME TYPE VALUE
------------------------------------ ----------- -----------------------
os_authent_prefix string OPS$
SQL>
```

6.5 Setting Up the Oracle Database for Reporting

For an existing installation of the Reporting database set up on your Oracle Database system, follow the instructions in the section, Upgrading an Existing Oracle Database Setup. For a new database installation, follow the instructions in the section, Setting Up a New Oracle Database for the ESSO Reporting Service.

6.5.1 Upgrading an Existing Oracle Database Setup

Perform the following steps to run version 11.1.2 of the Reporting Service with integrated authentication under the Reporting Domain User account.

- Upgrade the Database Tables Schema.

- Grant appropriate permissions to the new Reporting Domain User account so that it can access the required Oracle objects.

- Create Public `SYNONYM` for `SP_WRITEEVENTS`.

6.5.1.1 Upgrading an Existing Oracle Database Setup

Run the provided script, `Oracle_Setup.sql` as the SSO Database table owner.

The initial location of the `StoredProcedures.java` file is `D:\orcl_scripts`. If you plan to use a different location, refer to the script's comment header for the exact line number where you can make this change.

After updating the `StoredProcedures.java` location (if necessary), execute the following script using `SQL*Plus` (the Oracle SQL command line tool) to accomplish the remaining tasks:

`$ sqlplus username/user_password < path_to_file\Oracle_Setup.sql`

where *username* is the existing SSO Database table owner, *user_password* is that user's password, and *path_to_file* is the path to the SQL script file.

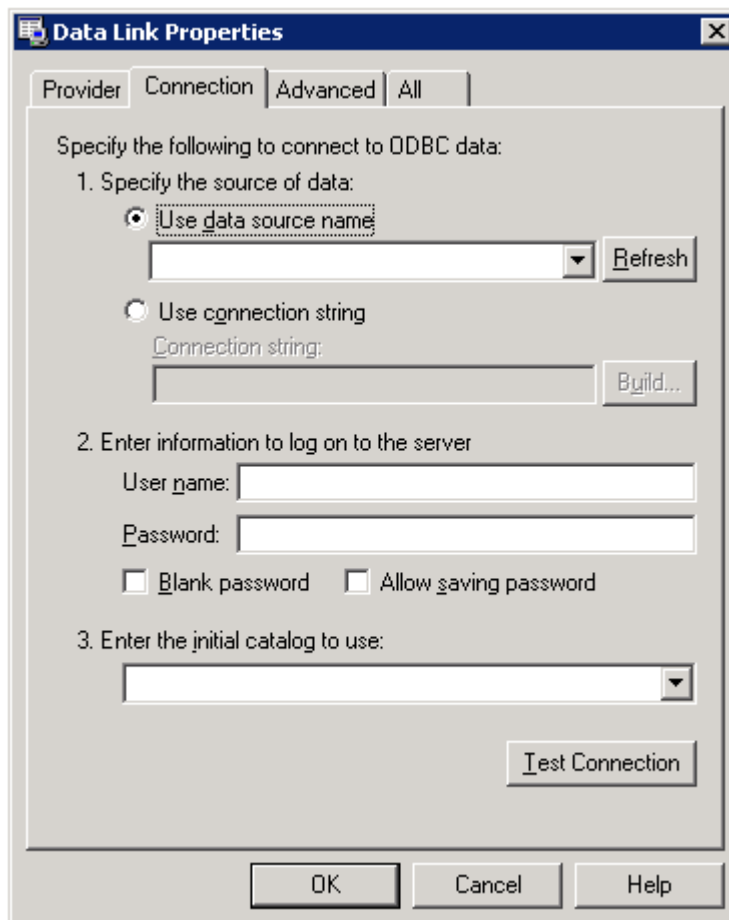Example

```
$ sqlplus orauser/oracle < Oracle_Setup.sql
```

or:

```
C:\>sqlplus orauser/oracle < C:\oracle_setup\Oracle_Setup.sql
```

6.5.1.2 Providing the Required Permissions to the New Reporting Domain User

Allow the new Reporting Domain User Execute permission on SP_WRITEEVENTS.

1. Log in to SQL*Plus with the existing `orauser` account and password. The `orauser` is the SSO Database table owner.

2. Grant the Execute permission on `SP_WRITEEVENTS` to the new Reporting Domain User, `OPS$DOMAINNAME\USERNAME`, with the following command:

   ```
   GRANT EXECUTE ON SP_WRITEEVENTS TO "username";
   ```

   The username will be in the format, `OPS$DOMAINNAME\USERNAME`, where `OPS$` is the value of `OS_AUTHENT_PREFIX` for your database, `DOMAINNAME` is the name of the domain, and `USERNAME` is the Reporting User with whose permissions the Reporting service would be running.

Example

```
C:\Users\reportuser1>SQLPLUS orauser/oracle@ORCL
SQL*Plus: Release 11.2.0.1.0 Production on Mon May 14 11:03:45 2012
Copyright (c) 1982, 2010, Oracle. All rights reserved.
Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options
SQL> SHOW USER
USER is "ORAUSER"
SQL> GRANT EXECUTE ON SP_WRITEEVENTS TO "OPS$ESSOIDCQA\REPORTUSER1";
Grant succeeded.
SQL> QUIT
Disconnected from Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 -
Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options
```

6.5.1.3 Creating a Public Synonym for SP_WRITEEVENTS

To create a public synonym, log on to SQL*Plus as SYSDBA and create a public synonym for `SP_WRITEEVENTS` using the following syntax:

```
CREATE OR REPLACE PUBLIC SYNONYM SP_WRITEEVENTS FOR USERNAME.SP_WRITEEVENTS;
```

Where `USERNAME` is the SSO Database table owner and the account whose permissions you used during your initial setup of Oracle Database for Reporting.

Example

```
C:\Users\reportuser1>SQLPLUS /NOLOG
SQL*Plus: Release 11.2.0.1.0 Production on Mon May 14 11:15:35 2012
Copyright (c) 1982, 2010, Oracle. All rights reserved.
SQL> CONNECT SYS AS SYSDBA
Enter password:
Connected.
SQL> CREATE OR REPLACE PUBLIC SYNONYM SP_WRITEEVENTS FOR ORAUSER.SP_WRITEEVENTS;
Synonym created.
SQL> QUIT
```

```
Disconnected from Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 -
Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options
```

> **Note:** For more information on Creating Synonyms, refer to the Oracle Database SQL Language Reference.

6.5.2 Setting Up a New Oracle Database for the ESSO Reporting Service

After you create the Reporting Domain User Identified Externally on the Oracle Database, run the provided script, `Oracle_Setup.sql` to:

- Create a new Database table.

- Set up required functions, and so forth.

Run `Oracle_Setup.sql` with integrated authentication of the new Reporting Domain User. After you run this script, this user becomes the ESSO Database table owner.

The initial location of the `StoredProcedures.java` file is `D:\orcl_scripts`. If you plan to use a different location, refer to the script's comment header for the exact line number where you can make this change.

After updating the `StoredProcedures.java` location (if necessary), execute the following script using SQL*Plus (the Oracle SQL command line tool) to accomplish the remaining tasks:

```
sqlplus / < path_to_file\Oracle_Setup.sql
```

where *path_to_file* is the path to the SQL script file.

> **Note:** Make sure you log on to the system as the Reporting Domain User. You will not need to enter a username or password to SQL*Plus when you provide the forward slash ("/") at the prompt. The current user is logged on automatically to the Oracle Database machine with the appropriate permissions.

Example to run the script

```
C:\Users\reportuser1>sqlplus / < C:\oracle_setup\Oracle\Oracle_Setup.sql
```

6.5.3 Creating the Connection String for Integrated Login

Use a `.udl` file to create a connection string for the integrated Login User as you would for any other Oracle Database user. For the Integrated Login User, do not specify any username or password. Enter the user name as "/" and test the connection.

> **Note:** Make sure you are logged on to the system as the Report Domain User who has been identified in Oracle Database as an external user, and that the `sqlnet.ora` file has `AUTHENTICATION_ SERVICES` set to `NTS`.
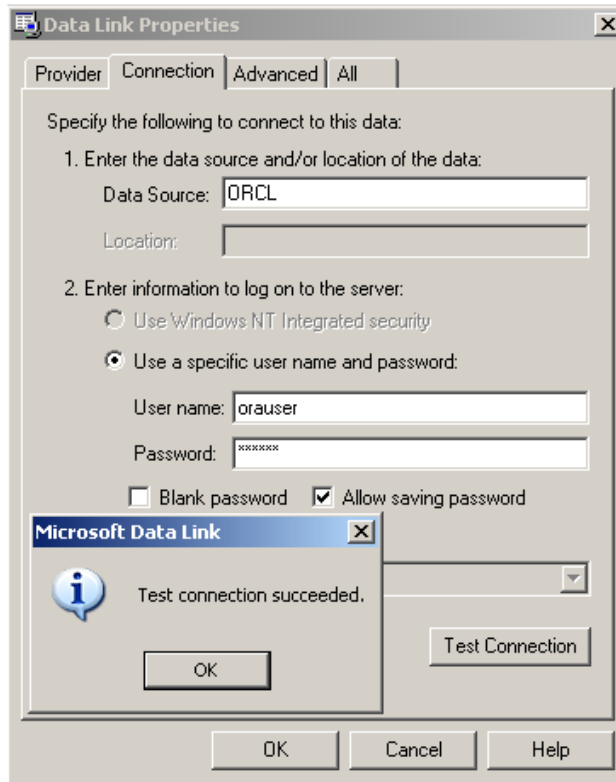
The connection string will read as follows:

```
Provider=OraOLEDB.Oracle.1;Persist Security Info=False;User ID=/;Data Source=ORCL
```

6.5.4 Configuring the Oracle Database on Client Machines

Refer to the section on Configuring the Oracle Client and Server for this procedure.

Ensure that the SQLNET.AUTHENTICATION_SERVICES parameter in the sqlnet.ora file is set to NTS on both the client and the server.

Also see the *Oracle Database Platform Guide* for more information on External User Authentication Task on the Client Computer and more.

> **WARNING:** It is important to keep in mind that using a database for reporting will result in having a number of connections equal to the number of active users. This will have a substantial impact on memory requirements (for performance) and storage requirements (for data logged).

6.5.5 Next Steps

After you configure the Agent to report events and the database to store them, you must configure BI Publisher to locate them for publication. Continue to Configuring Oracle Business Intelligence Publisher.

6.6 Microsoft SQL Server Configuration Overview

The following is a brief overview of the procedures that you must follow in order to successfully configure the SQL database to work with Reporting:

- Creating the Database Table and Setting Up Stored Procedures
- Creating the Reporting Database User
- Setting Permissions to Log On to the Reporting Administrative Console
- Setting Up a Domain Computers as a SQL User
- Enabling TCP/IP Protocol
- Next Steps

6.6.1 Creating the Database Table and Setting Up Stored Procedures

The following procedure creates a database table and stored procedures for a SQL Server database. You must perform these steps for both upgrades and new installations.

1. Open SQL Server 2005 or 2008. Click **All Programs** > **Microsoft SQL Server 2005** (or 2008) > **SQL Server Management Studio**.

2. Connect to the Database using Windows authentication, which should be the default.

3. On the left pane, navigate to **Databases**.

4. Right-click on **Databases** and select **New Database**. The New Database dialog opens.
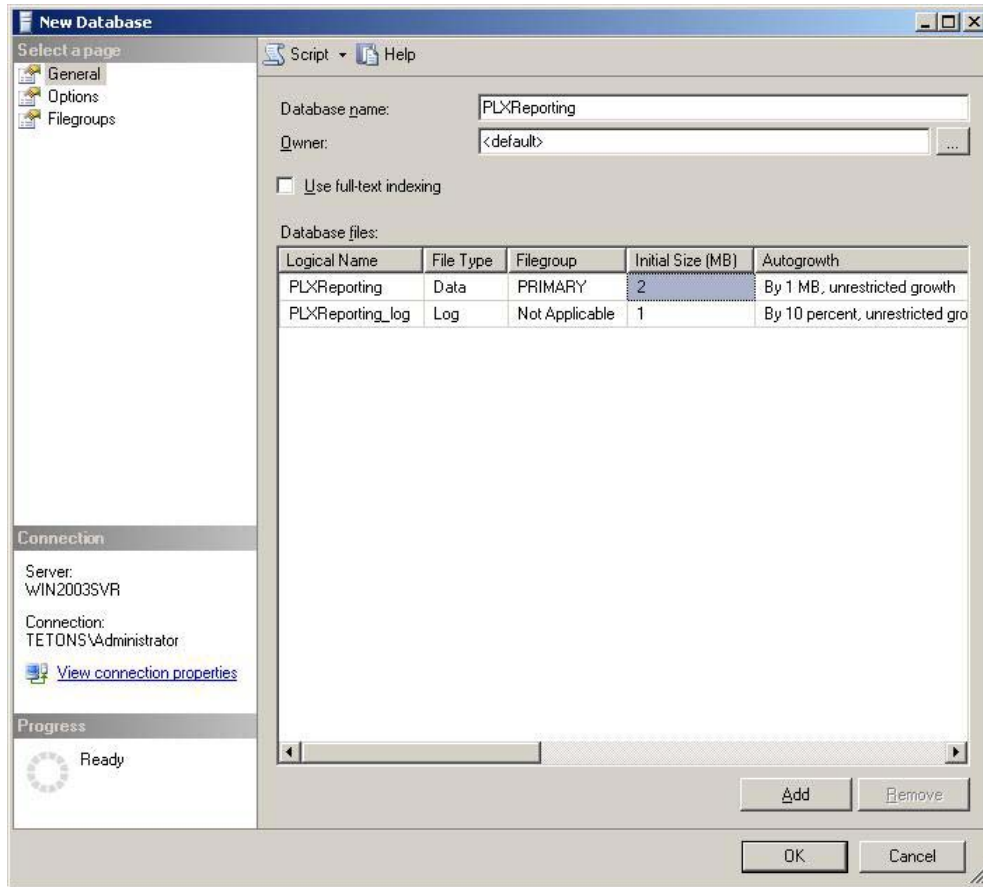
5. Enter a Database name, for example PLXReporting, and click **OK**. You should now see a PLXReporting database under Databases.

> **Note:** The database can have any name as long as the name is consistent in the queries and stored procedures.

6. Right-click on **PLXReporting** and select **New Query**.

7. Execute the following script on the SQL Server to instruct the database where to put the ESSO.Reporting.MSSQL.Decoding.dll:

- For SQL Server 2005:

```
DECLARE @AssemblyPath nvarchar(1024)
SELECT @AssemblyPath = REPLACE(physical_name,
'Microsoft SQL Server\MSSQL.1\MSSQL\DATA\master.mdf',
'Microsoft SQL Server\MSSQL.1\CLR\')
FROM master.sys.database_files WHERE name = 'master';
SELECT @AssemblyPath
```

- For SQL Server 2008 R2:

```
DECLARE @AssemblyPath nvarchar(1024)
SELECT @AssemblyPath = REPLACE(physical_name,
'Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\DATA\master.mdf',
'Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\CLR\')
FROM master.sys.database_files WHERE name = 'master';
SELECT @AssemblyPath
```

> **Note:** The result of this query provides the correct path for the file `ESSO.Reporting.MSSQL.Decoding.dll`. After receiving this information, create the folder where this file will be placed:
>
> 1. Browse to the path that resulted from the query above.
> 2. Create a folder named `CLR`.
> 3. Place `ESSO.Reporting.MSSQL.Decoding.dll` in this folder.

8. Open the `MSSQL_Setup.sql` file located in the Reporting package. Copy the contents of the file into the New Query panel.

> **Note:** The database name after the `Use` statement in the query must match the database name entered in Step 5 above.

9. Click **Execute**, which is located above the workspace pane. Upon completion, a success message appears in the bottom right pane.

   You have completed creation of the Database table `dbo.tblEventsLog`, under **PLXReporting - Tables**, and the stored procedures.
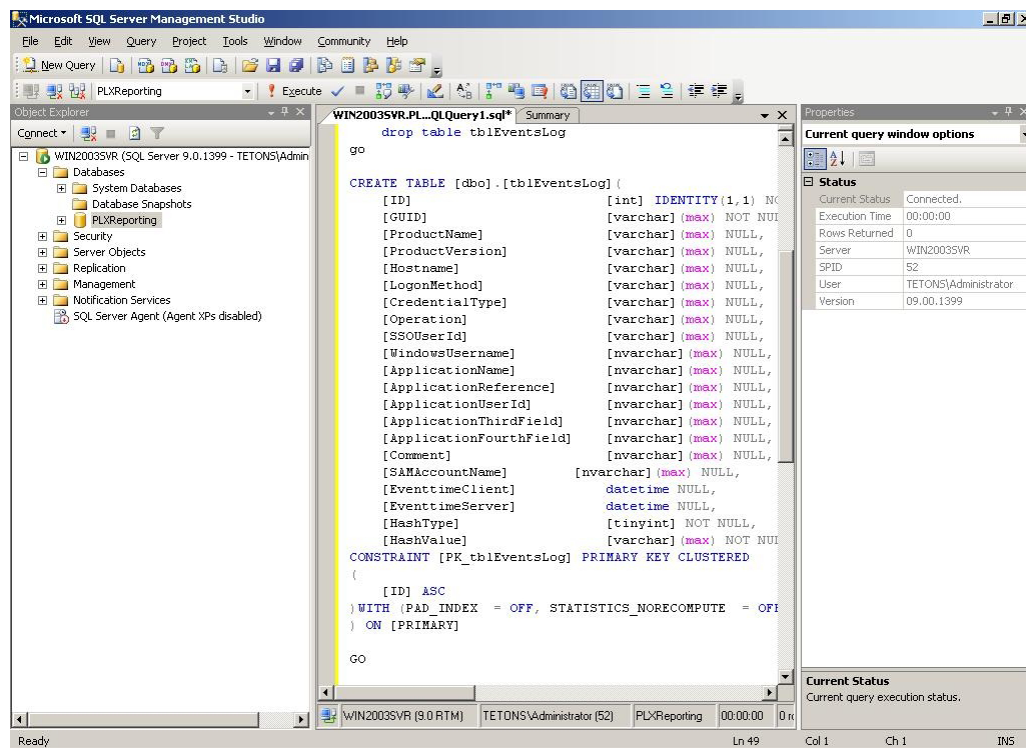
6.6.2 Creating the Reporting Database User

To create the Reporting database user:

1. In the SQL Server Management Studio left pane, expand the top node (server name), then navigate to **Security** > **Logins**.

2. Right-click on **Logins** and select **New Login**.

3. On the New Login dialog:

   a. Select **SQL Server Authentication**.

   b. Enter your login name and password.

   c. Unselect **User must change password and next login**.

   d. Select **User Mapping** in the left pane.

   e. Select the Reporting database (in this case, PLXReporting).

   f. Ensure all server roles except **public** are unchecked.

   g. Enable db_datareader, and db_datawriter.

4. Click **OK**.

6.6.3 Setting Up the Domain Computer

The following steps configure the Reporting Service to connect to the database.

1. In the SQL Server Management Studio left pane, expand the top node (server name), then navigate to **Security** > **Logins**.

2. Right-click on **Logins** and select **New Login**.
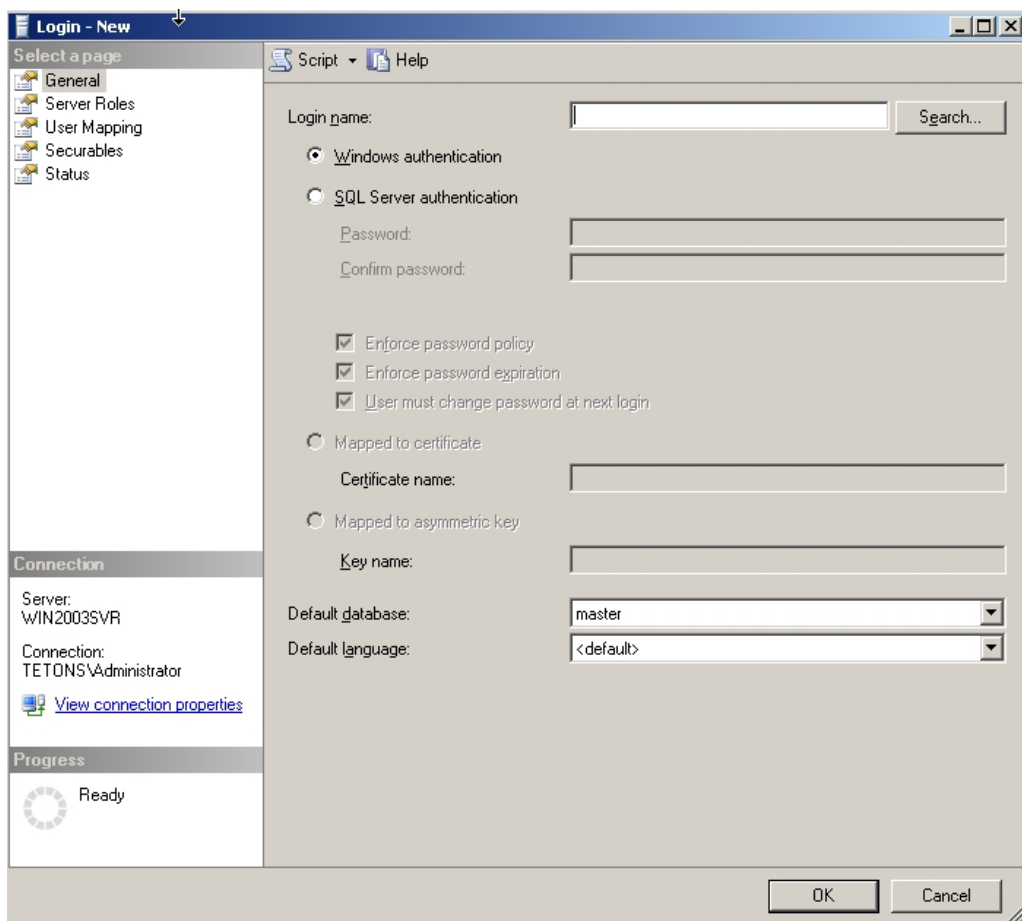
3. On the New Login dialog, enter *Domain*\Domain Computers in the **Login Name** field, and then select **Windows Authentication**.

4. Select **User Mapping** in the left pane.

5. In the right-hand pane, select the reporting database, (in this case, `PLXReporting`) as shown in the following screen.
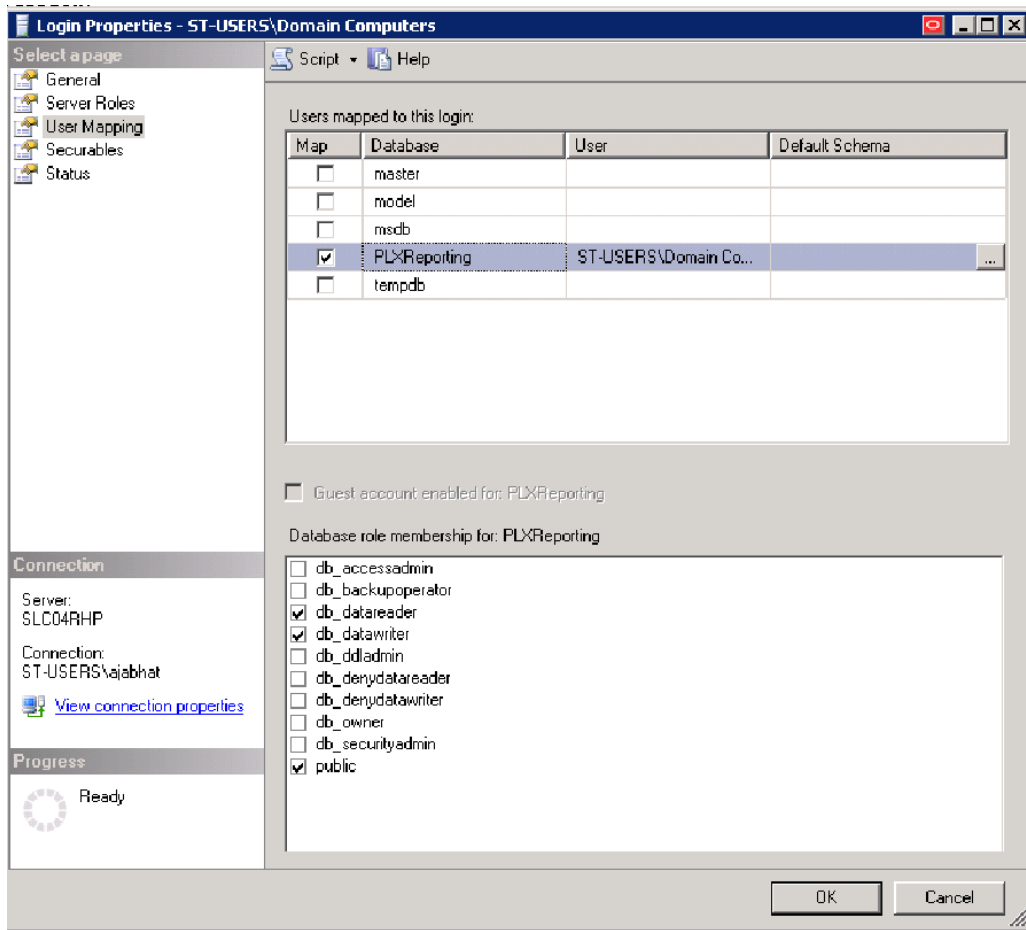
6. Enable db_datareader, and db_datawriter.

7. Click **OK**.

6.6.4 Setting Permissions to Log On to the Reporting Administrative Console

To set permissions to log on to the Reporting Administrative Console:

1. In the SQL Server Management Studio left pane, right-click on the database name (in this case, **PLXReporting**) and select **Properties**, then select **Permissions** from the left pane.

2. Highlight the user that was created to access the Reporting database (in this case, dbuser).

3. Ensure **Connect**, **Execute**, and **Select** are enabled in the Grant column, as shown in the following screens.
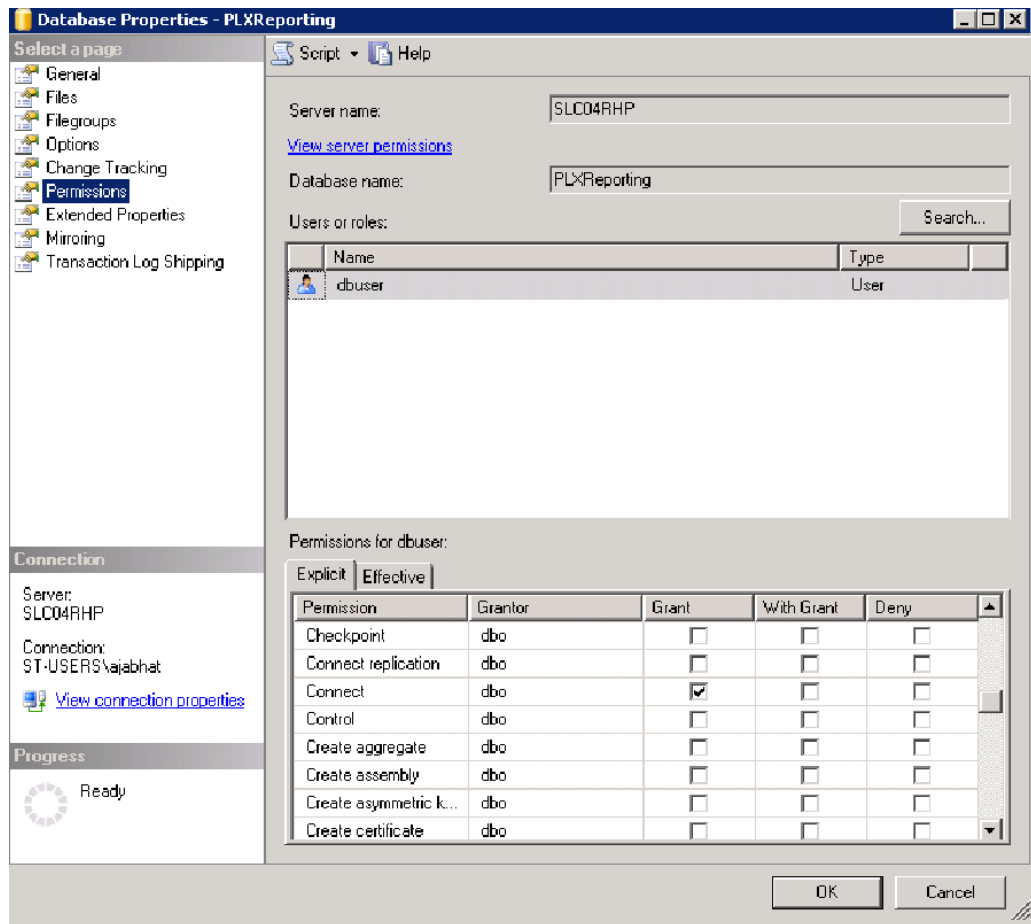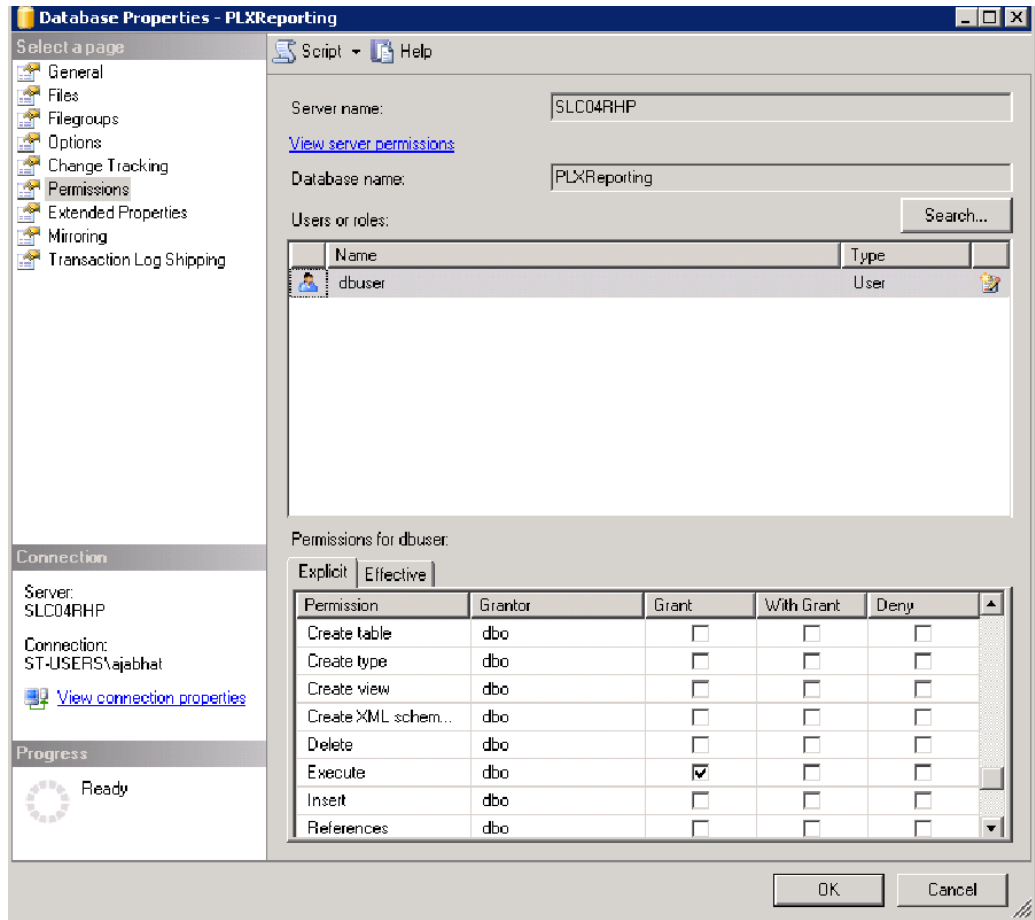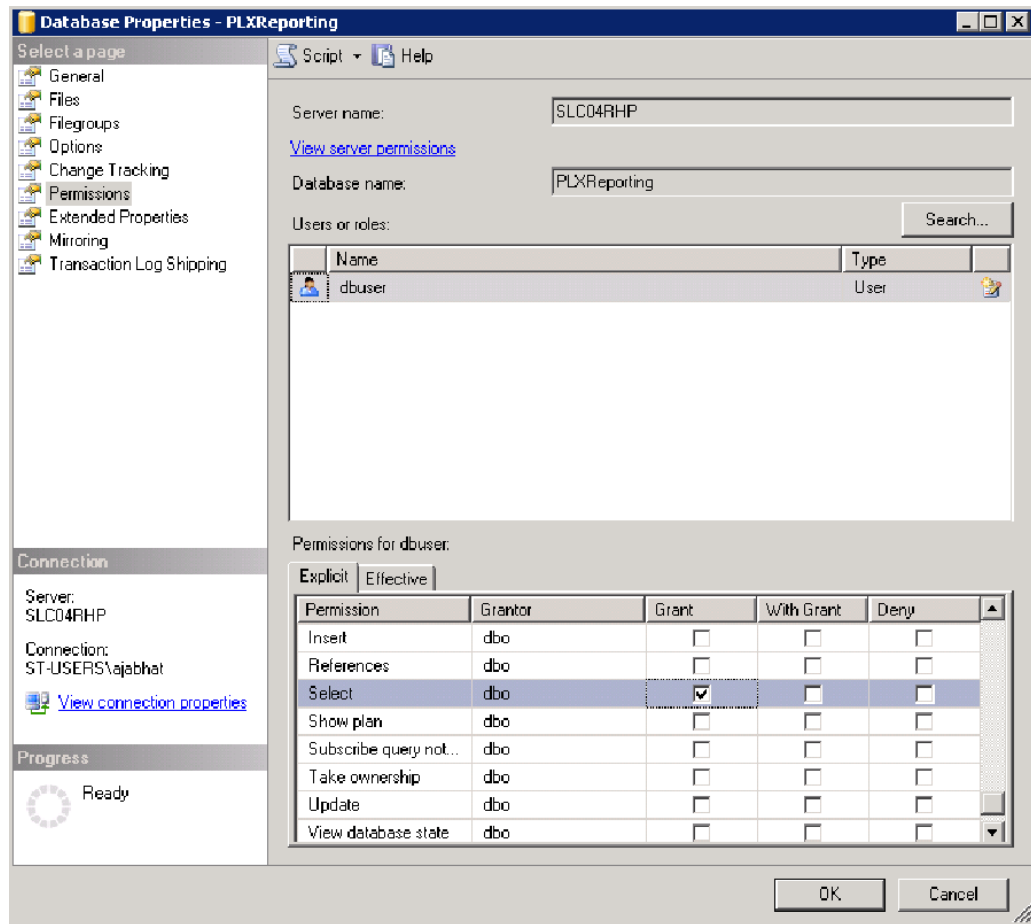
4. Click **OK**.

5. Right-click on the Reporting Database, and select **Properties**.

6. Select **Permissions** from the left pane.

7. Highlight *Domain***Domain Computers**.

8. Ensure **Connect** and **Execute** are enabled in the Grant column, as shown in the following screens.
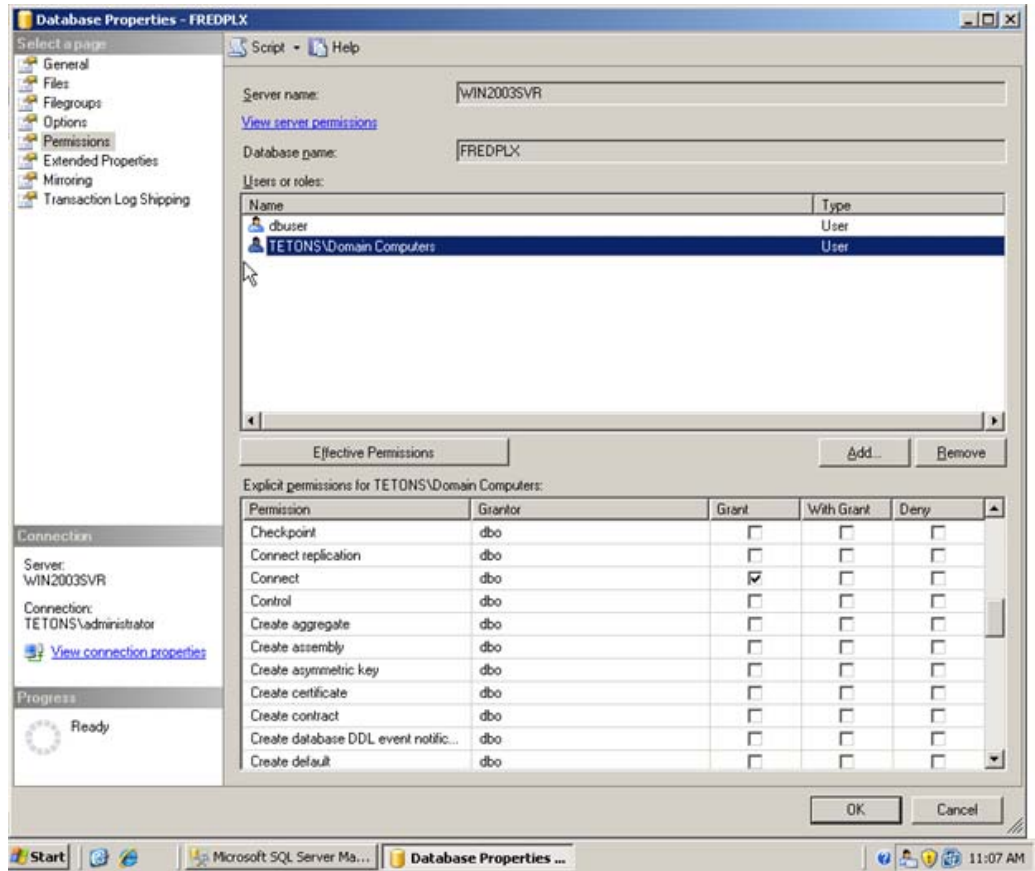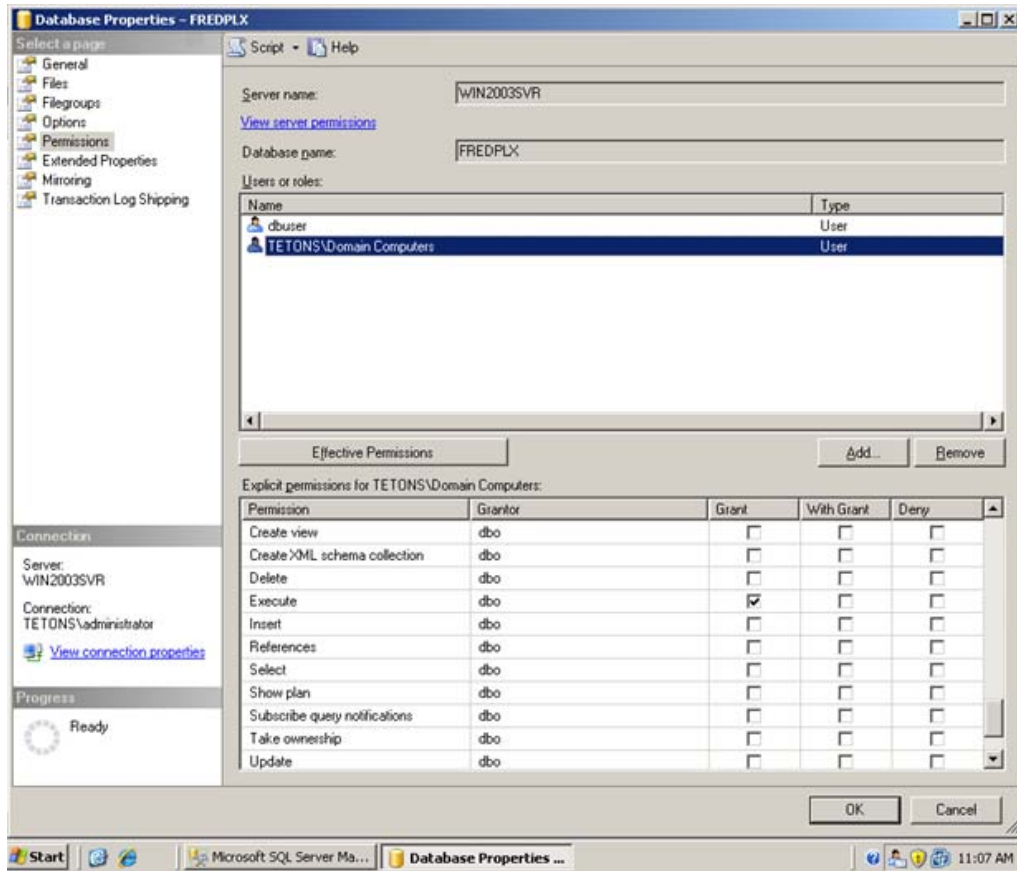
9. Click **OK**.

10. From the top node, go to **Security**> **Logins**.

11. Under **Logins**, select the user created to access the Reporting Console (in this case, dbuser), right-click, and select **Properties**.
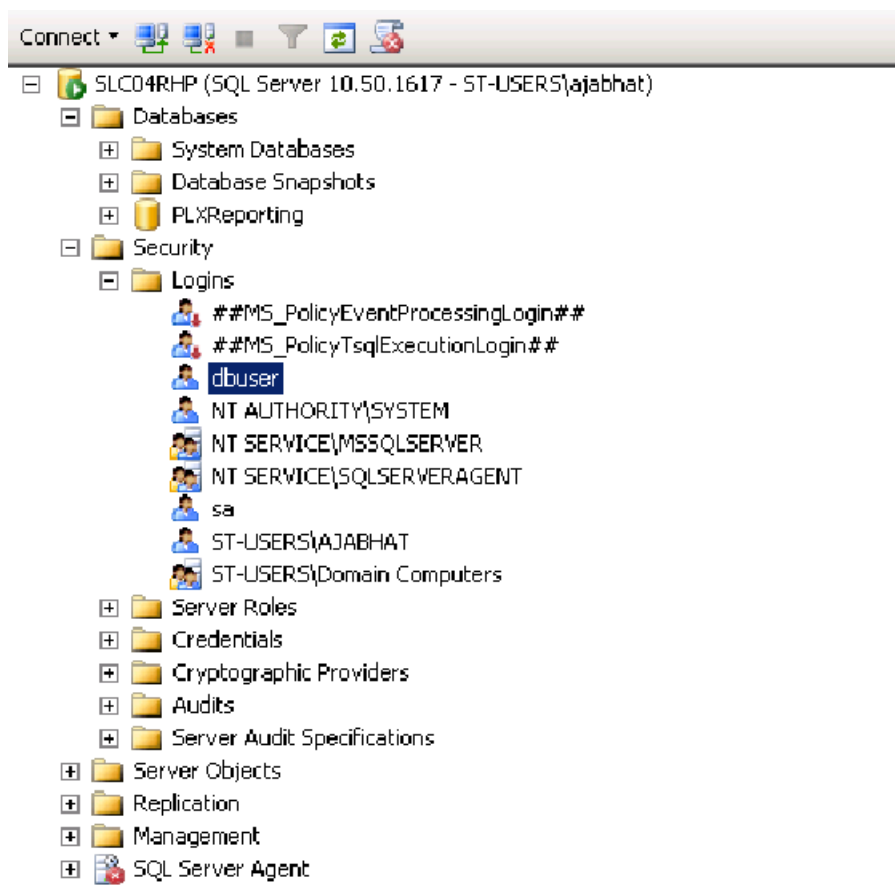
12. Select **Server Roles** from the left pane, and ensure all selections except **public** are unchecked.
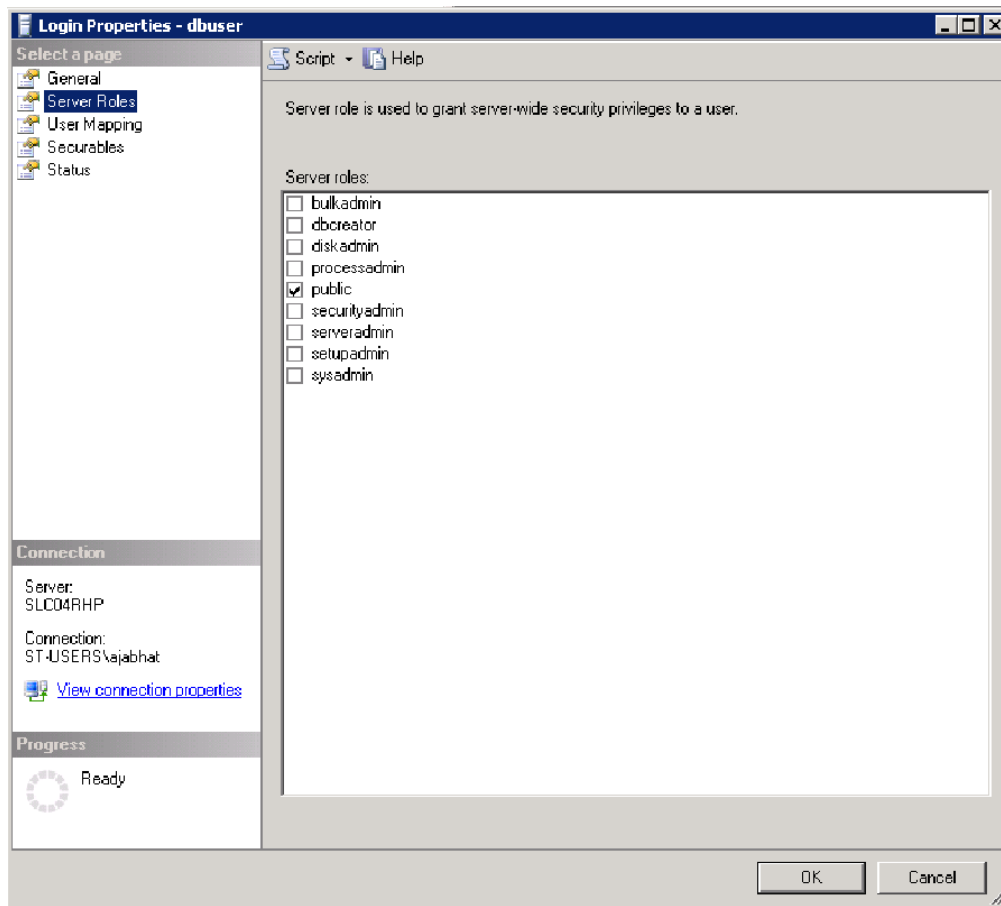
13. From the top node go to **Security** > **Logins**.

14. Under Logins, select *Domain*\\`Domain Computers`, right click, and select **Properties**.
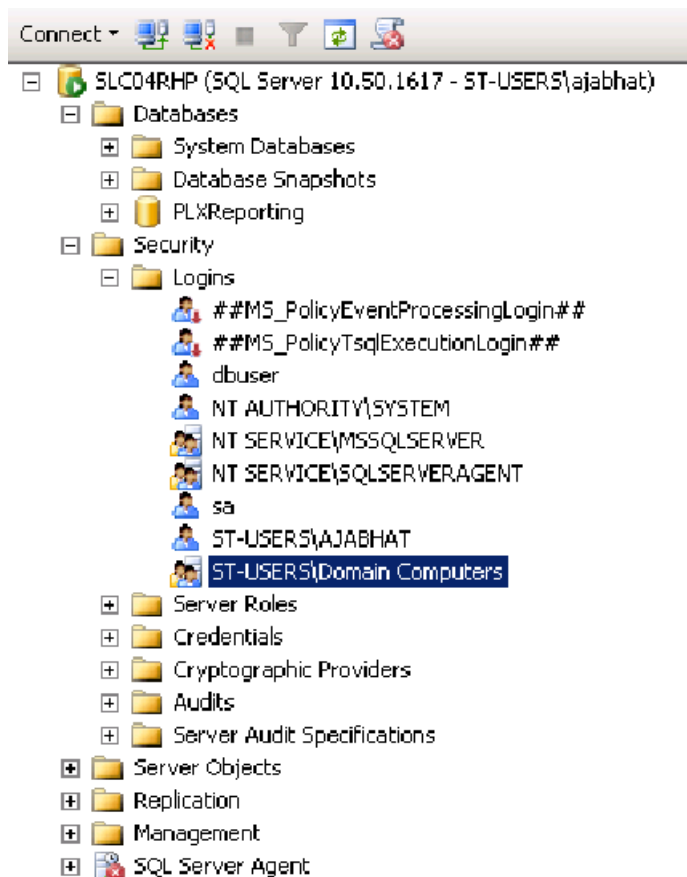
15. Select **Server Roles** from the left pane.

16. Ensure all selections except **public** are unchecked.
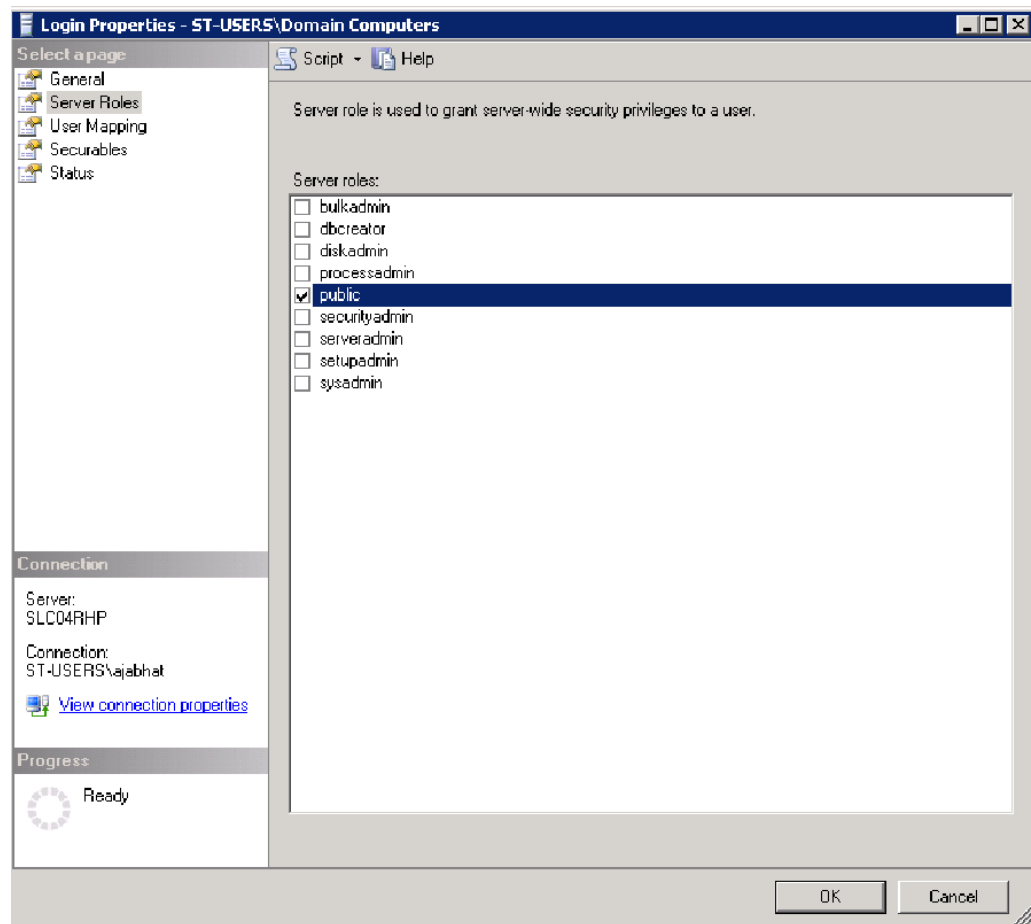
6.6.5 Enabling TCP/IP Protocol on SQL 2008 Server R2

> **Note:** This step only applies to SQL 2008 Server R2.

1. In the SQL Server Configuration Manager, select **SQL Server Network Configuration**.

2. Select **Protocols for MSSSQLSERVER**.

3. On the right pane, under Protocol Name, ensure that **TCP/IP** is enabled.
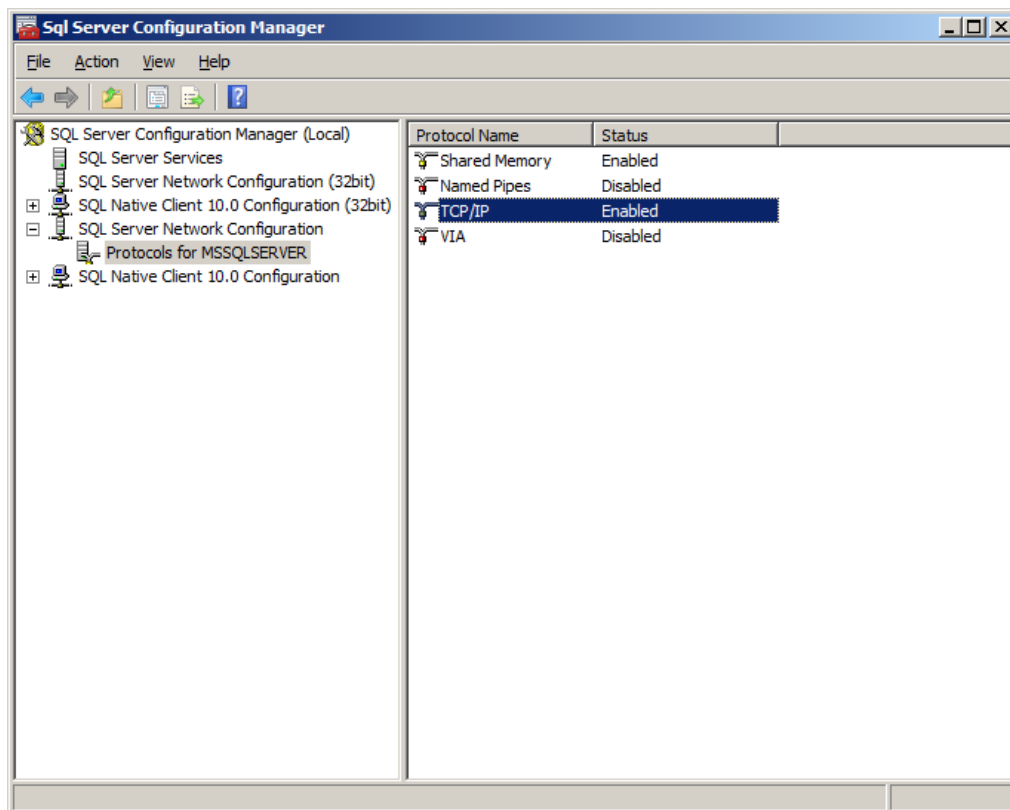
> **WARNING:** It is important to keep in mind that using a database for reporting will result in having a number of connections equal to the number of active users. This will have a substantial impact on memory requirements (for performance) and storage requirements (for data logged).

6.6.6 Setting Up Microsoft SQL Server to Use Reporting with Windows Integrated Authentication

To use Windows integrated authentication with Reporting, the ESSO Reporting Service must run as a domain user with permissions to write to the Reporting database (either Microsoft SQL Server or Oracle). To run the service as a domain user on a workstation, the user must have "Log on as a service" permissions.

You can modify this setting (as detailed in Section 6.6.6.1) on your domain controller so that the setting is published to all client computers.

6.6.6.1 Creating an Active Directory domain user that will write events to the database

Create a user in Active Directory (henceforth referred to as the "Reporting Domain User"). You will grant this user permissions to write Reporting events to the database.

6.6.6.2 Modifying the Default domain policy to allow the Reporting Domain User to Log on as a service

Modify the Default domain policy on your domain controller so that all client computers connected to the domain have this setting defined.

> **Note:** Oracle recommends that you create a backup of the current
> Group Policy before editing the default domain policy. To create a
> backup, in the console tree, open Domains/Current Domain
> Name/Group Policy objects. Right-click **Default Domain Policy**, and
> select **Back Up** from the context menu.

The Group Policy is domain-wide and overwrites the local policy. If you need to
configure any local accounts to log on as a service, refer to the documentation for the
Group Policy Management Console for this procedure.

1. On your domain controller, click **Start**, click **Run**, type `gpmc.msc`, and then click
   OK.

2. In the console tree, open **Domains** > **Current Domain Name** > **Group Policy
   Objects**. Right-click **Default Domain Policy**, and select **Edit** from the context
   menu.

3. In the Group Policy Management Editor's console tree, go to **Computer
   Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Local
   Policies** > **User Rights Assignment**.

4. In the details pane, double-click **Log on as a service**.

5. Verify that the **Define this policy setting** check box is selected, and click **Add User or Group**. Enter the new Reporting Domain User in the **User and group names** field.

6. Click **OK** when finished.

To apply the Group Policy change immediately:

- Restart the domain controller.

  or

- Open a command prompt, and type: `gpupdate /force`. Then press **Enter**.

6.6.7 Verifying Publication of the Active Directory Permission on the Client Machine

> **Note:** Also see Microsoft's technical note about modifying permissions on an Active Directory domain or local computer to allow a domain user to log on as a service.

1. Ensure that the client is updated by opening a command prompt and entering the `gpupdate/force` command. For a discussion of this procedure, see the Microsoft Technical library.

2. Go to **Administrator Tools** > **Local Security Policy**.

3. In Local Security Policy go to **Security Settings** > **Local Policies** > **User Rights Assignment** (as shown in the following figure).

4. In the Detail Panel check for the updated "Log on as a service" policy. It should include the Reporting Domain User among the users who have this permission.
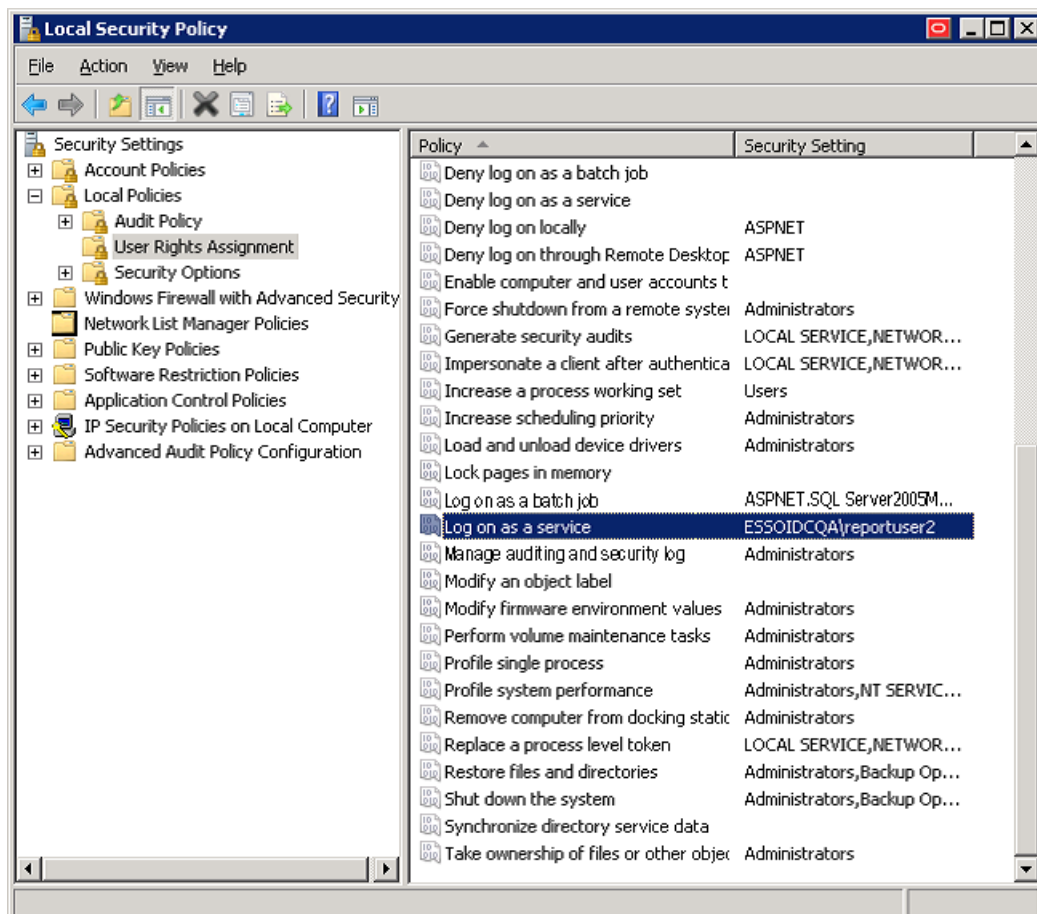
6.6.8 Configuring the ESSO Reporting Service on the Client Machine to run as this domain user

> **Note:** Perform these steps on all client computers where the ESSO Reporting Service is running.

To configure the ESSO Reporting Service to run under the Reporting Domain User account:

1. Open a command prompt and enter the following command:

   ```
   sc config "SSO Reporting Service" obj= "Domain\User" password= "password"
   ```

2. Press **Enter**.

   This command should return the following output:

   ```
   [SC] ChangeServiceConfig SUCCESS
   ```

3. Restart the ESSO Reporting Service:

   a. Open a command prompt and enter the following command.

   ```
   net stop "SSO Reporting Service" && net start "SSO Reporting Service"
   ```

   b. Press **Enter**.

This command should return the following output:

```
The ESSO Reporting Service service is stopping.
The ESSO Reporting Service service was stopped successfully.
The ESSO Reporting Service service is starting.
The ESSO Reporting Service service was started successfully.
```

Note: You can achieve the same results through the user interface by accessing the "Services" console on any client computer.

6.6.9 Setting Up Microsoft SQL Server for Integrated Authentication

Before performing the following steps for Microsoft SQL Server Integrated Authentication, you must complete the procedures described in Creating the Database Table and Setting Up Stored Procedures in the SQL Database Configuration section of this guide. You must perform those steps for both upgrades and new installations.

6.6.9.1 Configuring a Login and Role for the New Reporting Domain User in the Microsoft SQL Database

1. In the SQL Server Management Studio left pane, expand the top node (server name), then navigate to **Security** > **Logins**.

2. Right-click on **Logins** and select **New Login…**.
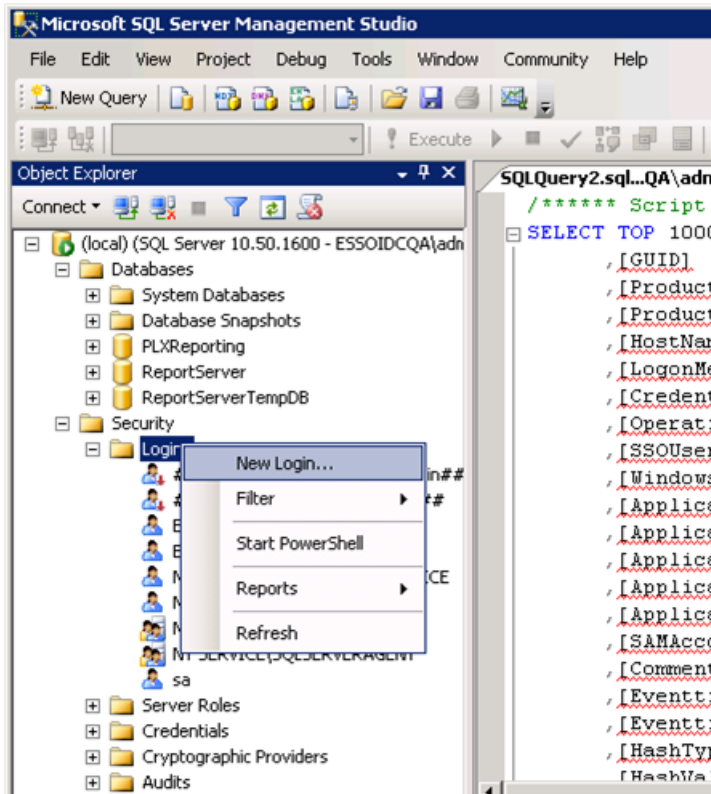
3. In the **New Login** dialog:

   a. Select **Windows authentication**. Enter the Reporting Domain User as the Login name.
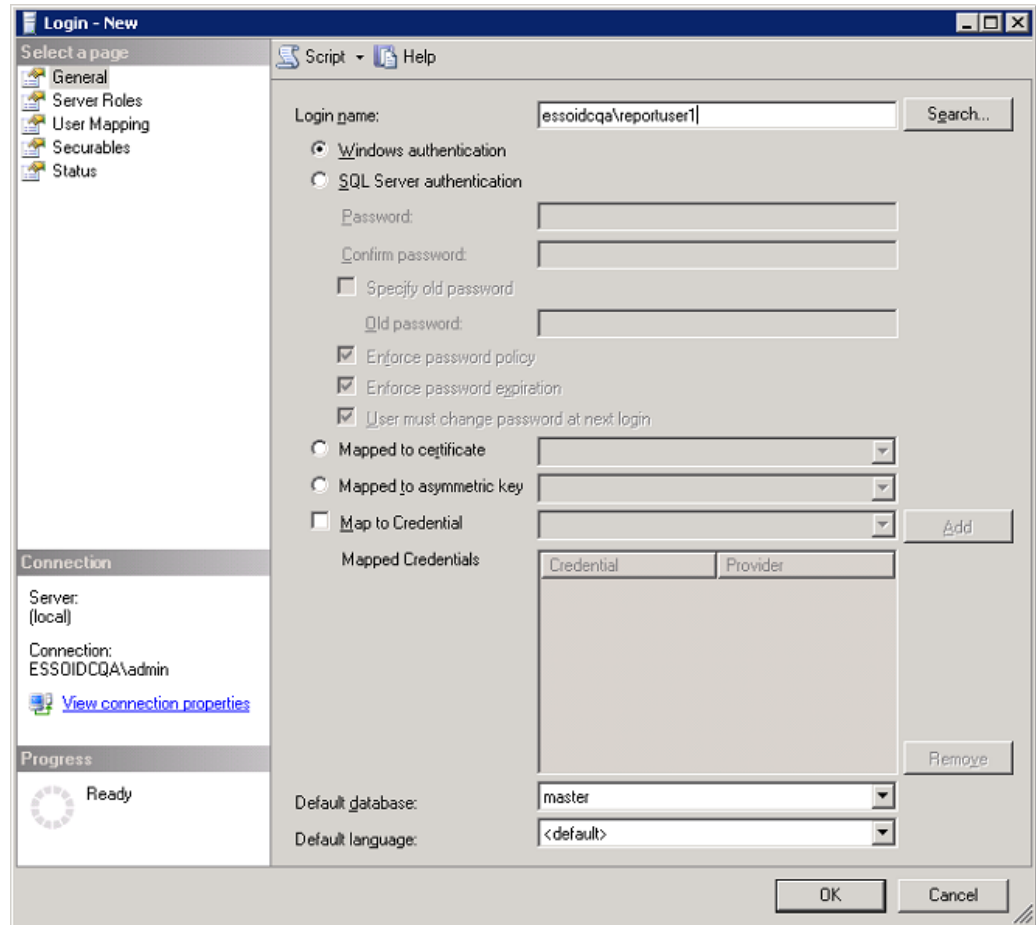
b. Select **User Mapping** in the left pane.

c. Map the Reporting Console user to the PLXReporting database.

d. Enable the db_datareader and db_datawriter role memberships for the Reporting Console User.
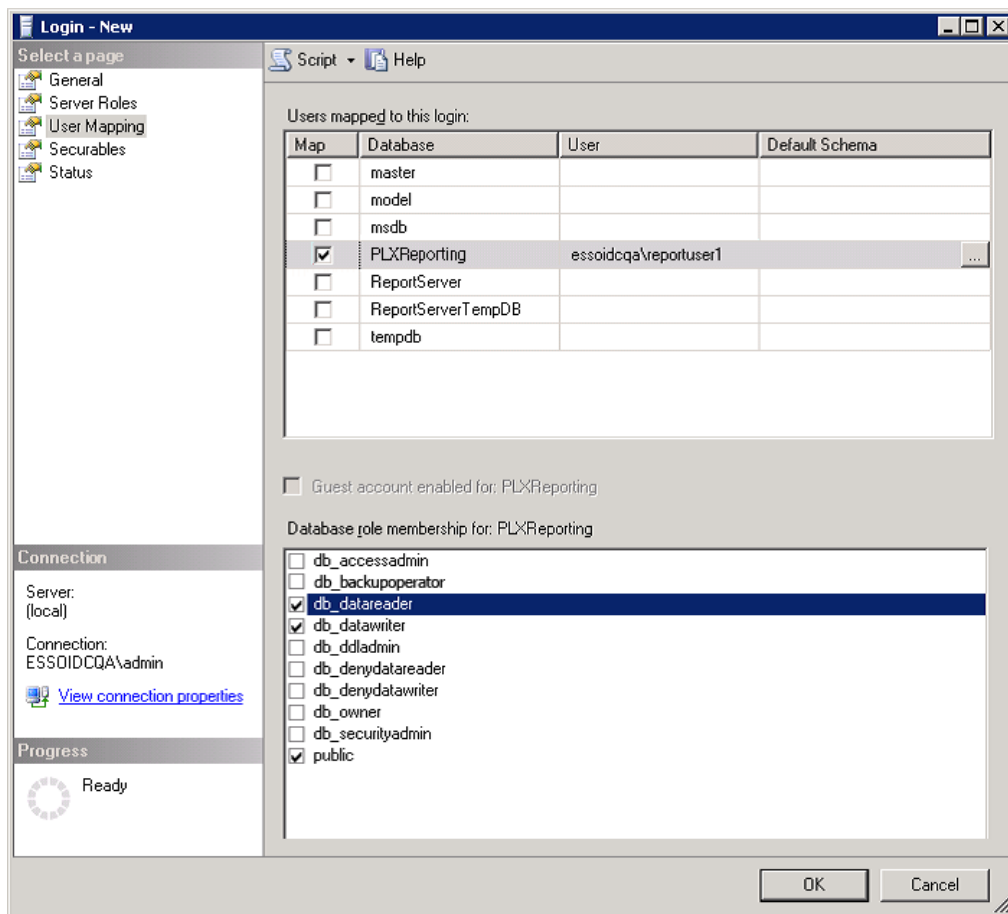
e. Select **Server Roles** in the left pane.

f. Ensure all roles except **public** are unchecked.
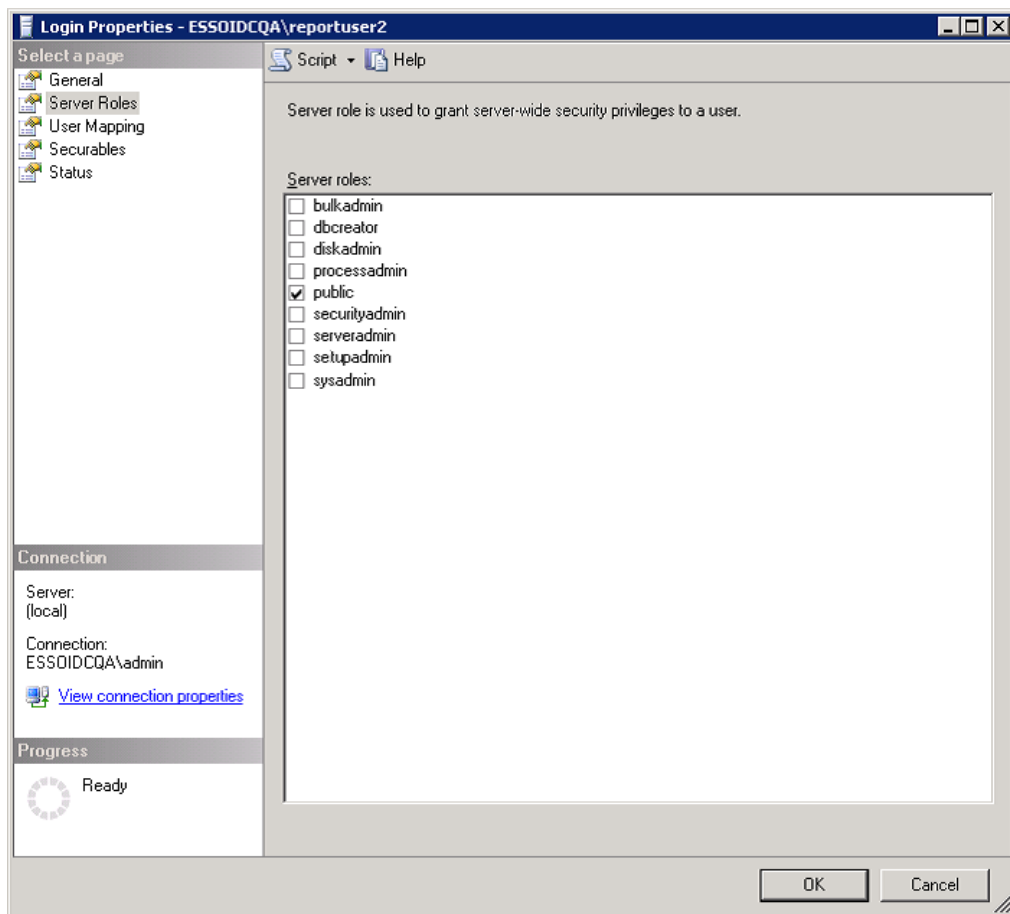
4. Click **OK**.

6.6.10 Setting Permissions for the Reporting Domain User

To set permissions for the Reporting domain user:

1. In the SQL Server Management Studio left pane, right-click on the top node (server name), and select **Properties**.

2. In the Properties dialog, select **Security** from the left pane.

3. Select the **SQL Server and Windows Authentication mode** radio button.

4. Select **Permissions** from the left pane.

5. Select the user (Reporting Domain User, created in the previous section) in the **Logins or roles** section.

6. In the bottom pane, **Explicit Permissions for <name>**, ensure **Grant** is enabled for the Connect SQL permission.
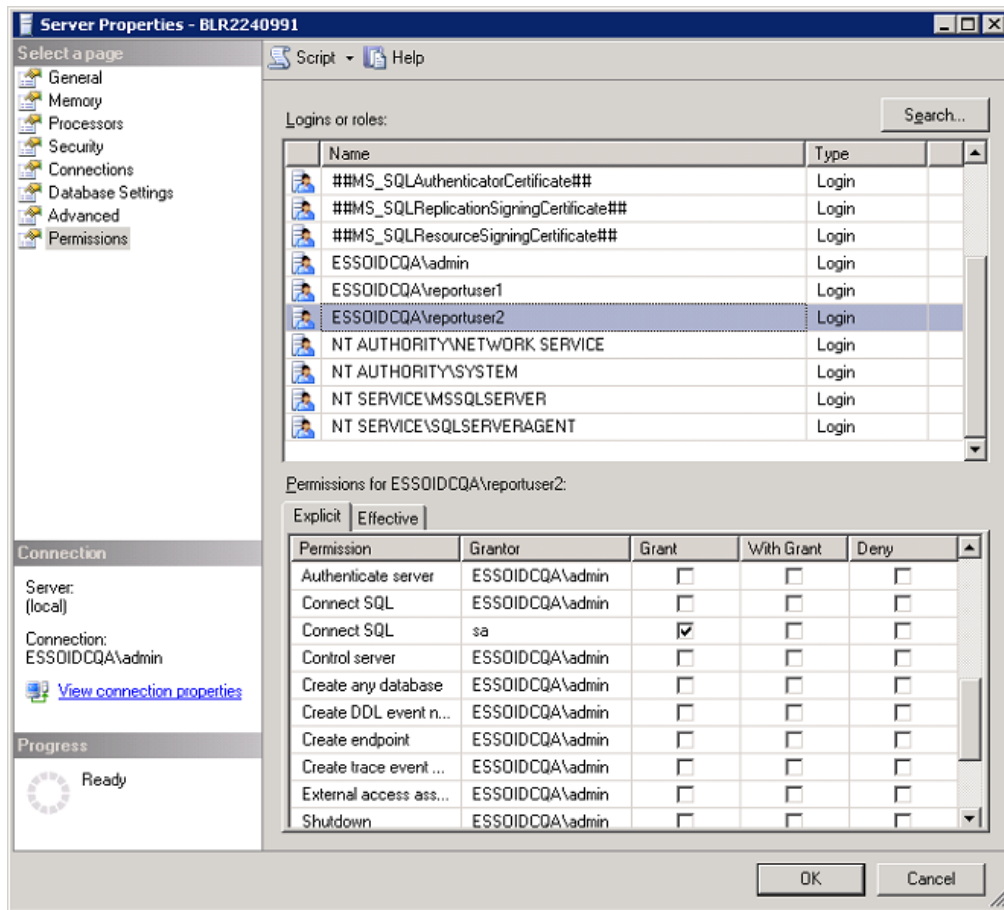
> **WARNING:** It is important to keep in mind that using a database for reporting will result in having a number of connections equal to the number of active users. This will have a substantial impact on memory requirements (for performance) and storage requirements (for data logged).

6.6.11 Next Steps

After you configure the Agent to report events and the database to store them, you must configure BI Publisher to locate them for publication. Continue to Configuring Oracle Business Intelligence Publisher.

6.7 Using Oracle Business Intelligence Publisher for Deployment with Reporting

The Reporting service uses Oracle Business Intelligence (BI) Publisher to generate reports for collected data. The following procedure explains how to configure BI Publisher to receive data from the Reporting Service. Refer to BI Publisher documentation for complete information about using this tool.

It is assumed that you have already installed BI Publisher 11g.

6.7.1 Configuring Oracle Business Intelligence Publisher

1. Open BI Publisher in your browser (the typical URL is

   `http://`*host*`:7001/xmlpserver).`

2. Submit credentials for an administrator account.

3. In the BI Publisher window, select the **Administration** menu.
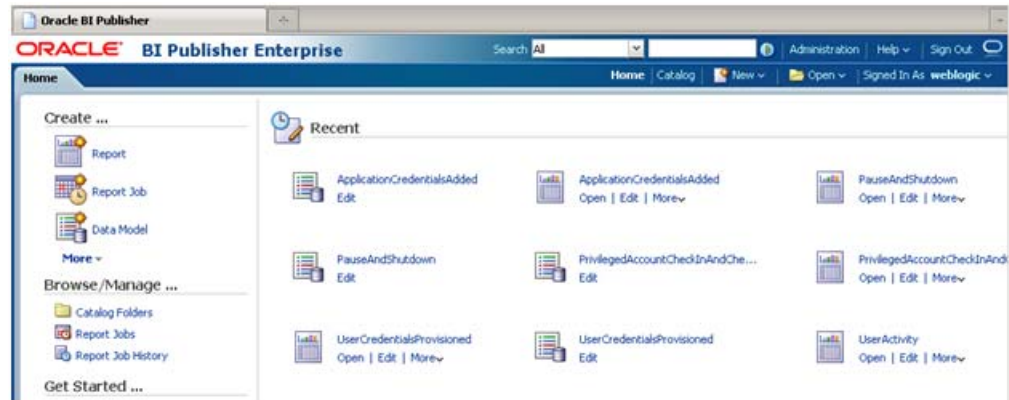
4. Under Data Source, select **JDBC Connection**.
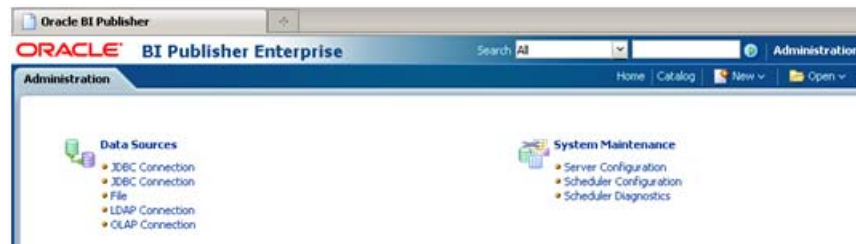
5. Click **Add Data Source**.
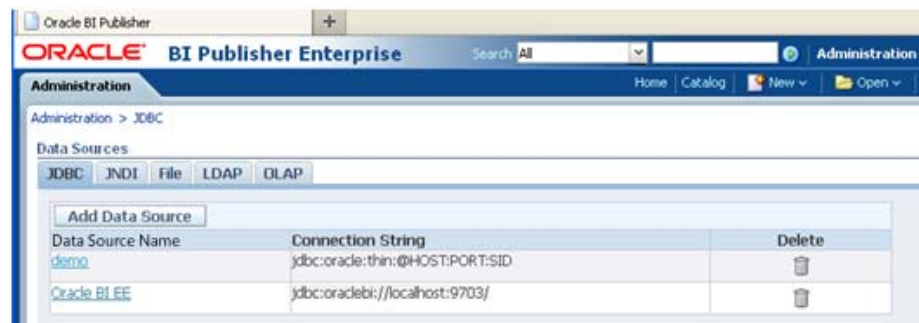
6. For the data source name, enter: `ESSOReportingDB`. Provide the Reporting database connection information as in the following examples:

   - Example of Oracle 11*g* connection information:

- Example of Microsoft SQL Server 2005 database connection information:

7. Click **Test Connection** to verify that the connection is operational. You will see a Confirmation message when the test succeeds.

8. In the Security section, set the roles that will have access to the ESSOReportingDB data source.

9. Click **Apply** to save your settings.

10. On the Administration page under System Maintenance, select **Server Configuration**.

11. In the Catalog section choose catalog type **Oracle BI Publisher - File System** and set a folder on your hard drive. This folder will be used for storing your reports. Click **Apply**.
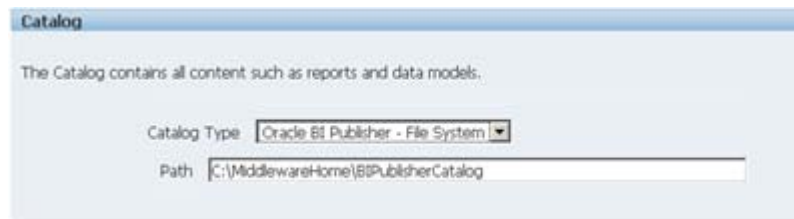
Continue to the next section to add Oracle Enterprise Single Sign-On Suite reports to Business Intelligence Publisher.

6.7.2 Deploying Reporting

To deploy Reporting

1. Open the BI Publisher Catalog folder on your hard drive.

2. Create a Reports folder in this location. BI Publisher searches for the Reports folder in the `BIPublisherCatalog` directory, so it is important that you create this folder in the correct place.
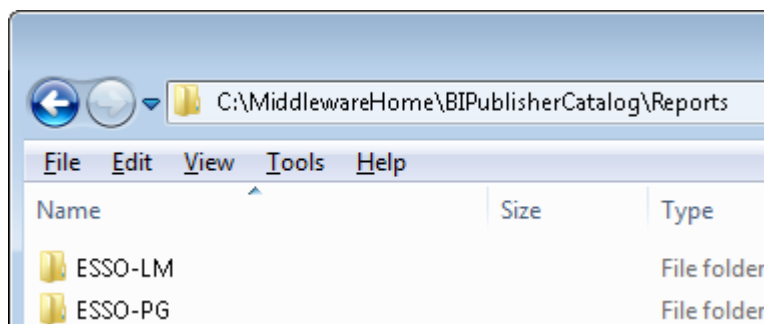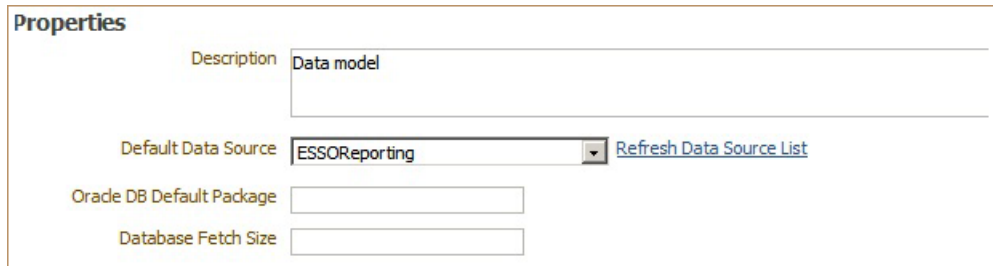
3. Copy Oracle Enterprise Single Sign-On Suite reports to the `Reports` subfolder.

4. Restart Business Intelligence Publisher.

5. Log on to Business Intelligence Publisher and navigate to **Catalog** > **Shared Folders**. Oracle Enterprise Single Sign-On Suite Reports are ready to use.

6. Under the Report Folder for each component (for example, Logon Manager), for each Report Type "Data Model," click **Edit**.

7. In the Properties dialog, select the database connection you created previously as the value for the Default Data Source.

Then select from the List of Values to the left of the Properties dialog. Change the Data Source in this dialog as you did in the step above, assigning the previously-created database connection.

8. Save your changes after completing this process.

Reports are ready to use.

7

Reference

This section contains important supplementary information about configuring and using Oracle Enterprise Single Sign-On Suite components.

- General Suite Information
- Logon Manager
- Password Reset
- Reporting
- Universal Authentication Manager Registry Settings

7.1 General Suite Information

This section contains information applicable to all products in the Oracle Enterprise Single Sign-On Suite.

> **Note:** Keep in mind the distinction between registry paths for 32-bit and 64-bit operating systems.
>
> The path for a 32-bit OS registry key begins with "`HKEY_LOCAL_MACHINE\SOFTWARE\...`".
>
> The equivalent registry key path for a 64-bit OS begins with "`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\...`".

7.1.1 Installing an AD LDS (ADAM) Instance

To install AD LDS (ADAM):

1. Launch `ADAMSetup.exe`.

2. Select **A unique instance** and click **Next**.

3. Enter your instance name and click **Next**.

4. Specify port numbers of 10000 and 10001 (10,000 range, for easy recall) and click Next.

5. Specify the root `DN` (for example, `OU=SSPR, DC=Oracle,DC=Com`) and click **Next**.

6. Specify an easy-to-find base location (for example, `%RootDrive%\ADAM\Instance`) and click **Next**.

7. Specify the run privileges and click **Next**.

8. Specify the administrative permissions and click **Next**.

9. Select **Do not import LDIF files for this instance of AD LDS (ADAM)** and click **Next**.

10. Click **Next** as requested to proceed.

11. Click **Finish**.

7.1.2 Obtaining a Certificate for SSL Connectivity

Before configuring applications for SSL connectivity, you must obtain an X.509 Certificate from a trusted certificate authority (CA). This trusted CA must be installed in the list of trusted Root CAs. The certificate must be valid for the current date and its subject must exactly match the network name (either its host name or fully-qualified URL containing a host name and domain suffix) that the various application instances will use when connecting to the corresponding server instance.

Refer to the following articles from the Microsoft Web site for information on installing certificates and setting up SSL:

- "How to: Obtain an X.509 Certificate"
  http://msdn2.microsoft.com/en-us/library/ms819929.aspx

- "How to: Set Up SSL on a Web Server"
  http://msdn2.microsoft.com/en-us/library/aa302411.aspx

If you use Microsoft Certificate Services to obtain the X.509 certificate, choose a Server Authentication Certificate. Also, enable the **Mark keys as exportable** and **Use local machine store options** under the **Key Options** section.

7.1.2.1 Considerations When Deciding to Use SSL

Logon Manager supports the use of Secure Sockets Layer (SSL) and enables it by default. When deciding whether to use SSL, consider the following:

- Logon Manager encrypts all credentials locally through the user's configured authentication method, and transmits and stores those credentials in encrypted form.

- For repositories that use pass-through authentication (for instance, Active Directory or AD LDS (ADAM)), Logon Manager secures all transactions with the central repository (including authentication to the repository); no credentials of any type are transmitted in clear text.

- When using LDAP repositories or pass-through repositories in conjunction with Kiosk Manager, the repository authentication will be a clear-text LDAP transaction if SSL is not enabled. If this authentication must be secure, enable SSL for transactions between the client and the repository.

For complete instructions on setting up SSL certificates, refer to the following documentation:

- Microsoft Active Directory Server: Microsoft MSDN

- Oracle Directory Server Enterprise Edition: Oracle Directory Server Enterprise Edition Administrator's Guide

- Novell eDirectory: eDirectory 8.5 Administration Guide

SSL is configured with the registry keys `UseSSL` and `SSLFallback`.

7.2 Logon Manager

This section contains information applicable specifically to Logon Manager.

7.2.1 Understanding the Application Configuration Files

Logon Manager stores its application logon instructions in a file named `aelist.ini` that typically resides in the each user's `%AppData%\Passlogix` directory (`C:\Documents and Settings\username\Application Data\Passlogix`). The Agent creates `aelist.ini` by merging two component files:

- `entlist.ini`, which you create using the Administrative Console to provide your organization with customized logons for Windows, Web site, and mainframe/host applications. The Agent's synchronizer extension places `entlist.ini` in `%AppData%\Passlogix`.

- `applist.ini`, which is included in the Agent installation package and contains predefined logons for network and web pop-up logon dialogs and for many online service providers. The `applist.ini` file resides in the Agent's installation directory.

> **Note:** Pre-configured logons for many Windows and Web applications are provided in the Administrative Console templates.
>
> All Administrative Console configuration files (including `entlist.ini` and `ftulist.ini`) can only be created and edited using the Administrative Console.

7.2.1.1 How the Agent Uses entlist.ini

The Agent merges `entlist.ini` with `applist.ini` to create `aelist.ini` in the `%AppData%\Passlogix` directory. The Agent overwrites `aelist.ini` periodically, including at Agent startup. The Agent then uses `aelist.ini` to detect known applications.

If using a synchronizer extension (for example, Directory Server or File System), a remote object overrides any local `entlist.ini` file, and is then merged with `applist.ini`.

If there is no remote object or local `entlist.ini` file, the Agent will utilize `applist.ini` without creating the `aelist.ini` file.

> **Note:** You can modify `entlist.ini` or the `SSOentlist` object while the Agent is running. To force the Agent to re-merge to create a new `aelist.ini`, select **Refresh** in Logon Manager.

See the following topics for more information about creating and distributing application logons:

- Creating logons from templates:

  - Chapter 2.13.3, "Creating a New Windows or Java Application Template"

  - Chapter 2.13.5, "Creating a New Web Application Template"

  - Chapter 2.13.6, "Creating a New Host/Mainframe Application"

- Distributing logons:

置

- – [Chapter 2.3.4, "Administration and Management"](#)

- – [Chapter 2.12, "Creating and Using Templates"](#)

See [Chapter 2.17.3, "Global Agent Settings in Depth"](#) for detailed descriptions of Global Agent Setting options.

7.2.1.2 How the Agent Uses aelist.ini

The file that results from the merger of `aelist.ini` contains all the information necessary to identify and respond to logon and password change events for all configured applications. This information comprises:

- Application-type settings such as Error Loop settings; for example, how many times the Agent will retry a logon within the specified time period.

- Application-specific configuration information; for example, application executable name or Web site URL, password change behavior, password policies, error loop settings, and data file extension.

- Scenario-specific configuration information for the logon and password change scenarios; for example, window dialog title strings, form names, and locations for credentials.

- Dialog-specific matching settings; for example, that a string or control is or is not present.

- Other settings; for example, name of a third or fourth field.

- The merged file, `aelist.ini`, has a hierarchical structure, containing all the information necessary for the Agent to uniquely identify and respond to logon and password change events for each application to configure. It organizes logons in sections and subsections as in the following table.

Structure	Reference

`[*Other Apps]`
`Section1=Application logon 1`
`Section2=Application logon 2`
	This section exemplifies two administrator-defined Windows applications defined later in the file. See [Chapter 2.12.3, "Adding Windows Applications"](#) for details.

`[*Mainframe]`
`Section1=Host logon 1`
`Section2=Host logon 2`
`&`
	This section exemplifies two host/mainframe applications defined later in the file. See [Chapter 2.12.5, "Adding Host/Mainframe Applications"](#) for details

`[*Shared Groups]`
`Section1=Shared Group 1`
`Section2=Shared Group 2`
`&`
`SectionN=Shared GroupN`
`&`
	This section exemplifies two groups used for credential sharing. See [Chapter 2.8, "Working with Credential Sharing Groups"](#) for details.

`[*PasswordPolicies]` `&`	This section enables Password Policies. See [Chapter 2.6, "Setting Password Policies"](#) for details.

The application configurations in `entlist.ini` allow the Agent to automatically recognize and respond to logon and password-change requests from applications specific to your organization.

When present as a local file or downloaded from a remote object, the Agent downloads an `entlist` object (if available) to an `entlist.ini` file, and combines your downloaded or local `entlist.ini` with those Oracle supplies in `applist.ini` to create `aelist.ini`, the complete list of predefined applications available to users. (If `entlist.ini` is not present, the Agent utilizes `applist.ini`.)

> **Note:** Because Oracle provides updates to `applist.ini`, it is strongly recommended that you make no changes to this file. Future Logon Manager releases may overwrite your changes, and Oracle cannot guarantee that future releases will support changes made to `applist.ini`.

7.2.2 Best Practices for Deploying the Agent in a Citrix Environment

Deploying Logon Manager on Citrix can be performed using several strategies, with dependencies on how the Citrix farm or farms are deployed, and how access is delivered to end-users. These methods do not change between using a Citrix ICA client on the desktop and using the Citrix Web portal to deliver applications, except where otherwise specified.

Fundamentally, three options exist:

- Deploying Logon Manager Per User. Enables you to deploy Logon Manager to all servers and all applications, yet still limit users who will utilize it on those servers and applications.

- Deploying Logon Manager Per Application. Enables you to deploy Logon Manager to all servers and users, but only on a per-application basis.

- Deploying Logon Manager Per Server. Enables you to deploy Logon Manager to individual servers.

This section covers these options in depth.

7.2.2.1 Installation

Regardless of the ultimate configuration, the initial Agent installation process is the same for all deployment options.

Before starting, be certain that you have properly configured your Global Agent Settings, have a solid understanding of Logon Manager, and decided which extensions you need to install with the Agent. Generally these will be the same extensions and very similar GAS settings to the user workstations in your environment. For more detailed instructions on installing Logon Manager on Citrix, see Chapter 2.16.5, "Configuring the Agent in a Citrix Environment."

To install Logon Manager on Citrix MetaFrame:

1. Log on to the Terminal server as an administrator and close all applications.

2. Click **Start** and then click **Run**. The **Run Dialog** window appears.

3. Type `cmd` and press **Enter**. The **Command Prompt** window appears.

4. Type `change user/install` and press **Enter**.

5. Install Logon Manager with the appropriate installation options for your environment.

6. At the command prompt, type `change user/execute` when installation is complete.

7.2.2.2 Deploying Logon Manager Per User

Deploying Logon Manager per user allows you to control access to those users/groups that should and should not be granted access to use Logon Manager.

The steps to deploy Logon Manager per user are as follows:

1. Create a group on your domain for Logon Manager Users. Include all users in your environment who will use Logon Manager for Citrix published applications.

2. On each Citrix server, edit the Security properties of the `ssoshell.exe` file located in the `C:\Program Files\Passlogix\v-GO SSO` directory.

3. Add the previously-created SSO Users group to the ACL of the directory. Be sure to give this group the rights "Read" and "Read & Execute" to this file. Remove the Users, Domain Users or any other group that may have read access to this file. To accomplish this, you may have to uncheck **inherit permissions from parent**.

   This method of permission settings will still allow any administrators full access to this file, and thus the ability to use Logon Manager. There are many other possible combinations or ways to set these permissions. The ultimate goal is to give those users needing access to Logon Manager the permissions to read/execute `ssoshell.exe` and keep all other users from being able to access/read it at all.

   Using the per-user deployment option in Citrix means you can leave all applications published to all users and do not have to use `ssolauncher.exe` to configure each of your Published Applications.

4. If you do not wish to invoke Logon Manager immediately, delete the `ssolauncher.exe` value from the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AppSetup` key in the Windows registry.

   Without this key, Logon Manager will not respond to any applications. To elicit a response, you would have to either replace this key or modify your published applications commands to include `ssolauncher.exe`.

7.2.2.3 Deploying Logon Manager Per Application

Deploying Logon Manager per application allows you to enable Logon Manager on an application by application basis.

The steps to deploy Logon Manager per application are as follows:

1. Install Logon Manager on every server that will host a single sign-on-enabled application.

2. Prevent Logon Manager from launching automatically by deleting the `ssolauncher.exe` value from `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AppSetup` and deleting the `ssoshell.exe` value from the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\UserInit` key. For specific instructions on doing this, use the keyword "Citrix" in the SSO Console help files.

3. Modify the published applications that you wish to use Logon Manager with to include a command-line wrapper that calls `SSOLauncher.exe`, which subsequently calls the original command line. For specific instructions, see Chapter 2.16.5, "Configuring the Agent in a Citrix Environment."

7.2.2.4 Deploying Logon Manager Per Server

Deploying Logon Manager per Citrix server allows you to enable the Agent on a server-by-server basis. This is the easiest of the three methods to fully deploy.

1. Install Logon Manager on Citrix Servers that you wish to enable for single sign-on.

2. Direct Logon Manager users to the single sign-on-enabled servers.

   There is no need to modify any published applications, set any permissions, or remove any registry keys. Logon Manager automatically launches for all users on this server. This method works well if users access remote desktops via the Citrix server.

7.2.2.5 Global Agent Settings Specific to Citrix Servers

For the most part and in most cases, the Citrix servers will use Global Agent Settings that are extremely similar to those deployed to all of your other Logon Manager client machines. In a typical deployment, you would fully configure and test a client workstation prior to beginning Citrix. After you configure and validate your Global Agent Settings configuration, import these into the Administrative Console and rename them for use in your Citrix Environment.

You should configure the following Global Agent Settings for Citrix servers:

- **End-User\Experience\Advanced\Store user data on disk in encrypted format**: Set to "Do not store data in user disk file."

- **Synchronization\Delete local cache**: Set to "Delete."

- Eliminate drive letter hard-coding in Global Agent Settings: these are in the Synchronizer and Event Log settings. Simply change the "C:" to match whatever drive letter where you have installed Logon Manager on your Citrix server. If different Citrix servers use different drive letters, you would have to specify different settings for each server. This is crucial because Logon Manager uses this drive letter to locate components.

7.2.2.6 Publishing Applications

After completing the preceding procedures, Logon Manager is ready for use on your Citrix servers. You can begin enabling some or all of your published applications. To enable Logon Manager for an application, you need to modify its command line using ssolauncher.exe. For specific instructions, see Chapter 2.16.5, "Configuring the Agent in a Citrix Environment."

7.2.3 Logon Manager Application Compatibility Considerations

While Oracle officially tests and supports only the applications for which we provide templates, we have an exceptionally high success rate enabling the vast majority of business and productivity applications for Windows, the Web, Java applications and mainframe/AS400 emulators. Our support team will assist you in configuring any application template unless or until we determine that the application as it exists is incompatible with Logon Manager.

The following table identifies characteristics of applications for which Logon Manager is known to have support issues:

High Risk	Medium Risk
Application characteristics that generally hinder successful application template configuration	*Application characteristics that often result in incomplete SSO functionality or require an action on the part of the end-user to complete the sign-on or password change*

High Risk	Medium Risk
■ XWindows	■ Applications hosted on Terminal Server or Citrix, if Logon Manager cannot be installed on the Terminal Server or Citrix box.
■ Flash applications	
■ Outdated Java (earlier than 1.3.1)	■ Applications where the OK Button is missing and ENTER is not accepted. Logon Manager cannot process the submission and the user must manually submit the credentials or SendKeys must be used.
■ Non-HLLAPI emulators	
■ Emulator applications that already use HLLAPI, when used in conjunction with emulators that allow only one application to connect to HLLAPI	
■ DOS GUI applications and DOS applications not run in CMD	■ Applications where logon or password change requires an action (for example, a checkbox). SendKeys can be used for Windows applications.
■ Web Applications that:	■ Applications where the window title of the target application changes after creation but before the logon screen is active.
–Require SendKeys.	
–Require a delay.	■ Applications where logon fields are on a page with other logon or credential entry fields. Logon Manager cannot distinguish between multiple logons if they are on the same screen.
Logon Manager does not inject credentials until it sees that the page has fully loaded. With some Web sites, the page appears to be fully loaded from the perspective of the browser, but fields are not yet ready for credential injection.	■ Applications where the Submit button is in an image tag with a fully-qualified path and ENTER is not accepted. If the image path changes, Logon Manager will not insert and submit the credentials properly.
■ Applications that require matching to fix an issue (for example, logon looping, ignore, password change, etc.), but unique criteria is not available for matching.	■ Password change scenarios where the application password policy does not match the SSO capabilities, and the user is responsible for password selection (for example, if the application has a password history or dictionary requirement).
	■ SendKeys for Windows applications (Web applications are high risk and Mainframe applications lose the password change).

7.2.4 Configuring Host Emulators

Logon Manager provides single sign-on functionality for the following host/terminal emulators using built-in HLLAPI (high-level language application programming interface) support. The topics listed here outline how to enable HLLAPI support in each emulator.

- Attachmate EXTRA!/ myExtra!

- BlueZone Web-to-Host Emulator

- BOSaNOVA

- Ericom PowerTerm

- G&R Glink

- Hummingbird Host Explorer

- IBM Client Access

- IBM Client Access Express

- IBM Host On-Demand

- IBM Personal Communications

- Jolly Giant QWS3270 PLUS

- NetManage Rumba

- Net Soft NS/Elite

- Newhart Systems BLUES 2000

- Novell LAN Workplace

- PuTTY

- Scanpak Aviva for Desktops

- Seagull BlueZone

- WRQ Reflection

- Zephyr PC to Host

- Zephyr Web to Host

> **Note:** For emulators that do not implement HLLAPI support, you can configure a host/mainframe application as a Windows application (to detect the form by its window title) and using SendKeys (to supply user credentials). See Section 2.12.3, "Adding Windows Applications" for more information.

7.2.4.1 Attachmate EXTRA!/ myExtra!

> **Note:** For a complete list of supported versions, see Oracle support.

To set up each session of Attachmate EXTRA! to work with Logon Manager:

In the emulator:

1. Open the session.

2. Select **Global Preferences** from the **Options** menu.

3. Select **Advanced**, select the **Short name** (for example, A), select **Browse**, select the session document, and click **OK**.

> **Note:** This setting needs to be saved with each session configuration file.
>
> Background processes sometimes remain running after a mainframe or host session has ended. This may disrupt the Auto-Logon process and prevent the session from restarting.

7.2.4.2 BlueZone Web-to-Host Emulator

> **Note:** For a complete list of supported versions, see Oracle support.

To install and configure BlueZone Web-to-Host emulator:

1. Launch the **BlueZone Web-to-Host** setup.

2. In the **Setup Type** section, select **Install BlueZone Web-to-Host** and click **Next**.

3. Read the end-user license agreement carefully. If you agree to the terms, select the button next to **Yes, I agree with the terms of this software license**, and click **Next**.

4. Select a location to install the software. The installer defaults to your C: drive's Program Files directory.

5. Direct the installer to the location of the Seagull Activation File (SAF), or leave it blank if you do not have an SAF yet.

6. Select whether the installer should create a program group to use, and whether it should create a desktop shortcut for the BlueZone Web-to-Host Wizard, and click **Next**.

7. In the **Sites** dialog, select a language for the site from the dropdown menu.

8. Do one of the following:

   ■ Click **Create** and enter a path and folder name.

   ■ Click **Import** and navigate to the site you want to import.

   ■ Click **Copy** and navigate to the site you want to copy.

   ■ Click **Upgrade** and navigate to the site you want to upgrade.

   ■ If you want to delete an existing site, select it and click **Delete**.

9. In the **Launch Folders** dialog, select an existing launch folder, or click **Create** to create a new one. Click **Next**.

10. In the **New BlueZone Launch Folder** dialog, enter the folder name, and select from the folder options whether to distribute as a standard web-to-host or as a served desktop. Click **OK**.

11. When you return to the **Launch Folders** dialog, which now displays your new launch folder, click **Next**.

12. In the **Sessions** dialog, click **Create**.

13. In the **New BlueZone Session** dialog, select **Mainframe Display** from the dropdown menu and click **OK**.

14. Enter a name for the session and specify whether to use an existing profile. Select an existing profile if appropriate. Select whether to allow local saves. Click **OK**.

15. In the **Define New Connection** dialog, enter your connection information and click **OK**.

16. Review the information in the **Session Properties** window. Edit any information that you want to change. Click **OK** when you are done.

17. Select **Session** in the BlueZone Mainframe Display and click **Connect**.

7.2.4.3 BOSaNOVA

> **Note:** For a complete list of supported versions, see Oracle support.

Logon Manager supports BOSaNOVA emulator. No steps are necessary to set up BOSaNOVA to work with Logon Manager.

> **Note:** There is an open issue with the BOSaNOVA emulator when used with Logon Manager. When closing the emulation, the following warning message appears: "There are active applications connected to the emulation via the HLLAPI/DDE interface. Closing the emulation now may cause unpredictable results. Are you sure?"
>
> If you click **Yes**, Logon Manager stops responding to the BOSaNOVA emulator and you must restart it. Note that the restart may take a few additional seconds. Another workaround for this issue is to shut down Logon Manager before closing the emulation, close the emulation, and then restart Logon Manager.

7.2.4.4 Ericom PowerTerm

> **Note:** For a complete list of supported versions, see Oracle support.

To set up Ericom PowerTerm to work with Logon Manager:

In the emulator:

1. Select **Terminal** from the **Setup** menu.

2. Select the **General** tab.

3. Under HLLAPI Names, set **Short** to a unique value.

4. Click **OK**.

In order to enable Logon Manager support for PowerTerm InterConnect, Plus, and Lite editions, the complete and exact path to the emulator must be specified in the Agent's host/mainframe-configuration file, MfrmList.ini. The default path in the mainframe configuration is `C:\Program Files\Ericom Software\PowerTerm`.

If one of these editions of the PowerTerm emulator is installed in any other directory or on any other drive, you must modify this default path in `MfrmList.ini`. This file can only be edited using the Administrative Console.

1. On the **Tools** menu, point to **Modify Configuration**, then click **MfrmList**.

2. In the INI editor, select **Ericom PowerTerm Lite/Plus/InterConnect** from the **Section** dropdown list.

3. For **ValueName=** edit the path to the emulator as needed.

4. Click **Save** (click **OK** to restart the Agent if prompted), then **Close**.

7.2.4.5 G&R Glink

> **Note:** For a complete list of supported versions, see Oracle support.

To set up G&R Glink to work with Logon Manager:

Configure short names in the `glHLLAPI.ini` file, which is found in the `GLWin\WHLLAPI` directory within the G&R Glink installation path. This file must be copied to the user's `%WinDir%` directory to take effect. Oracle recommends that the default values be left as they are, except for those values that refer to the short names, which take the form of:

```
A]Name=HLLAPI long nameConfig=config file name
```

where *A* represents the short name.

7.2.4.6 Hummingbird Host Explorer

> **Note:** For a complete list of supported versions, see Oracle support.

To set up Hummingbird Host Explorer to work with Logon Manager:

In the emulator:

1. Select **API Settings** from the **Options** menu.
2. Under **HLLAPI Options**, select **Update screen after PS update**.
3. Under **EHLLAPI Compatibility**, select **Attachmate**.
4. Click **OK**.

7.2.4.7 IBM Client Access

> **Note:** For a complete list of supported versions, see Oracle support.

Logon Manager supports IBM Client Access. No steps are necessary to set up IBM Client Access to work with Logon Manager.

7.2.4.8 IBM Client Access Express

> **Note:** For a complete list of supported versions, see Oracle support.

Logon Manager supports IBM Client Access Express. No steps are necessary to set up IBM Client Access Express to work with Logon Manager.

7.2.4.9 IBM Host On-Demand

> **Note:** For a complete list of supported versions, see Oracle support.

Logon Manager support for IBM Host On-Demand is tested with Microsoft Windows, Microsoft Internet Explorer or Mozilla Firefox, and the updated JVM (Java Virtual Machine). If Microsoft Internet Explorer is installed, the JVM should not have to be updated.

One issue with these methods is that clients might not be able to save configured sessions, and entering the auto-start name each time a session is used is quite tedious. Alternatively, administrators can replicate the existing sessions that are available to the client, and HLLAPI-enable these sessions as explained below. Clients can then be offered both standard and HLLAPI-enabled sessions.

To set up IBM Host On-Demand to work with Logon Manager:

In Microsoft Internet Explorer or Mozilla Firefox:

1. Launch the browser.

2. Go to IBM FixCentral and download the Host On-Demand EHLLAPI Bridge Download for the particular version of IBM Host On-Demand.

3. Unzip the downloaded file to the Logon Manager installation directory.

4. Install `Ehllapibridge.exe`.

5. Select **Internet Options** from the **Tools** menu.

6. Select the **Advanced** tab.

7. Under **Microsoft VM**, select **Java console enabled** (requires restart).

8. Click **Apply**, then **OK**. If necessary, exit the browser.

9. Restart the computer.

In Host On-Demand:

1. Configure each individual session to run the HLLAPI enabler through the Host On-Demand applet.

2. Select **Properties** from the menu.

3. Select the **Advanced** tab.

4. Select **Applet** from the Auto-Start drop-down list box.

5. Enter `com.ibm.eNetwork.hllbridge.HLLAPIEnabler` in the **Name** text box.

6. Enter `ENABLE_PCSAPI=YES` in the **Parameter (Optional)** text box.

7. Select **Yes** in the **Auto-start HLLAPI Enabler** check-box.

8. Alternatively, run this applet after the session starts by selecting **Assist**, then **Run applet**.

7.2.4.10 IBM Personal Communications

> **Note:** For a complete list of supported versions, see Oracle support.

To set up IBM Personal Communications to work with Logon Manager:

1. From the **Edit** menu in the emulator, point to **Preferences** and select **API Settings**.

2. Select the **DDE/EHLLAPI** checkbox.

3. Click **OK**.

7.2.4.11 Jolly Giant QWS3270 PLUS

> **Note:** For a complete list of supported versions, see Oracle support.

Logon Manager supports Jolly Giant QWS3270 PLUS emulator. No steps are necessary to set up Jolly Giant QWS3270 PLUS to work with Logon Manager.

7.2.4.12 NetManage Rumba

> **Note:** For a complete list of supported versions, see Oracle support.

Setting Up NetManage Rumba in the Emulator

1. Select **API** from the **Options** menu.

2. Select the **Identification** tab.

3. Set the **Session Short Name**.

4. Click **OK**.

> **Note:** NetManage Rumba appears to have an incomplete implementation of HLLAPI. NetManage Rumba connects and sees the Presentation Space (emulator screen), but it does not appear to support connections for more than one session. Logon Manager can only provide single sign-on support to the last session started.

7.2.4.13 Net Soft NS/Elite

> **Note:** For a complete list of supported versions, see Oracle support.

Logon Manager supports Net Soft NS/Elite. No steps are necessary to setup NS/Elite to work with Logon Manager.

7.2.4.14 Newhart Systems BLUES 2000

> **Note:** For a complete list of supported versions, see Oracle support.

Logon Manager supports Newhart Systems BLUES 2000 emulator. No steps are necessary to set up Newhart Systems BLUES 2000 to work with Logon Manager.

7.2.4.15 Novell LAN Workplace

> **Note:** For a complete list of supported versions, see Oracle support.

In order to enable Logon Manager support for Novell LAN Workplace Pro, the complete and exact path to the emulator must be specified in the Agent's host/mainframe-configuration file, `MfrmList.ini`. The default path in the mainframe configuration is `c:\Program Files\Novell\LAN Workplace\Terminals\Bin`.

If the Novell LAN Workplace emulator is installed in any other directory or on any other drive, you must modify this default path in `MfrmList.ini`. This file can only be edited using the Administrative Console.

1. On the **Tools** menu, point to **Modify Configuration**, then click **MfrmList**.

2. In the INI editor, select Novell LAN Workplace Pro 5.2 from the **Section** dropdown list.

3. For **ValueName=** edit the path to the emulator as needed.

4. Click **Save** (click **OK** to restart the Agent if prompted), then **Close**.

7.2.4.16 PuTTY

> **Note:** For a complete list of supported versions, see Oracle support.

Due to the way PuTTY and support for PuTTY in Logon Manager have been designed, you must keep the following information in mind when creating templates for applications accessed via PuTTY:

> **Note:** Use PuTTY's **Copy All to Clipboard** feature when creating a PuTTY-based template.

- **PuTTY Treats Fixed-Screen Applications as Scrolling-Screen**

  Because PuTTY treats all applications as scrolling-screen, you must create scrolling-screen templates even if the application in question is fixed-screen.

- **PuTTY Does Not Support Detection or Setting of Cursor Position**

  Because PuTTY cannot detect or set the cursor position, you must do the following when creating templates:

  - Fixed-screen applications. Configure the template to manually position the cursor into the target row and column by sending appropriate keyboard characters such as tabs and spaces.

  - Scrolling-screen applications. Configure the template with the assumption that the cursor is always positioned after the last character on the last line of the screen, plus a separating space.

- **Screen Updates in PuTTY Are Not Immediate**

  Because PuTTY does not update its screen display immediately due to host echo (text entered is first sent to the server then returned back to the terminal and displayed), it is necessary to add delays when switching fields and/or submitting the credentials, depending on the latency of the echo. If you need to delay the "Submit" action, you must disable the "Auto Submit" feature.

7.2.4.17 Scanpak Aviva for Desktops

> **Note:** For a complete list of supported versions, see Oracle support.

Logon Manager supports Scanpak Aviva for Desktops (formerly Eicon Aviva). To set up Scanpak Aviva for Desktops to work with Logon Manager:

In the emulator:

1. Select **Settings**, then **Properties** from the menu.

2. Select **Automation**.

3. Ensure the **Choose first available short name** checkbox is selected.

> **Note:** Only the session and destination parameters must be configured.

7.2.4.18 Seagull BlueZone

> **Note:** For a complete list of supported versions, see Oracle support.

Logon Manager supports Seagull BlueZone. No setup steps are necessary.

7.2.4.19 WRQ Reflection

> **Note:** For a complete list of supported versions, see Oracle support.

To set up WRQ Reflection to work with Logon Manager:

In the emulator:

1. Select **Setup**, then **Terminal** from the menu.

2. Set the HLLAPI names for Short and Long. (Short must be unique, Long can be anything the program permits.)

3. Click **OK**.

7.2.4.20 Zephyr PC to Host

> **Note:** For a complete list of supported versions, see Oracle support.

To set up Passport to work with Logon Manager:

In the emulator:

1. Select **Communication**, then **Setup** from the menu.

2. Select HLLAPI. If **Automatically Select** is checked there are no additional steps necessary. If **Manually Specif**y is checked, you must select either a Short Name or Long Name.

7.2.4.21 Zephyr Web to Host

> **Note:** For a complete list of supported versions, see Oracle support.

Logon Manager supports Passport Web to Host. No steps are necessary to setup Web to Host to work with Logon Manager.

7.2.5 SAP Configuration

Logon Manager supports SAP applications. In order for Logon Manager to work with SAP applications, scripting must be turned on. (Note that in your environment, scripting may be turned off by default.) The following configuration changes must be made to all SAP desktops that will run Logon Manager. If these configuration changes are not made, end users will receive an SAP error unless Logon Manager is shut down.

To set up SAP to work with Logon Manager:

1. Configure the Client.

    a. Open the SAP Client and log on (SAPGUI Front End).

    b. On the **SAP Easy Access** screen, open the **Options** dialog. (Click **Alt F12** or select **Customizing of local layout** from the **Standard Toolbar** on any SAP screen).

    c. Select the **Scripting** tab.

    d. Under **User Settings**, make sure that **Enable Scripting** is checked and that **Notify when a script attaches to a running GUI** is not checked.

    e. Click **Apply**.

2. Configure the Server

    a. Open the SAP Application Server.

    b. Start transaction RZ11.

    c. On the **Maintain Profile Parameters** screen, in the Param. Name, enter `sapgui/user_scripting` and click **Display**.

    d. On the **Display Profile Parameter Attributes** screen, select **Change Value** from the **Application Toolbar**.

    e. On the **Change Parameter Value** screen, enter **TRUE** in the **New Value** field.

    f. Click **Save** (lower left hand corner).

3. Edit the Registry

    a. Open the Registry.

    b. Drill down to `HKCU\software\SAP\SAPGUI Front\SAP Frontend Server\Security:WarnOnAttach`.

    c. Set the `WarnOnAttach` value to zero (0).

    d. Push out this change to all desktops that will use SAP applications with Logon Manager.

> **Note:** The SAP Helper must be present for this process. Run the Logon Manager Agent Installer, select **Advanced Setup**, expand the **Extensions** tree and drill down to Logon Manager. Select **SAP Helper** and choose **This Feature will be installed on the local hard drive**. Select **Next** and follow the onscreen instructions to complete the installation.

7.2.5.1 Border Values for Web Logon Credential Fields

Values for Feedback Color follow the standard for the border attribute in cascading style sheets (CSS). The table below lists valid colors and their RGB values. See Section 2.17.3.4, "Web Application Response" for the Feedback Color setting in which these values are used.

Attribute	Possible Values
Width	■ Thin
	■ Medium
	■ Thick
	■ A unit of pixels, inches, etc (examples: 3px.).

Attribute	Possible Values
Style	■ none
	■ dotted
	■ dashed
	■ solid
	■ double
	■ groove
	■ ridge
	■ inset
	■ outset
Color	A color keyword or RGB value; common examples are listed in the next table.

Keyword	RGB Equivalent	Keyword	RGB equivalent
aqua	#00FFFF	navy	#000080
black	#000000	olive	#808000
blue	#0000FF	purple	#800080
fuchsia	#FF00FF	red	#FF0000
gray	#808080	silver	#C0C0C0
green	#008000	teal	#008080
lime	#00FF00	white	#FFFFFF
maroon	#800000	yellow	#FFFF00

7.2.6 Understanding the Logon Manager Secondary Authentication API

The secondary authentication API allows a third party application to programmatically supply a passphrase to the Windows Authenticator v2 (a.k.a. MSAuth) and LDAP Authenticator v2 (LDAPv2) during an authentication session. This eliminates the need for interaction with the user and automates the authentication process.

The API consists of the following functions:

■ SecondaryAuthKey. Allocates the passphrase answer buffer, fills the buffer with the passphrase answer, and returns a pointer to the answer buffer.

■ Free SecondaryAuthKey. Clears the answer buffer once the answer is no longer needed by third party code.

> **Note:** The custom secondary authentication library must be validated and digitally signed by Oracle; otherwise, it will not be accepted by Logon Manager. For assistance with this process, please contact Oracle Support.

7.2.6.1 The SecondaryAuthKey Method

This method is used to obtain the user's passphrase answer (in our example, the user's directory SID) and store it in memory at a specified address for later retrieval.

```
BOOL SecondaryAuthKey( LPBYTE* pbAnswer, LPDWORD pdwSize ) {
```

```
BOOL fRetVal = FALSE;

// check for invalid parametersif ( NULL != pbAnswer ) {

// obtain user's SID - it will be used as passphrase answer CSid sid;
CString strSid( sid.Sid() );

// allocate the memory buffer LPBYTE pByte = new BYTE[strSid.GetLength() +
1];

// copy the SID to the buffer ::memcpy( pByte, strSid.GetBuffer(),
strSid.GetLength() );

// save the address of the buffer to the passed pointer *pbAnswer = pByte;

// save the size of the buffer to the passed pointerif ( NULL != pdwSize )
{

*pdwSize = strSid.GetLength() + 1;

}

// set successful return code fRetVal = TRUE;

}

return fRetVal;

}
```

7.2.6.2 The FreeSecondaryAuthKey Method

This method is used to clear the passphrase answer buffer after SecondaryAuthKey
has been successfully called.

```
void FreeSecondaryAuthKey( LPBYTE pbAnswer )

{

// free the memory bufferdelete[] pbAnswer;

}
```

7.2.6.3 Driver Code for Testing a Custom Secondary Authenticator

Below is example code for a driver code that will allow you to test your custom
secondary authenticator.

```
BOOL CResetDlg::SecondaryAuth( LPCTSTR pszDllPath ) {

BOOL fRetVal = FALSE;

// load SecondaryAuth.dll HMODULE hSecondaryAuth = LoadLibrary( pszDllPath
);

If ( NULL != hSecondaryAuth ) {

SECONDARYAUTHKEY pfnSecondaryAuthKey = (SECONDARYAUTHKEY) GetProcAddress(
hSecondaryAuth, "SecondaryAuthKey" ); if ( NULL != pfnSecondaryAuthKey ) {

LPBYTE pbByte = NULL; DWORD dwAnswerSize = 0;

// call SecondaryAuthKey to get the passphrase answer BOOL bAnswerResult =
pfnSecondaryAuthKey( &pbByte, &dwAnswerSize );

// use the returned answer - pbByte// ...

// call FreeSecondaryAuthKey to let the library free the memory
FREESECONDARYAUTHKEY pfnFreeSecondaryAuthKey = (FREESECONDARYAUTHKEY)
```

```
GetProcAddress( hSecondaryAuth, "FreeSecondaryAuthKey" ); if ( NULL !=
pfnFreeSecondaryAuthKey ) {

pfnFreeSecondaryAuthKey( pbByte );

}

// set successful return code fRetVal = TRUE;

}

// unload SecondaryAuth.dll FreeLibrary( hSecondaryAuth );

}

return fRetVal;

}
```

7.2.6.4 Switching Secondary Authentication Methods

You have the ability to change the method used by Windows Authenticator v2
(WinAuth v2) or LDAP Authenticator v2 (LDAPAuth v2) to verify the user's identity
to another method if necessary. The following scenarios are supported:

- WinAuth v2/LDAPAuth v2 built-in secondary authentication to external
  secondary authentication

- External secondary authentication to WinAuth v2/LDAPAuth v2 built-in
  secondary authentication

- One external secondary authentication library to another

7.2.6.5 Switching from Built-In Secondary Authentication to External Secondary Authentication

To configure WinAuth v2 for recovery via custom secondary authentication library, do
the following:

1. Start the Administrative Console.

2. In the tree in the left pane, right-click the **Global Agent Settings** node and select
   Import > From Live HKLM from the context menu.

3. Under the **Live** settings set, navigate to **Authentication > Windows v2 or LDAP
   v2**.

   If you have previously configured Logon Manager to use either the user's
   directory SID or a secure random key as a secondary authentication method,
   revert back to interactive passphrase by deselecting the check box next to the
   Recovery Method option. (This reverts the option to its default value, User
   passphrase.)

4. Create a directory named identically to the GUID of your custom library in the
   following directory:

   `<oracle_install_dir>`\v-GO SSO\AUI\Recovery\

   > **Note:** Substitute the full path of the directory in which Oracle
   > Enterprise Single Sign-On products are installed for `<oracle_
   > install_dir>`.

For example, if your library's GUID is
`{B623C4E7-A383-4194-A719-7B17D074A70F}`, you would create the following
directory:

`<oracle_install_dir>\v-GO`
`SSO\AUI\Recovery\{B623C4E7-A383-4194-A719-7B17D074A70F}`

5. Place your custom library file in the directory you created in step 4.

6. Add a GUID entry to the Logon Manager secondary authentication methods list
for your custom library by creating a key named identically to the GUID of your
custom library. Use the following locations:

- On 32-bit systems:

  `HKEY_LOCAL_MACHINE\Software\Passlogix\AUI\MsAuth\RecoveryMethods\`

- On 64-bit systems:

  `HKEY_LOCAL_MACHINE\Software\Wow6432Node\Passlogix\AUI\MsAuth\`
  `RecoveryMethods\`

  For example, if your library's GUID is
  `{B623C4E7-A383-4194-A719-7B17D074A70F}`, you will create the following key
  on a 32-bit system:

  `HKEY_LOCAL_MACHINE\Software\Passlogix\AUI\MsAuth\RecoveryMethods\`
  `{B623C4E7-A383-4194-A719-7B17D074A70F}`

7. Set the Logon Manager recovery method to your custom secondary authentication
library. If it does not already exist, create a string value named
`ResetMethodGUIDunderHKEY_LOCAL_`
`MACHINE\Software\Passlogix\AUI\MsAuth\RecoveryMethods\`and set it to the
GUID of your custom library.

8. Reinitialize the WinAuth v2 settings with the newly selected configuration:

  a. Launch Logon Manager, double-click its system tray icon, and select **Settings**
  in the left-hand pane of the window that appears.

  b. Select the **Authentication** tab, then click **Change**. The **Setup Wizard** appears.

  c. Follow the prompts in the wizard. When prompted to select your primary
  logon method, make sure that Windows Logon v2 or LDAP v2 remains
  selected.

  d. Complete the remaining steps in the wizard.

7.2.6.6 Switching from External Secondary Authentication to Built-In Secondary Authentication

To configure WinAuth v2 or LDAPAuth v2 for recovery via one of Logon Manager's
built-in secondary authentication methods, do the following:

1. Start the Administrative Console.

2. In the tree in the left pane, right-click the **Global Agent Settings** node and select
Import > From Live HKLM from the context menu.

3. Under the **Live** settings set, navigate to **Authentication > Windows v2 or LDAP
v2**.

4. Select the check box next to the **Recovery Method** option and do one of the
following:

- To use the interactive passphrase prompt with a user-supplied passphrase for secondary authentication, select **User passphrase** from the drop-down list

- To use silent secondary authentication using the user's directory SID as the passphrase answer, select **Passphrase suppression using user's SID** from the drop-down list

- To use silent secondary authentication with a secure random key as the passphrase answer, select **Passphrase suppression using secure key** from the drop-down list.

- To use the entryUUID for silent secondary authentication, select P**assphrase suppression using entryUUID** from the drop-down list

5. Save your changes locally or publish them to the repository, as applicable.

6. Reinitialize the WinAuth v2 or LDAP v2 settings with the newly selected configuration:

   a. Launch Logon Manager, double-click its system tray icon, and select **Settings** in the left-hand pane of the window that appears.

   b. Select the **Authentication** tab, then click **Change**. The **Setup Wizard** appears.

   c. Follow the prompts in the wizard. When prompted to select your primary logon method, make sure that Windows Logon v2 or LDAP v2 remains selected.

   d. Complete the remaining steps in the wizard.

7.2.6.7 Switching from One External Secondary Authentication Library to Another

If you are currently using one external secondary authentication library and want to switch to a different external library, repeat the steps in Switching from Built-In Secondary Authentication to External Secondary Authentication.

7.2.7 Configuring Windows Authenticator Version 2

This section describes how to install and configure the Windows Authenticator v2 for each of the secondary authentication methods described earlier in this document. It covers the following topics:

- Migrating a WinAuth v1 Installation to WinAuth v2

- Configuring WinAuth v2 for Authenticator Key Management via Windows DPAPI

- Configuring WinAuth v2 for Recovery via Interactive Passphrase Prompt

- Configuring WinAuth v2 for Recovery via Logon Manager Secondary Authentication API

- Configuring WinAuth v2 for Kiosk Environments

- Resetting the User-Provided Passphrase Answer

> **Note:** The steps in this section illustrate how to manually perform the procedures listed above. If you wish to automate and/or customize any of those processes, see the *Oracle Enterprise Single Sign-On Suite Installation Guide* and/or request the assistance of Oracle Support to develop a deployment plan tailored specifically to your environment.

7.2.7.1 Migrating a WinAuth v1 Installation to WinAuth v2

To manually migrate from an existing WinAuth v1 deployment to WinAuth v2, do the following:

1. Reconfigure the First-Time Use wizard so that WinAuth v2 is the only available logon method:

   a. Start the Administrative Console.

   b. In the tree in the left pane, right-click the **Global Agent Settings** node and select **Import > From Live HKLM** from the context menu.

   c. Under the **Live** settings set, navigate to **User Experience > Setup Wizard**.

   d. Select the check box next to the **Selected Authenticator** option and select **Windows v2** from the drop-down list.

   e. Save your changes locally or publish them to the repository, as applicable.

2. Using a plain text editor, create a batch (`.cmd`) file with the following content:

   ```
   ##Install WinAuth v2

   <esso-lm_installer> /s /v"/qb RUNVGO="YES" ADDLOCAL="MSauth""

   ##Initiate primary logon method change

   "<oracle_install_dir>\v-GO SSO\ssoShell.exe" /shellLoad Themes
   /shellLock
   ```

   > **Note:** Substitute the full path and name of the Logon Manager installer executable in place of `<esso-lm_sso_installer>`, as well as the full path of the directory in which Oracle Enterprise Single Sign-On products are installed for `<oracle_install_dir>`.

3. Save and close the file.

4. Run the file on the target machine.

5. When the FTU wizard appears, follow the displayed instructions to complete the migration process.

7.2.7.2 Configuring WinAuth v2 for Authenticator Key Management via Windows DPAPI

To configure WinAuth v2 for authenticator key management via Windows DPAPI, complete the steps below.

> **Note:** This procedure assumes WinAuth v2 has already been installed and configured to work with your Logon Manager deployment.

Before you begin, ensure that your environment meets the following minimum software requirements in order for secondary authentication via Windows DPAPI to function:

- Domain controllers: Windows Server 2008 and above.
- Client machines running Logon Manager:
    - Windows Server 2008 and above

- – Windows Server 2012

- – Windows 7

- – Windows 8

> **Note:** Windows Server 2008 requires KB907247: Credential Roaming Software Update.

The following Microsoft Developer Network and TechNet articles provide detailed information on Windows DPAPI and credential roaming:

- Windows Data Protection:
  http://msdn.microsoft.com/en-us/library/ms995355.aspx

- Credential Roaming:
  http://technet.microsoft.com/en-us/library/cc700815.aspx

If your environment meets the listed minimum requirements, configure WinAuth v2 to use Windows DPAPI as the secondary authentication method as follows:

1. Start the Administrative Console.

2. In the tree in the left pane, right-click the **Global Agent Settings** node and select **Import > From Live HKLM** from the context menu.

3. Under the **Live** settings set, navigate to **Authentication > Windows v2.**

4. If you have previously configured Logon Manager to use either the user's directory SID or a secure random key as a secondary authentication method, revert back to interactive passphrase by deselecting the check box next to the **Recovery Method** option. (This reverts the option to its default value, **User passphrase**.)

5. Enable Windows DPAPI for WinAuth v2. Select the check box next to the **Use Windows Data Protection (DPAPI)** option, then select **Yes** from the drop-down list.

6. Save your changes by publishing them to the repository.

7. Test your configuration. The tests below ensure proper configuration of Logon Manager and your environment to handle credential roaming, password changes, and keyset rotation:

   a. Enroll a new user with Logon Manager by completing the First Time Use (FTU) wizard; during enrollment, Logon Manager will prompt for the user name and password but should not prompt to select a passphrase answer.

   b. Enroll an application with Logon Manager and store a set of credentials for the application.

   c. Close and re-open the application. Logon Manager should automatically respond and log you on to the application without prompting for a passphrase answer.

   d. Log out of the machine and log on to another machine as the same user. Logon Manager should behave exactly as on the original machine, without prompting for a passphrase answer or any other extraneous information.

   e. Use the **Log on using Logon Manager** option (accessed by right-clicking the Logon Manager system tray icon) to confirm that application response functions as desired.

f. Open the properties dialog for the application within the Agent and use the **Reveal Password** option to reveal the stored password. There should be no prompt for the passphrase answer.

g. Change the user's Windows password before the Agent is launched, and then again while the Agent is running. There should be no prompt for the passphrase answer; stored credential should remain accessible.

h. Log on to a third machine and confirm that stored credentials remain accessible.

i. Test that the 90-day keyset rotation enforced by Windows DPAPI functions correctly. Advance the machine's clock, as well as the domain controller's clock, by 120 days, then log on to at least two different machines and confirm that the stored credentials remain accessible.

7.2.7.3 Configuring WinAuth v2 for Recovery via Interactive Passphrase Prompt

To configure WinAuth v2 for authenticator key recovery via interactive passphrase prompt, simply install WinAuth v2 as described in Migrating a WinAuth v1 Installation to WinAuth v2. The **Recovery Method** option in the Console defaults to **User passphrase unless manually changed**.

> **Note:** This procedure assumes WinAuth v2 has already been installed and configured to work with your Logon Manager deployment.

1. Start the Administrative Console.

2. In the tree in the left pane, right-click the **Global Agent Settings** node and select **Import > From Live HKLM** from the context menu.

3. Under the **Live** settings set, navigate to **Authentication > Windows v2**.

4. If you have previously configured Logon Manager to use either the user's directory SID or a secure random key as a secondary authentication method, revert back to interactive passphrase by deselecting the check box next to the **Recovery Method** option. (This reverts the option to its default value, **User passphrase**.)

5. Configure the user warning that appears during recovery. This warning should emphasize the importance of remembering the passphrase answer:

a. Under the **Live** settings, navigate to **Authentication > Windows v2 > Passphrase**.

b. Select the check box next to the **Message** option and enter a message explaining the importance of remembering the passphrase answer to the user. (When filling in the fields in the steps below, use the \n character sequence to indicate a line break.)

This message appears during enrollment and requires the user to check a check box and click the **OK** button in order to continue.

c. Select the check box next to the **Message Dialog Title** option and enter the desired window title for the dialog.

d. Select the check box next to the **Checkbox Label** option and enter the desired label for the check box that appears in the dialog.

e. Select the check box next to the **Reset with old password** option and select **Yes** from the drop-down list. This option allows the user to recover access to their credential store using the old (most recent) password.

f. Ensure that the check box next to the **Force password re-enrollment when using old password to reset** option is not selected (i.e., option is at its default value of **Yes**).

This setting forces Logon Manager to re-enroll the user when the **Reset with old password** option is in effect, and the user has used the old (most recent) password as the passphrase answer during recovery.

For example, if you configure the warning as follows:
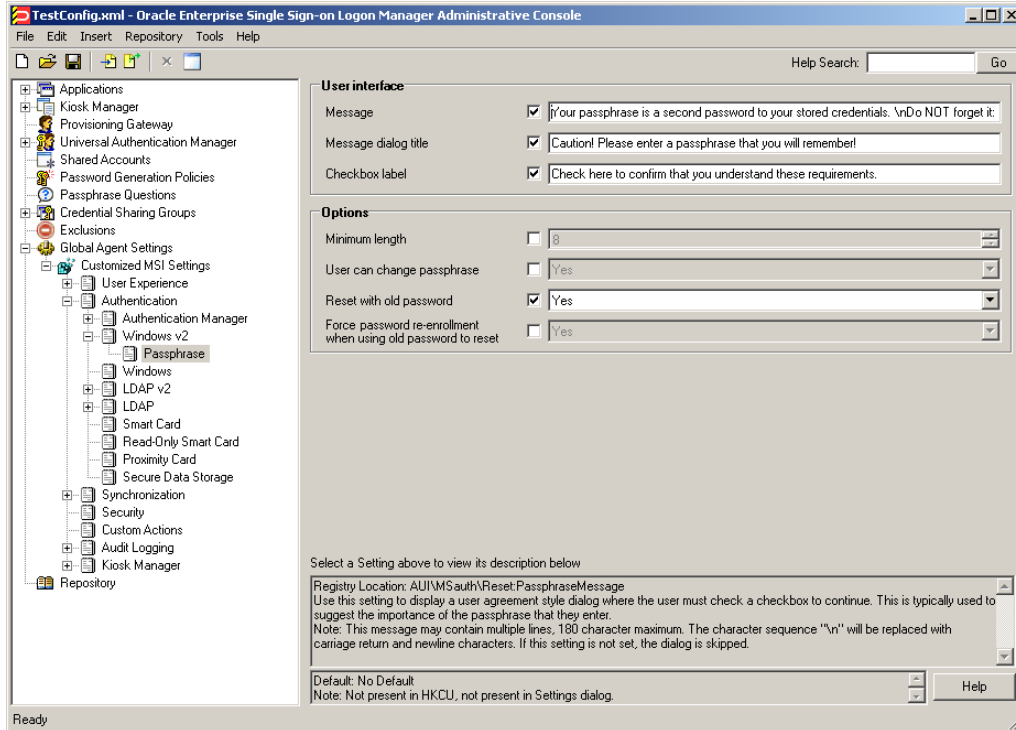
It will appear as follows when the user is prompted for the passphrase answer during recovery:

6. Save your changes locally or publish them to your repository, as appropriate.

7.2.7.4 Configuring WinAuth v2 for Recovery via Logon Manager Secondary Authentication API

To configure WinAuth v2 for recovery via the Logon Manager secondary authentication API, complete the instructions in one of the following sections.

- Recovery via Custom Secondary Authentication Library

- Recovery via a Built-In Silent Secondary Authentication Method

7.2.7.4.1 Recovery via Custom Secondary Authentication Library Before starting this procedure, make sure you have done the following:

- Written your custom secondary authentication library according to the section Understanding the Logon Manager Secondary Authentication API.

- Ascertained your custom library's GUID and made sure that library returns that GUID to Logon Manager via its `GetID` method.

- Submitted your custom library file to Oracle to obtain a digital signature and received a digitally signed copy of the file back from Oracle. Logon Manager will not load the custom file without a valid digital signature.

To configure WinAuth v2 for recovery via custom secondary authentication library, do the following:

1. Start the Administrative Console.

2. In the tree in the left pane, right-click the **Global Agent Settings** node and select **Import > From Live HKLM** from the context menu.

3. Under the **Live** settings set, navigate to **Authentication > Windows v2**.

   If you have previously configured Logon Manager to use either the user's directory SID or a secure random key as a secondary authentication method, revert back to interactive passphrase by deselecting the check box next to the **Recovery Method** option. (This reverts the option to its default value, **User passphrase.**)

4. Create a directory named identically to the GUID of your custom library in the following directory:

   `<oracle_install_dir>``\v-GO SSO\AUI\Recovery\`

   Note: Substitute the full path of the directory in which Oracle Enterprise Single Sign-On products are installed for *`<oracle_install_dir>`*.

   For example, if your library's GUID is `{B623C4E7-A383-4194-A719-7B17D074A70F}`, you would create the following directory:

   ```
   <oracle_install_dir>\v-GO SSO\AUI\Recovery\
   {B623C4E7-A383-4194-A719-7B17D074A70F}
   ```

5. Place your custom library file in the directory you created in step 4.

6. Add a GUID entry to the Logon Manager secondary authentication methods list for your custom library by creating a key named identically to the GUID of your custom library. Use the following locations:.

   - On 32-bit systems:

```
HKEY_LOCAL_MACHINE\Software\Passlogix\AUI\MSAuth\ResetMethods\
```

- On 64-bit systems:

```
HKEY_LOCAL_MACHINE\Software\
Wow6432Node\Passlogix\AUI\MSAuth\ResetMethods\
```

For example, if your library's GUID is `{B623C4E7-A383-4194-A719-7B17D074A70F}`, you will create the following key on a 32-bit system:

```
HKEY_LOCAL_MACHINE\Software\Passlogix\
AUI\MSAuth\ResetMethods\{B623C4E7-A383-4194-A719-7B17D074A70F}
```

7. Under the key you created in step 6a, create a string value named Path and set it to the full path and file name of your custom library. In our example, you would set it to:

```
<oracle_install_dir>\v-GO SSO\AUI\Recovery\
{B623C4E7-A383-4194-A719-7B17D074A70F}\<MyCustomLibrary.dll>
```

Where <oracle_install_dir> is the full path of the directory in which Oracle Enterprise Single Sign-On products are installed and `<MyCustomLibrary.dll>` is the file name of your custom library.

8. Set Logon Manager's recovery method to your custom secondary authentication library.

If it does not already exist, create a string value named ResetMethodGUID under `HKEY_LOCAL_MACHINE\Software\Passlogix\AUI\MSAuth\ResetMethods\` and set it to the GUID of your custom library.

9. Reinitialize the WinAuth v2 settings with the newly selected configuration:

    a. Launch Logon Manager, double-click its system tray icon, and select Settings in the left-hand pane of the window that appears.

    b. Select the **Authentication** tab, then click **Change**. The Setup Wizard appears.

    c. Follow the prompts in the wizard. When prompted to select your primary logon method, make sure that **Windows Logon v2** remains selected.

    d. Complete the remaining steps in the wizard.

7.2.7.4.2 Recovery via a Built-In Silent Secondary Authentication Method To configure WinAuth v2 for recovery via one of Logon Manager's built in silent secondary authentication methods, do the following:

1. Start the Administrative Console.

2. In the tree in the left pane, right-click the **Global Agent Settings** node and select **Import > From Live HKLM** from the context menu.

3. Under the **Live** settings set, navigate to **Authentication > Windows v2**.

4. Select the check box next to the **Recovery Method** option and do one of the following:

    - To use the user's directory SID for silent secondary authentication, select **Passphrase suppression using user's SID** from the drop-down list

    - To use a secure random key for silent secondary authentication, select **Passphrase suppression using secure key** from the drop-down list

5. Save your changes locally or publish them to the repository, as applicable.

7.2.7.5 Configuring WinAuth v2 for Kiosk Environments

If you are configuring a Kiosk Manager environment to use WinAuth v2 for authentication, only the secondary authentication methods shipped with WinAuth v2 are supported; custom secondary authentication libraries are not supported.

To configure WinAuth v2 for a Kiosk Manager environment, the following options must be configured in addition to those already described in this section:

- The **Delete Local Cache** option (located under **Global Agent Settings** > *[target settings set]* **> Synchronization** must be set to **Yes**.'

- For Active Directory deployments, the **Credentials to Use** option (located under **Global Agent Settings** > *[target settings set]* **> Synchronization** must be set to **Use Active Directory Server Account**.

- For AD LDS (ADAM) deployments, the **Credentials to Use** option (located under **Global Agent Settings** > *[target settings set]* **> Synchronization** must be set to **Use AD LDS (ADAM) Server Account.**

- The **Prefill Username/ID on FTU** option (under **Global Agent Settings** > **Windows Authenticator v2** > **User interface**) must be set to **No**. This prevents the username/ID field from being populated with the previous user's name during FTU.

7.2.7.6 Resetting the User-Provided Passphrase Answer

To force a user to provide a new passphrase answer based on new passphrase questions, do the following as a user with administrative privileges:

1. Using the Administrative Console, do the following:

   a. Disable existing questions that are no longer desired.

   b. Add the new questions.

2. For each user, perform the following steps on the target machine as the target user:

   a. Delete the following registry key and its contents:

      ```
      HKEY_CURRENT_USER\Software\Passlogix\AUI\MSauth\Reset
      ```

   b. Execute the following command:

      ```
      <oracle_install_dir>\v-GO SSO\ssoshell.exe /forceverify now
      ```

      Note: Substitute the full path of the directory in which Oracle Enterprise Single Sign-On products are installed for `<oracle_install_dir>`.

When automating the above steps, Oracle highly recommends that you:

- Create a script to manage the process

- Provide end-user instructions that explain what is happening

- Include a logging capability that centrally records the success or failure of each step, including:

  – Script launch

  – Old registry key deletion

  – New registry key creation

–   Passphrase answer entry by user

■   Include reporting capability to audit recorded data for users who have successfully completed passphrase answer change

■   Once all users have completed the change, delete the unwanted passphrase questions.

7.2.7.7 Enabling WinAuth v2 Strong Authentication Device Support

> **Note:** The following instructions apply to Windows 7 and Windows 8 only.

If you are planning to use strong authentication devices, such as Smart Cards, to authenticate to Windows, you must configure Windows to permit the hand-off of strong authentication events to third-party credential providers, such as Logon Manager deployed with WinAuth v2. Otherwise, Logon Manager will not be able to communicate with the device and you will not be able to authenticate to Logon Manager.

To do so, complete the following steps:

1. Launch the Windows registry editor and navigate to the following path:

    ```
    HKEY_LOCAL_MACHINE\Software\Microsoft\
    WindowsNT\CurrentVersion\Winlogon\Notify
    ```

2. Under the above key, create a `DWORD` value named `SmartCardLogonNotify`.

3. Set the above value to `1`.

4. Restart the machine.

7.2.8 Configuring LDAP Authenticator Version 2

This section describes how to install and configure the LDAP Authenticator v2 for each of the secondary authentication methods described earlier in this document. It covers the following topics:

■   Migrating an LDAPAuth v1 Installation to LDAPAuth v2

■   Configuring LDAPAuth v2 for Recovery via Interactive Passphrase Prompt

■   Configuring LDAPAuth v2 for Recovery via Logon Manager Secondary Authentication API

■   Resetting the User-Provided Passphrase Answer

> **Note:** The steps in this section illustrate how to manually perform the procedures listed above. If you wish to automate and/or customize any of those processes, see the Oracle Enterprise Single Sign-On Suite Installation Guide and/or request the assistance of Oracle Support to develop a deployment plan tailored specifically to your environment.

7.2.8.1 Migrating an LDAPAuth v1 Installation to LDAPAuth v2

To manually migrate from an existing LDAPAuth v1 deployment to LDAPAuth v2, do the following:

1. Reconfigure the First-Time Use wizard so that LDAPAuth v2 is the only available logon method:

    a. Start the Administrative Console.

    b. In the tree in the left pane, right-click the **Global Agent Settings** node and select **Import > From Live HKLM** from the context menu.

    c. Under the "Live" settings set, navigate to **User Experience > Setup Wizard**.

    d. Select the check box next to the Selected Authenticator option and select **LDAP v2** from the drop-down list.

    e. Save your changes locally or publish them to the repository, as applicable.

2. Using a plain text editor, create a batch (`.cmd`) file with the following content:

    ```
    ##Install LDAPAuth v2

    <esso-lm_installer> /s /v"/qb RUNVGO="YES" ADDLOCAL="LDAPAuth""

    ##Initiate primary logon method change

    "<oracle_install_dir>\v-GO SSO\ssoShell.exe" /shellLoad Themes
    /shellLock
    ```

    > **Note:** Substitute the full path and name of the Logon Manager installer executable in place of `<esso-lm_sso_installer>`, as well as the full path of the directory in which Oracle Enterprise Single Sign-On products are installed for `<oracle_install_dir>`.

3. Save and close the file.

4. Run the file on the target machine.

5. When the FTU wizard appears, follow the displayed instructions to complete the migration process.

7.2.8.2 Configuring LDAPAuth v2 for Recovery via Interactive Passphrase Prompt

To configure LDAPAuth v2 for authenticator key recovery via interactive passphrase prompt, simply install LDAPAuth v2. The "Recovery Method" option in the Console defaults to **User passphrase** unless manually changed.

> **Note:** This procedure assumes LDAPAuth v2 has already been installed and configured to work with your Logon Manager deployment.

1. Start the Administrative Console.

2. In the tree in the left pane, right-click the **Global Agent Settings** node and select **Import > From Live HKLM** from the context menu.

3. Under the **Live** settings set, navigate to **Authentication > LDAP v2**.

4. If you have previously configured Logon Manager to use either the user's directory SID, secure key, or entryUUID as a secondary authentication method, revert back to interactive passphrase by deselecting the check box next to the **Recovery Method** option. (This reverts the option to its default value, **User passphrase**.)

5. Save your changes locally or publish them to your repository, as appropriate.

7.2.8.3 Configuring LDAPAuth v2 for Recovery via Logon Manager Secondary Authentication API

To configure LDAPAuth v2 for recovery via the Logon Manager secondary authentication API, complete the instructions in one of the following sections.

- Recovery via Custom Secondary Authentication Library

- Recovery via a Built-In Silent Secondary Authentication Method

7.2.8.3.1 Recovery via Custom Secondary Authentication Library Before starting this procedure, make sure you have done the following:

- Written your custom secondary authentication library according to the section "Understanding the Logon Manager Secondary Authentication API" in the *Oracle Enterprise Single Sign-On Suite Administrator's Guide*.

- Ascertained your custom library's GUID and made sure that library returns that GUID to Logon Manager via its `GetIDmethod`.

- Submitted your custom library file to Oracle to obtain a digital signature and received a digitally signed copy of the file back from Oracle. Logon Manager will not load the custom file without a valid digital signature.

To configure LDAPAuth v2 for recovery via custom secondary authentication library, do the following:

1. Start the Administrative Console.

2. In the tree in the left pane, right-click the **Global Agent Settings** node and select **Import > From Live HKLM** from the context menu.

3. Under the **Live** settings set, navigate to **Authentication > LDAP v2**.

   If you have previously configured Logon Manager to use either the user's directory SID, secure key, or entryUUID as a secondary authentication method, revert back to interactive passphrase by deselecting the check box next to the **Recovery Method** option. (This reverts the option to its default value, **User passphrase**.)

4. Create a directory named identically to the GUID of your custom library in the following directory:

   ```
   <oracle_install_dir>\v-GO SSO\AUI\Recovery\
   ```

   > **Note:** Substitute the full path of the directory in which Oracle Enterprise Single Sign-On products are installed for `<oracle_install_dir>`.

   For example, if your library's GUID is `{B623C4E7-A383-4194-A719-7B17D074A70F}`, you would create the following directory:

   ```
   <oracle_install_dir>\v-GO
   SSO\AUI\Recovery\{B623C4E7-A383-4194-A719-7B17D074A70F}
   ```

5. Place your custom library file in the directory you created in step 4.

6. Add a GUID entry to the Logon Manager secondary authentication methods list for your custom library by creating a key named identically to the GUID of your custom library. Use the following locations:.

   ■ On 32-bit systems:

   `HKEY_LOCAL_MACHINE\Software\Passlogix\AUI\LDAPAuth\ResetMethods\`

   ■ On 64-bit systems:

   `HKEY_LOCAL_MACHINE\`
   `Software\Wow6432Node\Passlogix\AUI\LDAPAuth\ResetMethods\`

   For example, if your library's GUID is`{B623C4E7-A383-4194-A719-7B17D074A70F}`, you will create the following key on a 32-bit system:

   `HKEY_LOCAL_MACHINE\Software\Passlogix\`
   `AUI\LDAPAuth\ResetMethods\{B623C4E7-A383-4194-A719-7B17D074A70F}`

7. Under the key you created in step 6a, create a string value named `Path` and set it to the full path and file name of your custom library. In our example, you would set it to:

   `<oracle_install_dir>\v-GO SSO\AUI\Recovery\`
   `{B623C4E7-A383-4194-A719-7B17D074A70F}\<MyCustomLibrary.dll>`

   Where `<oracle_install_dir>` is the full path of the directory in which Oracle Enterprise Single Sign-On products are installed and `<MyCustomLibrary.dll>` is the file name of your custom library.

8. Set Logon Manager's recovery method to your custom secondary authentication library.

   If it does not already exist, create a string value named `ResetMethodGUID` under `HKEY_LOCAL_MACHINE\Software\Passlogix\AUI\LDAPAuth\ResetMethods\` and set it to the GUID of your custom library.

9. Reinitialize the LDAP v2 settings with the newly selected configuration:

   a. Launch Logon Manager, double-click its system tray icon, and select **Settings** in the left-hand pane of the window that appears.

   b. Select the **Authentication** tab, then click **Change**. The Setup Wizard appears.

   c. Follow the prompts in the wizard. When prompted to select your primary logon method, make sure that LDAP v2 remains selected.

   d. Complete the remaining steps in the wizard.

7.2.8.3.2   Recovery via a Built-In Silent Secondary Authentication Method To configure LDAP v2 for recovery via one of Logon Manager's built in silent secondary authentication methods, do the following:

1. Start the Administrative Console.

2. In the tree in the left pane, right-click the **Global Agent Settings** node and select **Import > From Live HKLM** from the context menu.

3. Under the **Live** settings set, navigate to **Authentication > LDAP v2**.

4. Select the check box next to the **Recovery Method** option and do one of the following:

   ■ To use the user's directory SID for silent secondary authentication, select **Passphrase suppression using user's SID** from the drop-down list

- To use a random secure key for silent secondary authentication, select P**assphrase suppression using secure key** from the drop-down list

- To use the user's entryUUID for silent secondary authentication, select **Passphrase suppression using entryUUID** from the drop-down list

5. Save your changes locally or publish them to the repository, as applicable.

7.2.8.4 Resetting the User-Provided Passphrase Answer

To force a user to provide a new passphrase answer based on new passphrase questions, do the following as a user with administrative privileges:

1. Using the Administrative Console, do the following:

   a. Disable existing questions that are no longer desired.

   b. Add the new questions.

2. For each user, perform the following steps on the target machine as the target user:

   a. Delete the following registry key and its contents:

   ```
   HKEY_CURRENT_USER\Software\Passlogix\AUI\LDAPauth\Reset
   ```

   b. Execute the following command:

   ```
   <oracle_install_dir>\v-GO SSO\ssoshell.exe /forceverify now
   ```

   > **Note:** Substitute the full path of the directory in which Oracle Enterprise Single Sign-On products are installed for *<oracle_install_dir>*.

When automating the above steps, Oracle highly recommends that you:

- Create a script to manage the process

- Provide end-user instructions that explain what is happening

- Include a logging capability that centrally records the success or failure of each step, including:

  - Script launch

  - Old registry key deletion

  - New registry key creation

  - Passphrase answer entry by user

- Include reporting capability to audit recorded data for users who have successfully completed passphrase answer change

- Once all users have completed the change, delete the unwanted passphrase questions.

7.2.8.5 Enabling LDAPAuth v2 Strong Authentication Device Support

> **Note:** The following instructions apply to Windows 7 and Windows 8 only.

If you are planning to use strong authentication devices, such as Smart Cards, to authenticate to Windows, you must configure Windows to permit the hand-off of strong authentication events to third-party credential providers, such as Logon Manager deployed with LDAPAuth v2. Otherwise, Logon Manager will not be able to communicate with the device and you will not be able to authenticate to Logon Manager.

To do so, complete the following steps:

1. Launch the Windows registry editor and navigate to the following path:

   `HKEY_LOCAL_MACHINE\Software\Microsoft\`
   `WindowsNT\CurrentVersion\Winlogon\Notify`

2. Under the above key, create a `DWORD` value named `SmartCardLogonNotify`.

3. Set the above value to `1`.

4. Restart the machine.

7.2.9 Smart Card Monitor Utility (ssoSCDetect.exe)

The utility program ssoSCDetect monitors a workstation's smart card reader, making it possible to use the workstation as a multiple-user "kiosk" that can access and synchronize the remote SSO credential store of any user authenticated by a smart card.

When a user inserts a card into the reader, the ssoSCDetect utility starts the Agent and prompts for the user's primary logon credentials. It then synchronizes the user's credentials with the remote repository. When the user logs out of the workstation (for example, by removing the card from the reader), ssoSCDetect shuts down the Agent.

To run the utility, copy the executable file ssoSCDetect.exe from the Utilities directory of the Logon Manager CD to the installation directory (`%ProgramFiles%/Passlogix/v-GO SSO`) then launch the program.

7.2.10 Global Agent Settings

Various functions and behaviors of Logon Manager can be centrally defined by using the Settings dialog, setting Windows registry settings on the local workstation, and specifying administrative overrides via a Synchronizer extension.

> **Note:** Configure these settings in the Administrative Console. The table is provided only for reference.

Registry settings can be set by the Agent, by the Administrative Console, with the RegEdit Windows utility, and via a centrally managed software distribution mechanism. Registry settings are located in the following Windows Registry locations:

- `HKLM\...\` for computer-specific settings

- `HKCU\...\` for user-specific settings

Administrative override objects from Synchronizer extensions specify settings that override `HKLM\...\` Windows Registry settings, which in turn overrides the `HKCU\...\` Windows Registry settings.

The following table lists examples of settings and their override locations.

Setting	Sample Location
Synchronizer extension object overrides	`Extensions\AccessManager:MFEnable=DWORD:0`
Computer-specific Registry Location (`HKLM\…\`) overrides	`HKLM\…\Extensions\AccessManager:MFEnable`
User-specific Registry Location (`HKCU\…\`) or User setting in Settings dialog in Logon Manager Mainframe Enable	`HKCU\…\Extensions\AccessManager:MFEnable`

7.2.10.1 Recommended Global Agent Settings for SSO Kiosk Operation

For best performance and security, the following Global Agent Settings should be applied to the Logon Manager Agent running on a workstation configured as a kiosk:

Setting	Function
User Paths	(Active Directory only) For best performance, specify one or more fully-qualified paths to begin searching for user accounts. See the **Advanced** options, under **Synchronization>Active Directory**.

7.2.11 Configuring Registry Settings and Administrative Overrides

The Administrative Console can be used to configure `HKLM\&\` values and deploy them to synchronizer extensions.

1. In the Administrative Console, create a new set of settings (right click **Global Agent Settings** and choose **New Settings**), load a saved set of settings (right click **Agent Settings** and select **Import**), or select an existing set of settings (by selecting it in the left pane).

2. In the left pane, select and open the set of settings, and select and open the desired registry key.

   > **Note:** Registry entries beginning with `Extensions\` are displayed in the Administrative Console without the leading `Extensions\`.

3. In the right pane, select the desired registry value, select the checkbox, and enter the desired value.

4. Export to the desired format (Admin Override or HKLM Registry format):

5. Select the set of settings in the left pane

6. Choose **Export** from the **File** menu and choose an export format.

To deploy an administrative overrides file to a synchronizer extension, see the following topics:

- Chapter 2.16.2, "Configuring the Agent for Directory Server Synchronization"

- Chapter 2.16.3, "Configuring the Agent for Database Synchronization"

- Chapter 2.16.4, "Configuring the Agent for File System Synchronization"

To use an HKLM Registry format file, either launch it (for example, double-click on the file from Explorer), import it (for example, from RegEdit), or deploy it using your deployment tool.

Refer to Chapter 2.17.3, "Global Agent Settings in Depth" for a complete description of these settings, including:

- Screen layouts

- Setting names

- Setting descriptions

- Registry names

- Setting options and defaults

- Registry and Data Types

7.2.12 Directory Server Schema Definition

The following are Directory Server Container and Class Objects, their rights, and their attributes.

7.2.12.1 vGOSecret

Stores all user secrets. This includes an object that stores all deleted objects and their logon credentials. This is added to the SSOUserData object as an auxiliary class. All users can read this object, but only the owner can write to this object, and only the owner or administrator can delete this object.

Rights: The rights are inherited from the vGOUserData object.

Attribute Name	Syntax	Flag
vGOSecretData	Case Ignore String	Singled Valued, Synchronize
vGOSharedSecretDN	Not Used	
Other optional attributes	ou, dn, cn, o	

7.2.12.2 vGOUserData Object

A container allowing users to store their individual/personal secured credentials.

Rights: Users have write access to these attributes for their own user objects. The administrator has full rights but will not be able to read the secrets due to encryption.

Attribute Name	Syntax	Flag
vGOSecretData	Case Ignore String	Singled Valued, Synchronize
vGORoleDN	Not Used	
Other optional attributes	ou, dn, cn, o	

7.2.12.3 vGOConfig Object

Used to hold all configuration information that the Agent needs. This includes the application-supported list, mainframe/host application supported list, first-time use setup instructions, Password Policies, and admin overrides. All of these settings control Agent behavior.

Rights: All users have read-only rights to the attributes within this object. The administrator has full rights.

Attribute Name	Syntax	Flag
vGOConfigType	Case Ignore String	Singled Valued, Synchronize
vGOConfigData	Case Ignore String	Singled Valued, Synchronize
vGORoleDN	Not Used	
Other optional attributes	ou, dn, cn, o	

7.2.12.4 vGOLocatorClass

This is used to specify where to store user credentials.

Rights: All users have read/compare/search access to these attributes for all of this class of object. The administrator has full rights.

Attribute Name	Syntax	Flag
vGOLocatorAttribute	Case Ignore String	Single Valued
Other optional attributes	dn, cn, o	

7.2.13 Error Loop Quick Reference

This section serves as a quick-reference to the basic Error Loop settings.

> **Note:** Configure these settings in the Administrative Console. The table is provided only for reference.

The settings are inherited downward from global to application type to application. More specific settings override more general (application overrides application type, which overrides global).

> **Note:** For security settings (for example, MaskPW), the most secure setting is used, regardless of whether it is set globally, for an application type, or for an application.

Place the application-type settings in the `entlist.ini[*Root]` section.

Example 1
```
[*Root]
AppsTimeout=8
WebMaxRetry=3
Place the Application settings in the specific application's entlist.ini section.
```

Example 2
```
[Payroll]
WindowTitle1=Payroll
MaxRetry=3
Timeout=30
IDCtrl=203
...
```

Global (Registry)	Application Type([*Root])					
ParameterPurpose	Extensions\ AccessManager\ Dlg	Windows	Web	Host/Mainframe	Application	Default
Max # of retries (after first try) before Error Loop dialog appears	MaxRetry	AppsMaxRetry	WebMaxRetry	MainframeMaxRetry	MaxRetry	0
Max time between successive logon attempts before Error Loop dialog appears	Timeout	AppsTimeout	WebTimeout	MainframeTimeout	Timeout	30
Setting to indicate whether to hide the password confirmation field in the Error Loop dialog	HideConfirmPW	AppsHideConfirmPW	WebHideConfirmPW	MainframeHideConfirmPW	HideConfirmPW	0 (do not hide)

7.2.14 Configuring Logon Manager Event Logging for IBM DB2 Database Support

In order to configure Logon Manager to store event log data in a table in an IBM DB2 database, you must complete the following steps:

1. If you have not already done so, install and configure the IBM DB2 database as described in the vendor's documentation. Use the Typical installation scenario when prompted.

2. Set up the event log data table.

3. Install the Database Event Extension component for Logon Manager.

4. Configure Logon Manager to store its event log data in the table you created.

5. Test your event logging configuration.

7.2.14.1 Installing and Configuring the IBM DB2 Database

Before you begin configuring Logon Manager event logging, install and configure an instance of the IBM DB2 database as described in the vendor's documentation, if you have not already done so. Unless your environment dictates otherwise, select the "Typical" installation scenario when prompted by the installer.

7.2.14.2 Setting Up the Event Log Data Table

Before Logon Manager can store event log data in the database, you must set up a table that will store the data. The steps are as follows:

1. Launch the IBM DB2 Control Center application. By default, the application is located in

   `C:\Program Files\IBM DB2\General Administration Tools.`
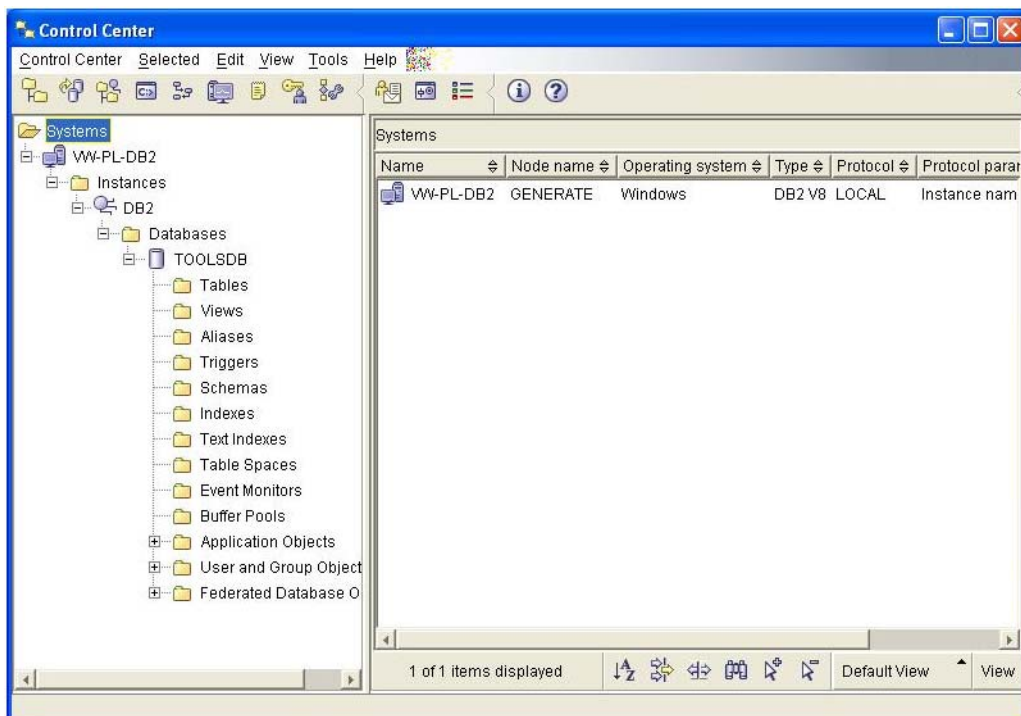
2. Within the database of your choice, create a table that will store Logon Manager event log data:

   a. Under the selected database, right-click Tables and select **Create…** from the context menu.

   b. In the **Create Table Wizard**, name the table in accordance with the vendor's naming schema, then click **Next**.
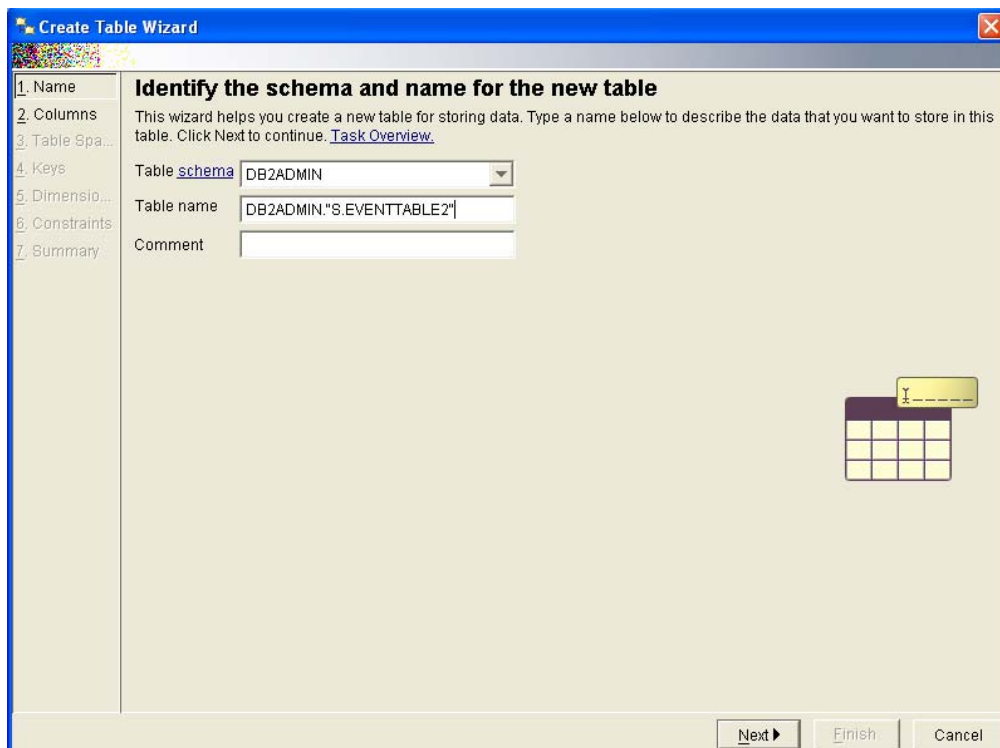
c. Set up the required table columns. For each required column, do the following:

– In the **Change column definitions for the new table** dialog, click **Add**.
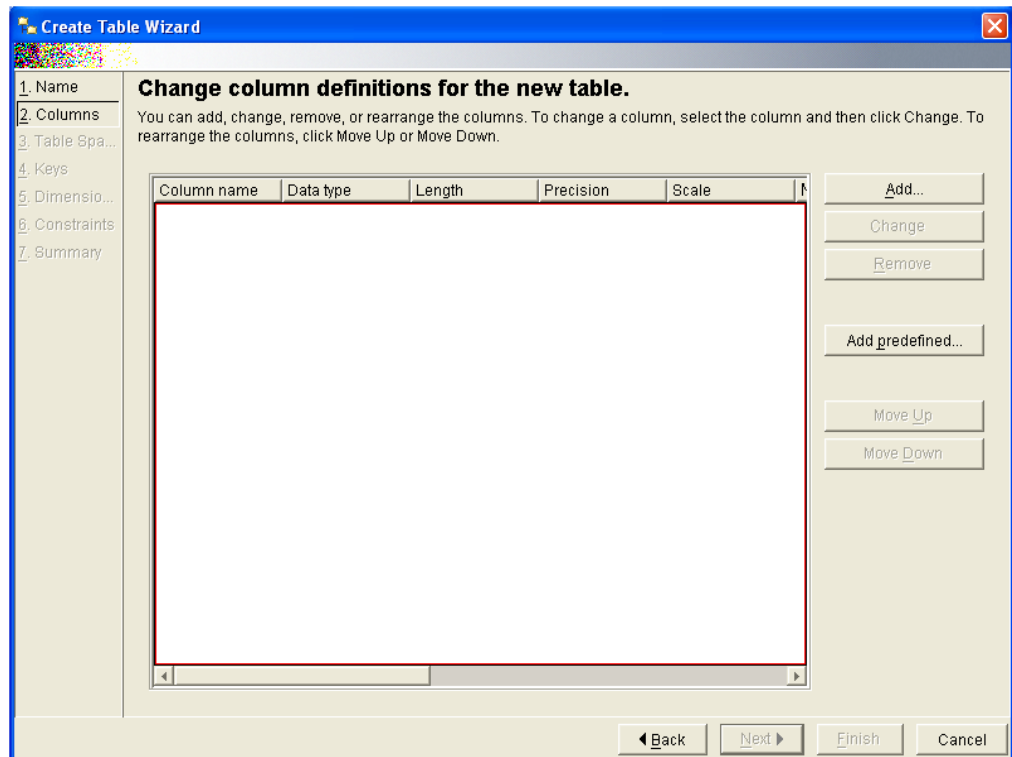
The **Add Column** dialog appears.
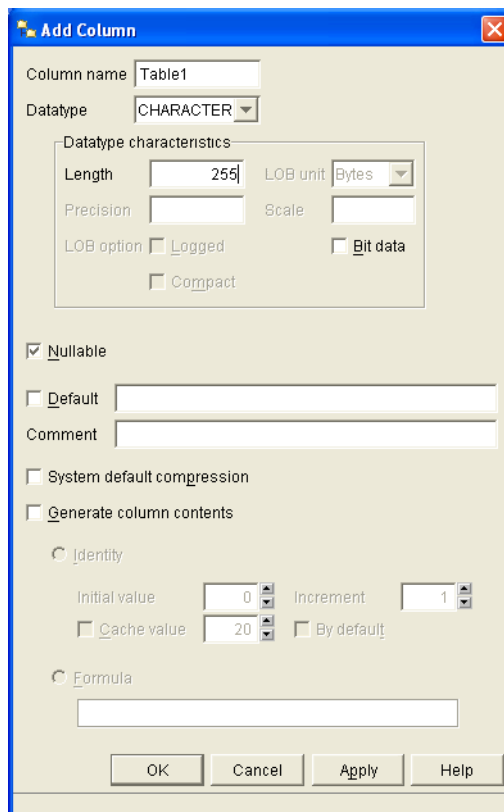
– Name the column. These column names will correspond to event log field names shown below that you will configure later in this document using the Administrative Console.
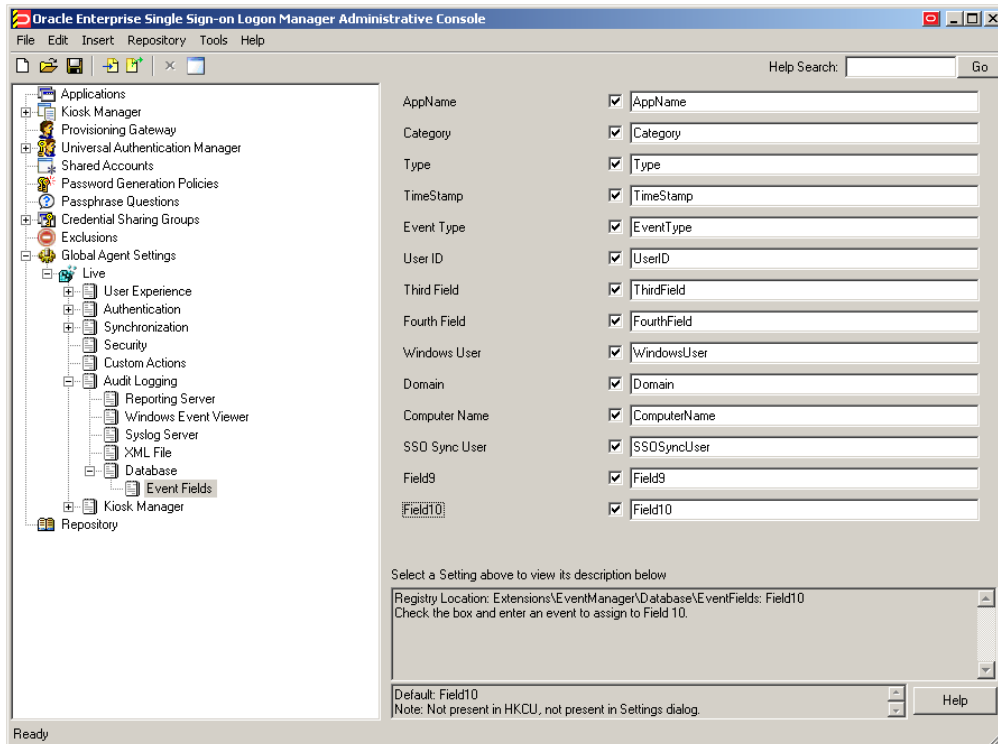
> **WARNING:** Each event log field must have a corresponding column with an identical name in the event log data table. Otherwise, event data will not be recorded.

– Select **CHARACTER** as the data type.

– Set the data length to 128.

– When you have populated the appropriate fields, click **Apply**, then **OK**.

When you have finished, the table configuration will look as follows:
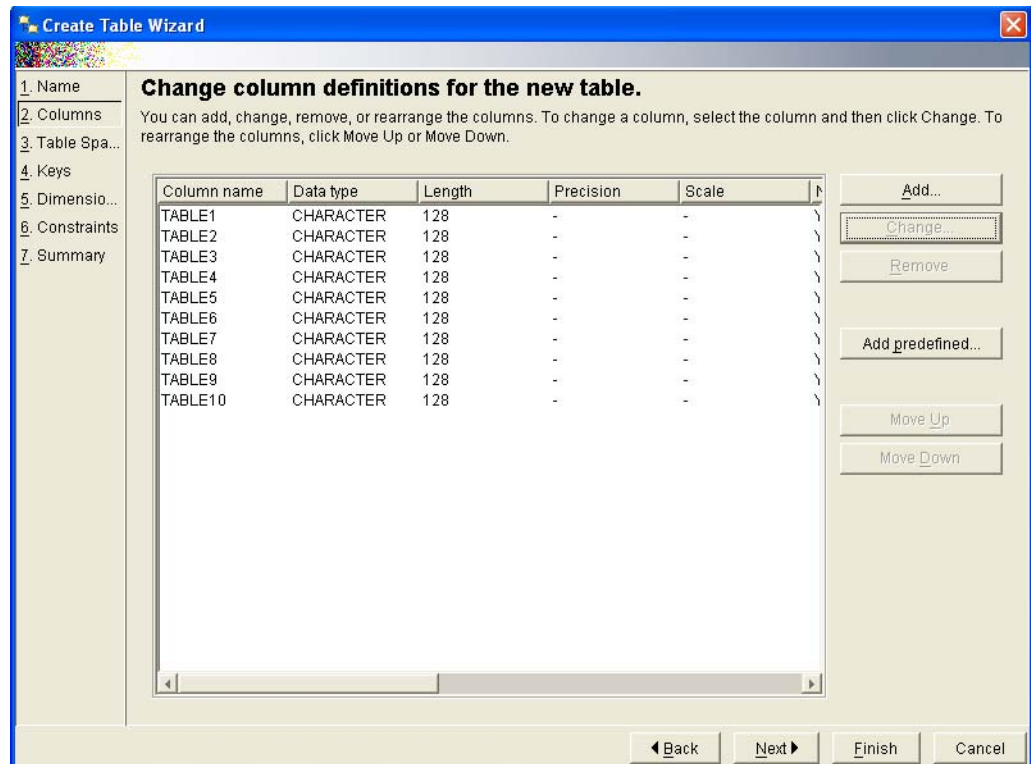
d. If you need to make any changes, select the desired column in the list and click **Change**. When the table configuration is complete, click **Next**.

e. When prompted to configure the table space, make a selection that is most appropriate to the level of Logon Manager event logging required by your environment, then click **Next**.
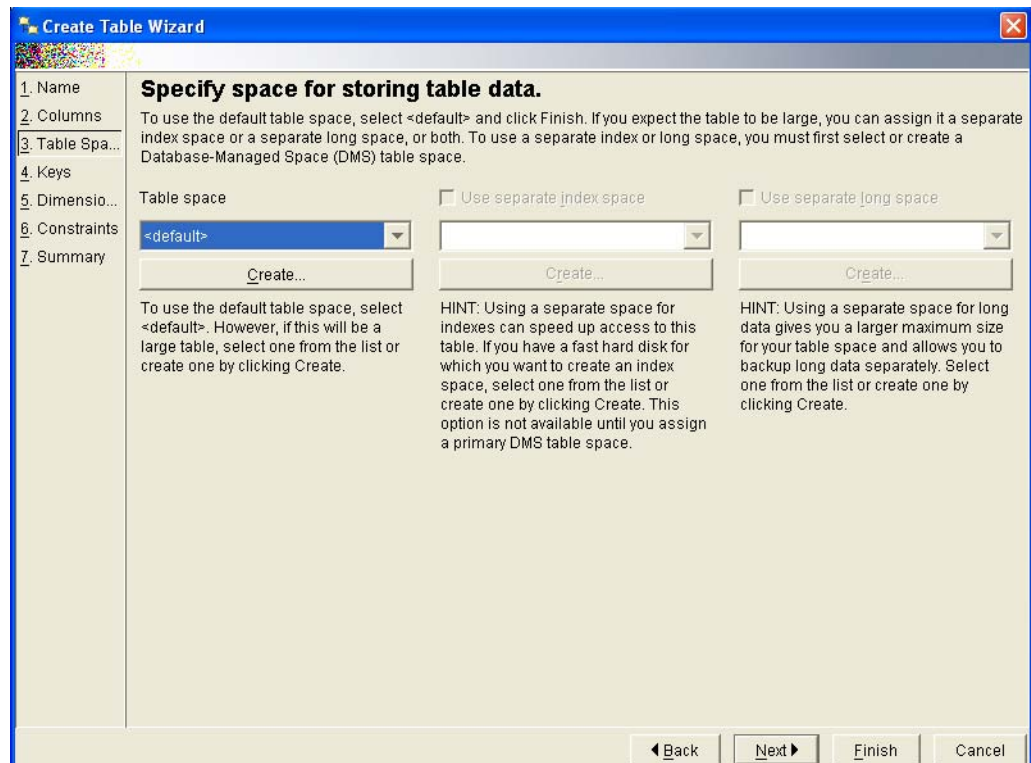
    f. For the remainder of the wizard, click **Next** to accept the defaults presented in each screen.

    g. In the configuration summary dialog, click **Finish**.
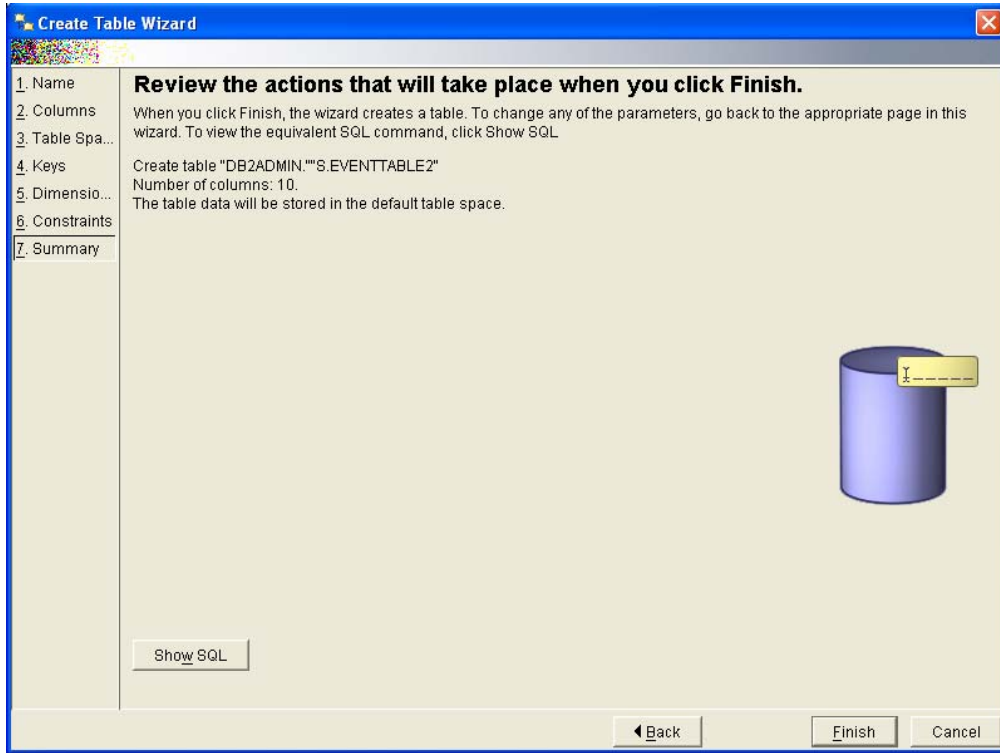
The table is created. Depending on the speed of your system, this can take a few moments.

3. Monitor the table creation process by checking the database log. When the table has been created successfully, the log will show the following:
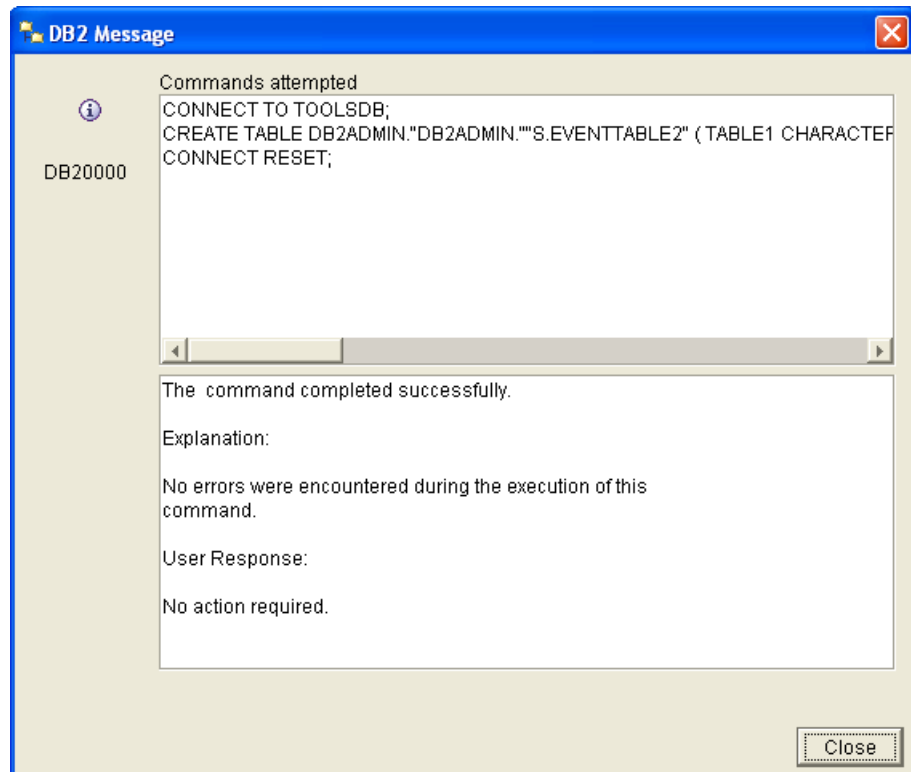
7.2.14.3 Installing the Database Event Extension Component for Logon Manager

The Database Even Extension component must be installed in order for Logon Manager to store event log data in the database. To install the component, do the following:

1. Click **Start > Settings > Control Panel**.

2. In the **Control Panel**, click **Programs and Features**.

3. In the applet, navigate to the **Logon Manager Agent** entry and click **Change**.

4. In the **Logon Manager Agent** installer, click **Next**.

5. In the **Program Maintenance** dialog, select **Modify** and click **Next**.

6. In the **Advanced Setup** dialog, expand the **Audit Logging Methods** node.

7. Under the **Audit Logging Methods** node, click the button next to **Database Event Extension** and select **This feature will be installed on local hard drive** from the context menu.
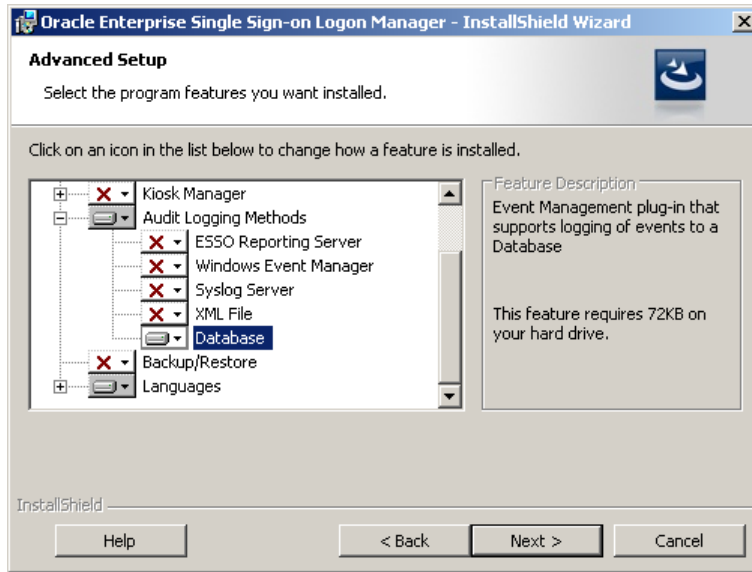
8. Click **Next**; then, in the dialog that follows, click **Install** and wait for the installation to complete.

9. When the installation completes successfully, click **Finish**.

7.2.14.4 Configuring Logon Manager Event Logging for Database Support

1. Launch the Administrative Console and load your current configuration set.

2. In the tree, navigate to **Global Agent Settings > [Current Configuration Set] > Audit Logging > Database**.

3. Select the check box next to **Events to log** and click the ellipsis ("**…**") button.

4. In the **Events to log** dialog, select the types of events you want to log.

WARNING: You must select the Event Types: Info item; otherwise, no data will be logged.

---
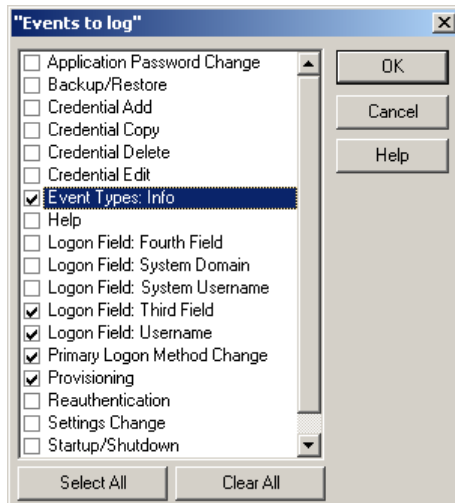
5. Under the **Audit Logging** node in the tree, select **Database** and configure Logon Manager as follows:

Setting	Value
Servers	`Provider=<db2_provider_name>;Password=<db2_admin_` `user_password>;User ID=<db2admin_user_name>;Data` `Source=<database_name>`
Default server	URL to your database server instance.
Default table	Name of the event log data table created earlier in this section. (`DB2ADMIN."S.EVENTTABLE2` in our example)
Retry interval	Set to the desired retry interval. See Chapter 2.17.3, "Global Agent Settings in Depth" for more information.
Events to log	Configure to exactly match the event types chosen in step 4.

6. Under the Database node in the tree, select **Event Fields**.

7. For each field, enter the name of the corresponding column in the event log data table. The names must match the names you specified for the database table columns.

> **WARNING:**   Do not alter the values of the AppName, Category, TimeStamp, and Type parameters.

8. When finished, push the modified configuration set to your directory or write them to the local registry, whichever option suits your environment.

9. Proceed to the next section to test your event logging configuration.

7.2.14.5 Testing Your Event Logging Configuration

This simple test procedure allows you to check whether Logon Manager is properly logging event data to the database. In our example, you will press the **Help** button in Logon Manager and check the database to see if the button press is logged.

1. Open Logon Manager and click **Help**.

2. Start the IBM DB2 Command Center. Typically, the shortcut is located in **Start > Program Files > IBM DB2 > Command Line Tools**.

3. Under **Database Connection**, click the ellipsis ("**…**") button.

4. In the **Select a Database** dialog, navigate to the target database, select it, and click **OK**.
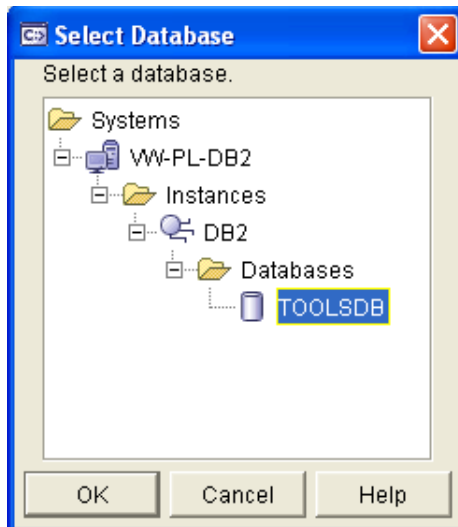
5. Under Command, enter the following, then press **Enter**:

   ```
   SELECT * FROM <name_of_event_log_data_table>;
   ```

6. The Command Center displays all Logon Manager events that have been logged in the database so far. The Help button press event should appear near or at the end of the list, as shown below.
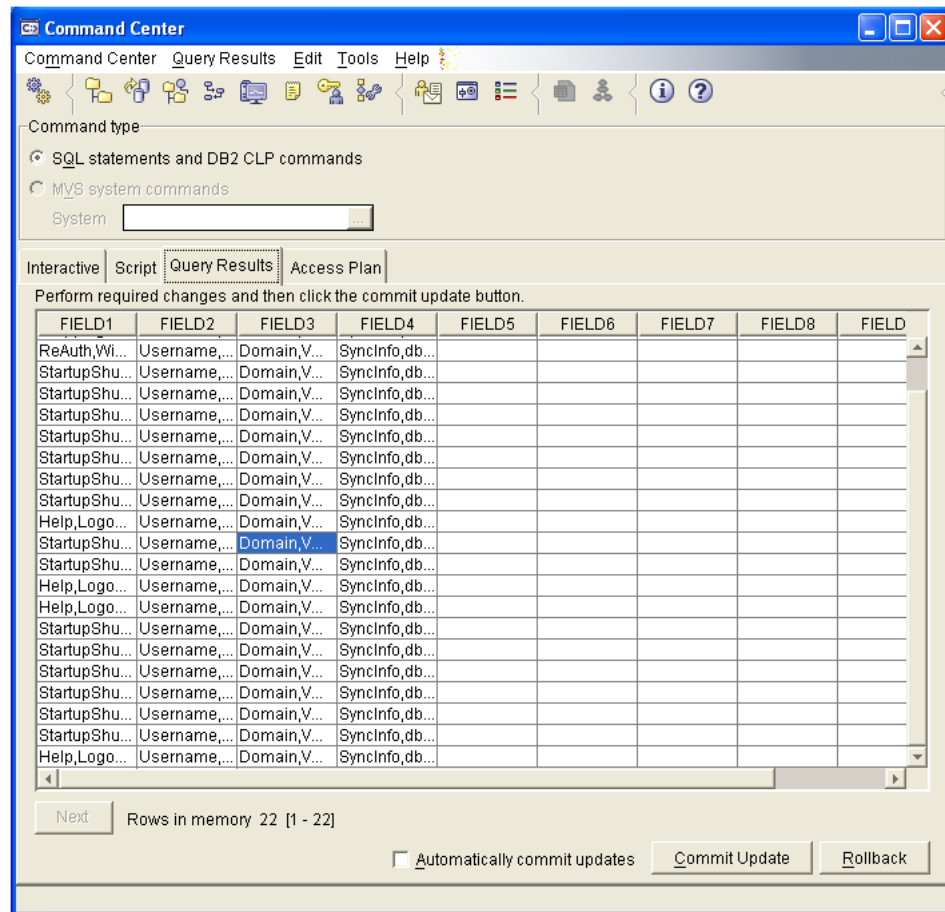
If the Help button press event does not appear, retrace your steps and check your database and Logon Manager configurations.

7.2.15 Configuring Logon Manager Event Logging with MS SQL Server 2005

In order to configure Logon Manager to store event log data in a table in an MS SQL Server 2005 database, you must complete the following steps:

1. Install and Configure MS SQL Server 2005.

2. Set Up the Event Log Data Table.

3. Install the Database Event Extension Component for Logon Manager.

4. Configure Logon Manager Event Logging for Database Support.

5. Test Your Event Logging Configuration.

7.2.15.1 Install and Configure MS SQL Server 2005

Before you begin configuring Logon Manager event logging, install and configure an instance of the MS SQL Server 2005 database as described in the vendor's documentation, if you have not already done so. Unless your environment dictates otherwise, select the **Typical** installation scenario when prompted by the installer.

7.2.15.2 Set Up the Event Log Data Table

Before Logon Manager can store event log data in the database, you must set up a table that will store the data. The steps are as follows:

1. Launch the SQL Server Management Studio application and navigate the left-hand tree to expand the database of your choice.

2. Within the selected database, create a table that will store Logon Manager event log data:

   a. Under the selected database, right-click **Tables** and select **New Table…** from the context menu. MS SQL Server creates a table with a default name (for example, Table_1).
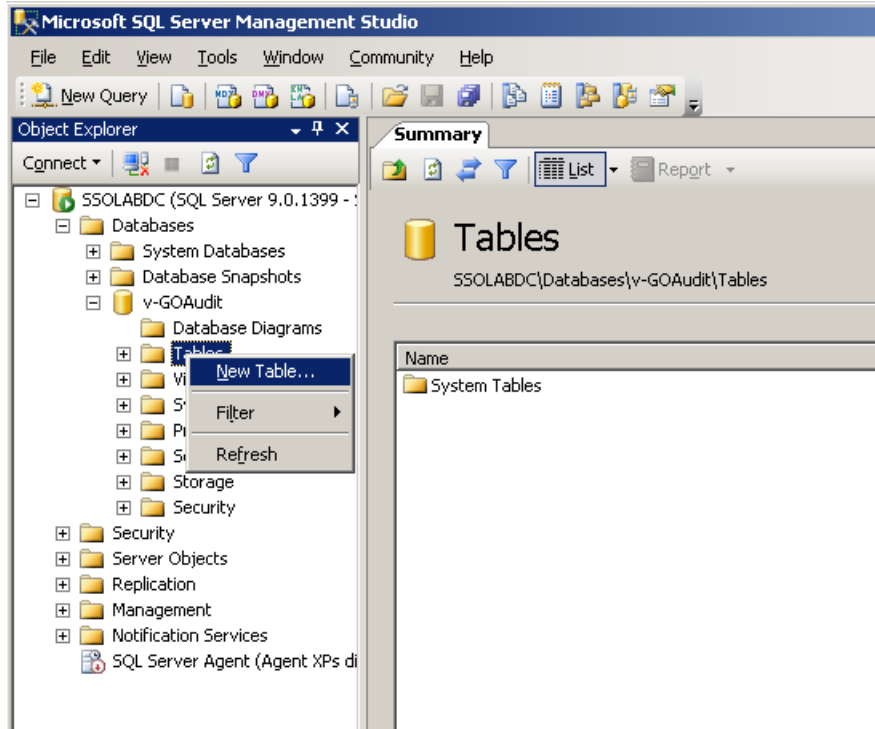
   b. Rename the table as desired using the **Name** field in the **Properties** pane on the right-hand side. You will supply this table name to Logon Manager later in this process.

   c. Set up the required table columns. For each required column, do the following:

   d. Name the column. These column names will correspond to event log field names shown below that you will configure later in this document using the Administrative Console.

   > **WARNING:** Each event log field must have a corresponding column with an identical name in the event log data table. Otherwise, event data will not be recorded.
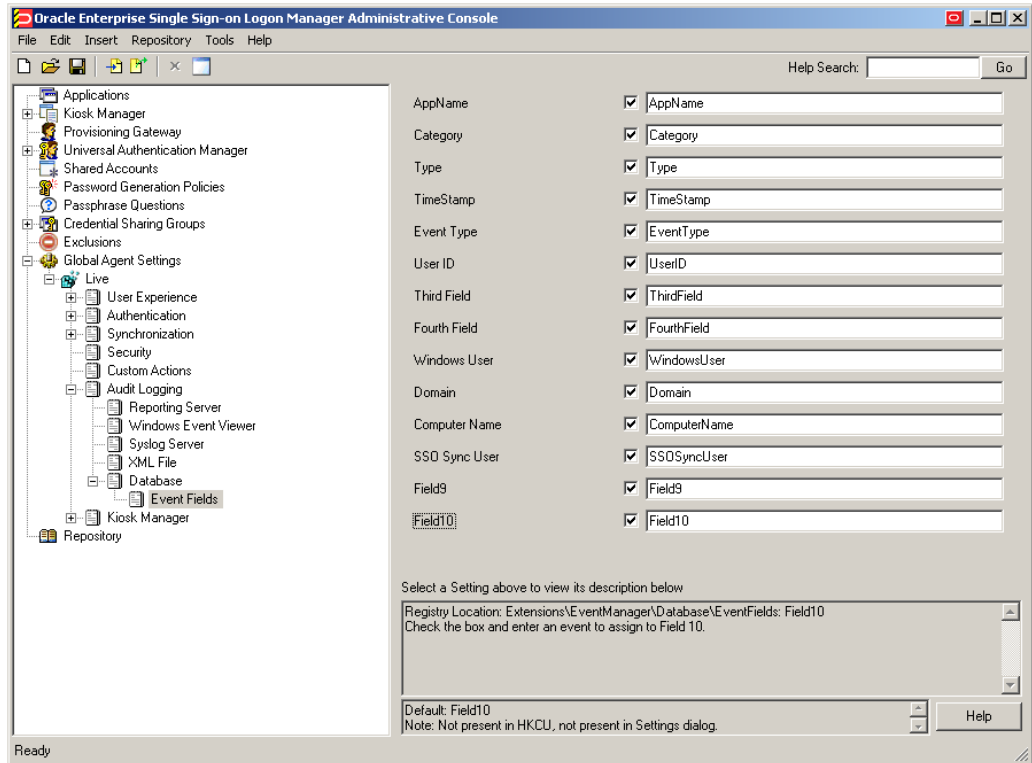
e. Select **char** as the data type.

f. Set the data length to 255.

g. Enable the **Allow Nulls** option.

h. When you have finished, save your changes (**File > Save Table**).

When complete, the table configuration will appear as follows:

7.2.15.3 Install the Database Event Extension Component for Logon Manager

The Database Event Extension component must be installed in order for Logon Manager to store event log data in the database. To install the component, do the following:

1. Click **Start > Settings > Control Panel**.

2. In the **Control Panel**, click **Programs and Features**.

3. In the applet, navigate to the **Logon Manager Agent** entry and click **Change**.

4. In the Logon Manager Agent installer, click **Next**.

5. In the **Program Maintenance** dialog, select **Modify** and click **Next**.

6. In the **Advanced Setup** dialog, expand the **Audit Logging Methods** node.

7. Under the **Audit Logging Methods** node, click the button next to **Database** and select **This feature will be installed on local hard drive** from the context menu.
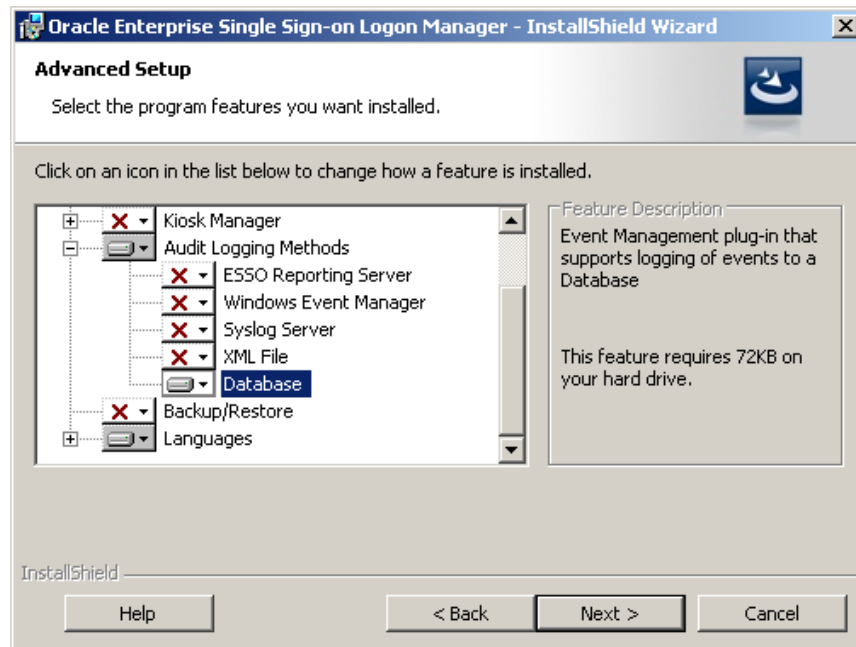
8. Click **Next**; then, in the dialog that follows, click **Install** and wait for the installation to complete.

9. When the installation completes successfully, click **Finish**.

7.2.15.4 Configure Logon Manager Event Logging for Database Support

1. Launch the Administrative Console and load your current configuration set.

2. In the tree, navigate to **Global Agent Settings > *[Current Configuration Set]* > Audit Logging Methods**.

3. Select the check box next to the **Events to log** option and click the ellipsis ("**…**") button.

4. In the **Events to log** dialog, select the types of events you want to log.

> **WARNING:** You must select the Event Types: Info item; otherwise, no data will be logged.

---
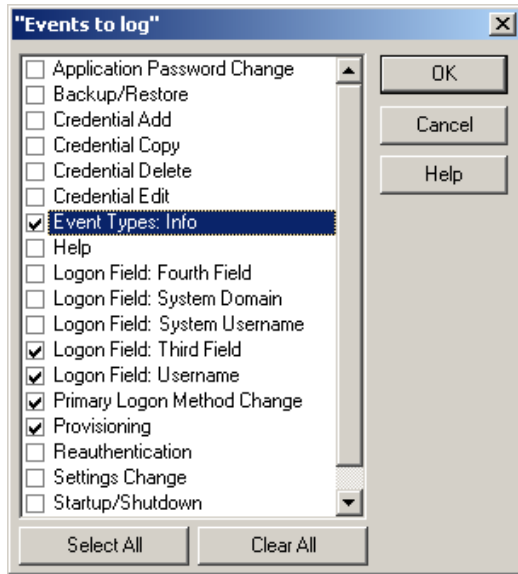
5. Under the **Audit Logging** node in the tree, select **Database** and configure Logon Manager as follows:

Setting	Correct Value

Servers	`Provider=<SQL_provider_name>;Password=<SQL_admin_`
	 `user_password>;User ID=<SQLadmin_user_name>;Data`
	 `Source=<database_name>`

Default server	URL to your database server instance. This will be Server1.
Default table	Name of the event log data table created earlier in this section. (Table_1 in our example)
Retry interval	Set to the desired retry interval. See Chapter 2.17.3, "Global Agent Settings in Depth" for more information.
Events to log	Configure to exactly match the event types chosen in step 4.

6. Under the **Database** node in the tree, select **Event Fields**.

7. For each field, enter the name of the corresponding column in the event log data table. The names must match the names you specified for the database table columns.

> **WARNING:** Do not alter the values of the AppName, Category, TimeStamp, and Type parameters.

8. When finished, push the modified configuration set to your directory or write them to the local registry, whichever option suits your environment.

9. Proceed to the next section to test your event logging configuration.

7.2.15.5 Test Your Event Logging Configuration

This simple test procedure allows you to check whether Logon Manager is properly logging event data to the database. In our example, you will press the **Help** button in Logon Manager and check the database to see if the button press is logged.

1. Open Logon Manager and click **Help**.

2. Start the Microsoft SQL Server Management Studio application. Typically, the shortcut is located in **Start > Program Files > Microsoft SQL Server 2005**.

3. In the left-hand tree, navigate to the event log data table.

4. Right-click the event log data table and select **Open Table** from the context menu.
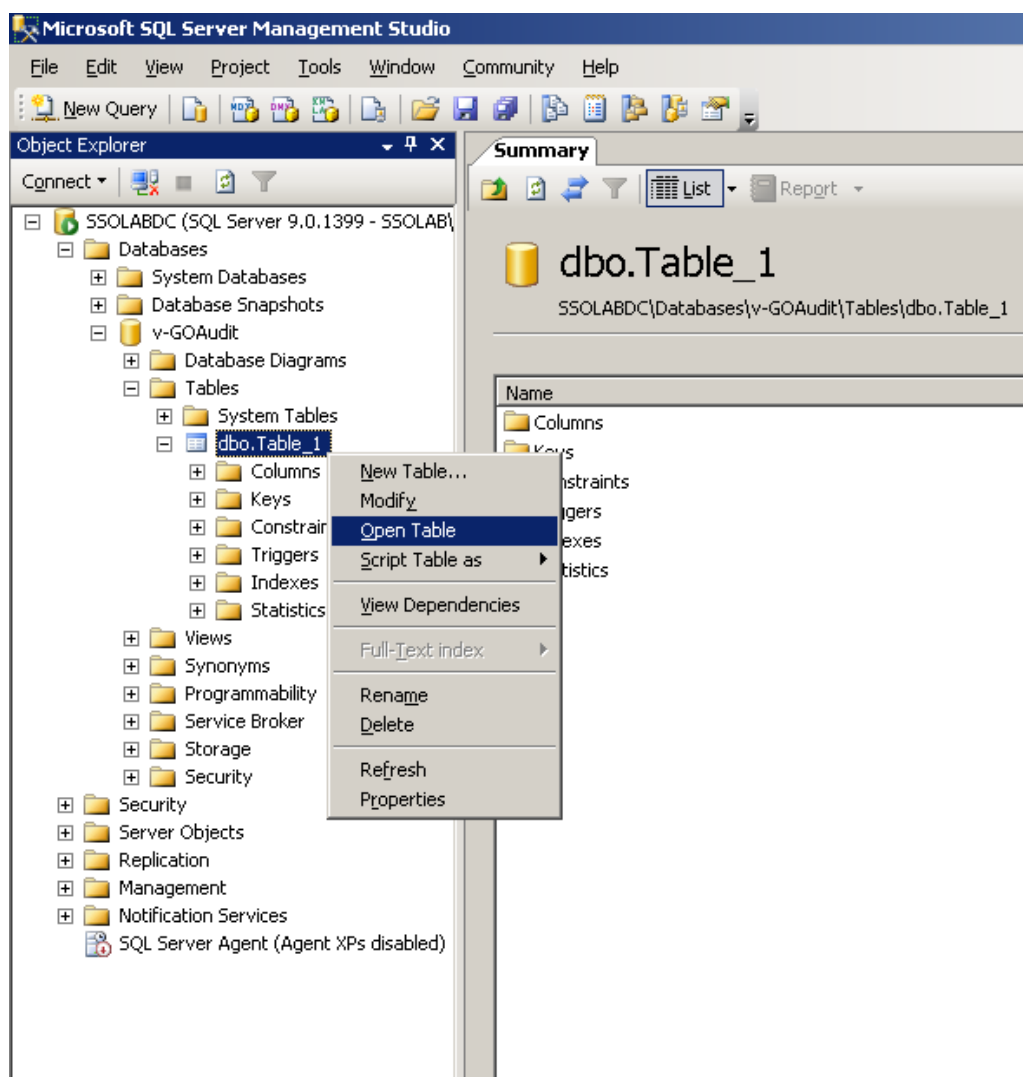
The Microsoft SQL Server Management Studio will display all Logon Manager events that have been logged in the database so far. The Help button press event should appear near or at the end of the list, as shown below.

AppName	Category	TimeStamp	Field1	Field2	Field3	Field4
NULL	Feature ...	11/19/2008 11:13:39 AM ...	StartupShutdown,Startup ...	Username,administrator ...	Domain,SSOLAB ...	SyncInfo,admini...
NULL	Feature ...	11/19/2008 2:14:43 PM ...	ReAuth,WinAuth SUCCESS ...	Username,administrator ...	Domain,SSOLAB ...	SyncInfo,admini...
NULL	Feature ...	11/19/2008 2:14:48 PM ...	ReAuth,WinAuth SUCCESS ...	Username,administrator ...	Domain,SSOLAB ...	SyncInfo,admini...
NULL	Feature ...	11/19/2008 2:15:16 PM ...	StartupShutdown,Shutdown ...	Username,administrator ...	Domain,SSOLAB ...	SyncInfo,admini...
NULL	Feature ...	11/24/2008 4:00:29 PM ...	StartupShutdown,Startup ...	Username,administrator ...	Domain,SSOLAB ...	SyncInfo,admini...
NULL	Feature ...	11/24/2008 4:02:40 PM ...	ReAuth,WinAuth SUCCESS ...	Username,administrator ...	Domain,SSOLAB ...	SyncInfo,admini...
Avent ...	Logon ...	11/24/2008 4:02:41 PM ...	username,rad ...	Username,administrator ...	Domain,SSOLAB ...	SyncInfo,admini...
Avent ...	Logon ...	11/24/2008 4:03:51 PM ...	username,rad ...	Username,administrator ...	Domain,SSOLAB ...	SyncInfo,admini...
NULL	Feature ...	11/24/2008 4:03:58 PM ...	ReAuth,WinAuth SUCCESS ...	Username,administrator ...	Domain,SSOLAB ...	SyncInfo,admini...
Avent ...	Logon ...	11/24/2008 4:04:04 PM ...	username,rad ...	Username,administrator ...	Domain,SSOLAB ...	SyncInfo,admini...
NULL	Feature ...	11/24/2008 4:04:18 PM ...	StartupShutdown,Shutdown ...	Username,administrator ...	Domain,SSOLAB ...	SyncInfo,admini...
NULL	Feature ...	11/26/2008 2:21:31 PM ...	StartupShutdown,Startup ...	Username,administrator ...	Domain,SSOLAB ...	SyncInfo,admini...
NULL	Feature ...	11/26/2008 2:25:43 PM ...	ReAuth,WinAuth SUCCESS ...	Username,FerdinandP ...	Domain,SSOLAB ...	SyncInfo,Ferdin...
NULL	Credential ...	11/26/2008 2:26:04 PM ...	add,Acrobat Reader ...	Username,FerdinandP ...	Domain,SSOLAB ...	SyncInfo,Ferdin...
NULL	Credential ...	11/26/2008 2:26:05 PM ...	add,GoldMine ...	Username,FerdinandP ...	Domain,SSOLAB ...	SyncInfo,Ferdin...
NULL	Feature ...	11/26/2008 2:26:08 PM ...	StartupShutdown,Startup ...	Username,FerdinandP ...	Domain,SSOLAB ...	SyncInfo,Ferdin...
NULL	Feature ...	11/26/2008 2:26:54 PM ...	Help,Logon Manager ...	Username,FerdinandP ...	Domain,SSOLAB ...	SyncInfo,Ferdin...
NULL	Feature ...	11/26/2008 2:27:00 PM ...	StartupShutdown,Shutdown ...	Username,FerdinandP ...	Domain,SSOLAB ...	SyncInfo,Ferdin...
NULL	Feature ...	11/26/2008 2:28:18 PM ...	StartupShutdown,Startup ...	Username,FerdinandP ...	Domain,SSOLAB ...	SyncInfo,Ferdin...
NULL	Feature ...	11/26/2008 3:08:48 PM ...	StartupShutdown,Shutdown ...	Username,FerdinandP ...	Domain,SSOLAB ...	SyncInfo,Ferdin...
NULL	Feature ...	11/26/2008 3:09:41 PM ...	StartupShutdown,Startup ...	Username,FerdinandP ...	Domain,SSOLAB ...	SyncInfo,Ferdin...
NULL	Feature ...	11/26/2008 3:13:34 PM ...	Help,Logon Manager ...	Username,FerdinandP ...	Domain,SSOLAB ...	SyncInfo,Ferdin...
NULL	NULL	NULL	NULL	NULL	NULL	NULL

7.2.16 Understanding the Logon Manager Event Notification API

The Logon Manager Notification Service (referred to as "the service" for the remainder of this section) allows the sending and receiving of event data between Oracle Enterprise Single Sign-On applications. The service runs as a Windows system service and acts as a global events repository and an event router.

The service runs as a Windows system service and distinguishes between the following application roles:

- Producer. An application that sends events to other applications

- Consumer. An application that receives events from other applications

7.2.16.1 Event Handling Tasks

The service handles events as follows:

- Stores events received from producers. The service enumerates and retains the latest 1000 events received for each producer and each running session. Once the event buffer is full, the oldest event is discarded for each new event that enters the buffer. Each event can be uniquely identified by producer GUID, session GUID, and its consecutive position in the buffer.

- Transmits events to consumers. The service uses the following interface to transmit events:

```
[

object,uuid(DD9E48CA-63D2-4106-876D-4DDEAA063B6F),dual,nonextensible,he
lpstring("Allows Consumers to access to the information about
event"),pointer_default(unique) ]interface ISSONotificationEvent:
IDispatch

{

[propget, id(1), helpstring("Gets event order number")] HRESULT
Number([out, retval] ULONG* pVal);
```

```
[propget, id(2), helpstring("Gets notification event code")] HRESULT
NotificationCode([out, retval] ULONG* pVal);

[propget, id(3), helpstring("Gets progress value")] HRESULT
Progress([out, retval] LONG* pVal);

[propget, id(4), helpstring("Gets event importance level")] HRESULT
Level([out, retval] ULONG* pVal);

[propget, id(5), helpstring("Gets additional data")] HRESULT
AdditionalData([out, retval] BSTR* pVal);

[propget, id(6), helpstring("Gets event time")] HRESULT Time([out,
retval] DATE* pVal);

};
```

7.2.16.2 The SSONotificationService Co-Class

The following IDL code describes the service's co-class used by producers and
consumers:

```
[

uuid(FBB13217-02AB-42DF-8867-69B8DD935BA9),helpstring("SSO Notification
Service class")

]coclass SSONotificationService {

// Allows Consumers to subscribe for event notifications: [default]
interface ISSONotificationService;

// Allows Consumers to access to the information about events:interface
ISSONotificationEventReader;

// Allows Producers to obtain ISSONotificationEventWriter pointer for
event raising:interface ISSOWriterManager;

};
```

7.2.16.3 Sending Data (Producer)

Producers should follow these guidelines to interface with the service properly.

7.2.16.3.1 Producer Identification A producer must implement the ISSOProducerInfo
interface to uniquely identify itself to the service:

```
[

object,uuid(4961B340-D358-4A0E-B8FB-6E2A4BF2DFDD),dual,nonextensible,helps
tring("Provides information about Producer"),pointer_default(unique)

]interface ISSOProducerInfo : IDispatch {

[propget, id(1), helpstring("Gets Terminal Services session identifier")]
HRESULT SessionId([out, retval] ULONG* pVal);

[propget, id(2), helpstring("Gets Producer GUID")] HRESULT
ProducerGuid([out, retval] BSTR* pVal);

[propget, id(3), helpstring("Gets Producer description")] HRESULT
ProducerDescription([out, retval] BSTR* pVal);

};
```

7.2.16.3.2 Event Notification When an event occurs, the producer passes the event data to the service via the ISSONotificationEventWriter COM interface:

```
[

object,uuid(72A23F33-927D-4e01-8B50-759262519076),dual,nonextensible,helps
tring("Allows Producers to raise new events"),pointer_default(unique)

]interface ISSONotificationEventWriter : IDispatch {

[id(1), helpstring("Raises new event")] HRESULT AddEvent([in] ULONG
nNotificationCode, [in] LONG nProgress, [in] ULONG nLevel, [in] BSTR
sAdditionalData);

};
```

To obtain a pointer to this interface, the producer must implement the ISSOProducerInfo interface mentioned earlier and pass its pointer into the GetWriter method of the service's ISSOWriterManager interface shown below:

```
[

object,uuid(4490B430-81FD-48f5-BCD9-F9F0A82C6832),dual,nonextensible,helps
tring("Allows Producers to obtain ISSONotificationEventWriter pointer for
event raising"),pointer_default(unique)

]

interface ISSOWriterManager : IDispatch

{

[id(1), helpstring("Returns ISSONotificationEventWriter pointer for
specified Producer")]

HRESULT GetWriter([in] IDispatch* pProducerInfo, [out,retval] IDispatch**
pEventWriter);

};
```

7.2.16.3.3 Security Measures The service only accepts events from producers whose executables have been signed by Oracle.

A producer requesting a pointer to the ISSONotificationEventWriter using the ISSOWriterManager::GetWriter method is validated as follows:

1. The producer's process identifier (PID) is obtained (based on the producer's ISSOProducerInfodata passed into the method via theCoGetServerPIDfunction).

2. The signature of the producer executable corresponding to the retrieved PID is checked against the information stored in the Windows registry or through the COM Security Initialization process.

> **Note:** The service cannot guarantee a valid signature check when the producer executable is remote.

Additionally, Oracle highly recommends that producers and consumers validate the service's signature as follows:

1. Obtain the service's PID using the CoGetServerPID function from one of the ISSONotificationService sub-interfaces (ISSONotificationEventReader, ISSOWriterManager, ISSONotificationEventWriter, or ISSONotificationEvent).

2. Check the signature of the executable corresponding to the retrieved PID.

7.2.16.4 Receiving Data (Consumer)

Consumers can receive data using either the "push" or "pull" model.

7.2.16.4.1 Receiving Data in a "Push" Model In the "push" model, consumers must do the following to receive event data:

1. Implement the `_ISSONotificationServiceEvents` interface to handle events:

    [

    uuid(88AD71A0-0A9A-4916-BE26-E82C4F41BF3F),helpstring ("Sink interface to handle events")

    ]dispinterface _ISSONotificationServiceEvents {

    properties:methods: [id(1), helpstring ("Handles notification event")] HRESULT HandleEvent([in] IDispatch* pEvent);

    };

    The pEvent parameter referenced above stores the pointer to the object implementing the `ISSONotificationEvent` and `ISSOProducerInfo` interfaces described earlier:

    [

    uuid(C8DCA6F1-2009-4A04-9E4C-BA7CB4CBA86C),helpstring("SSO Event class")

    ]coclass SSONotificationEvent {

    [default] interface ISSONotificationEvent;interface ISSOProducerInfo;

    };

2. Subscribe to the service event stream by passing the `_ISSONotificationServiceEvents` event handler interface into the method of the `ISSONotificationService` interface:

    [

    object,uuid(079F0093-99CB-4FCF-900E-18DAD87ED316),dual,nonextensible, helpstring ("Allows Consumers to subscribe and unsubscribe for events"), pointer_default(unique)

    ]interface ISSONotificationService : IDispatch {

    [id(1),

    helpstring ("Subscribes event handler to events from specified producer and user and returns subscription cookie")]

    HRESULT SubscribeToEvents([in] ULONG nSessionId, [in] BSTR sProducerGuid, [in] IUnknown* pEventHandler, [out,retval] ULONG* pCookie);

    [id(2),helpstring ("Unsubscribes event handler from events from specified producer and user using cookie returned by SubscribeToEvents method")] HRESULT UnsubscribeFromEvents([in] ULONG nSessionId, [in] BSTR sProducerGuid, [in] ULONG nCookie);

    };

When a new event arrives, the service transmits the event data to all subscribed consumers.

7.2.16.4.2 Receiving Data in a "Pull" Model In the "pull" model, a consumer receives the latest events from a producer using the service's `ISSONotificationEventReader` interface:

[

object,uuid(5C4C57D9-D0B1-46AC-A45C-E41C55A7FEF8),dual,nonextensible,helpstring("Allows Consumers to get the information about latest events"),pointer_default(unique)

]interface ISSONotificationEventReader : IDispatch {

[id(1), helpstring("Gets the latest event from specified producer and user")]

HRESULT GetLastEvent([in] ULONG nSessionId, [in] BSTR sProducerGuid, [out, retval] IDispatch** pVal);

[id(2), helpstring("Returns array containing specified number of latest events from specified producer and user")]

HRESULT GetLatestEventsList([in] ULONG nSessionId, [in] BSTR sProducerGuid, [in] ULONG nCount, [out, retval] VARIANT* eventsArray);

};

The service returns event data as pointer (or a safe array of pointers) to the implementations of the `ISSONotificationEvent` interface described earlier.

7.2.17 Using the Trace Controller Utility

The Trace Controller utility allows you to monitor and log events occurring within an Oracle Enterprise Single Sign-On application. You have the choice to monitor events as they occur in real-time, or log them to a file for later review.

The basic components of trace logging are:

- Provider. An Oracle Enterprise Single Sign-On application that supports trace logging. Each application represents a separate provider and establishes a separate logging session when trace logging is enabled.

- Consumer. An application that parses, interprets, and displays the logged events, such as the Trace Controller utility (tracecontroller.exe) or Windows Event Viewer

The Trace Controller utility serves the following purposes:

- Control and configure the logging of Logon Manager events. This involves creating a session and enabling logging in the desired provider(s)

- Display the logged events in the desired format, including filtering by a number of criteria.

The utility allows you to select the desired provider, logging method, and event types, as well as configure additional logging options.

After you enable logging for a provider, it remains enabled even when Trace Controller, the provider application, or Windows itself is shut down. When Windows starts back up and/or the provider application is relaunched, event capture continues until you explicitly disable it.

Oracle Enterprise Single Sign-On applications support the following log verbosity levels.

Level	Level Name	Description
1	Critical	Abnormal exit or termination
2	Error	Server errors that need logging
3	Warning	Warnings such as allocation failure
4	Information	Includes non-error cases (for example, Entry-Exit)
5	Debug	Detailed traces from intermediate steps

When capture is complete, the Trace Controller utility allows you to display one or more event logs in a single viewer that organizes the events in chronological order. For example, you can view Logon Manager and Authentication Manager events in a single list, which can then be filtered by a number of custom criteria.

7.2.17.1 Using the Trace Controller Utility in Graphical Mode

This section explains how to use the Trace Controller utility in its graphical (interactive) mode. Using the utility via command line is explained in the section, Using the Trace Controller Utility in Command Line Mode.

> **Note:** You must have administrative privileges to run the Trace Controller utility. If you are not logged on as a user with administrative privileges, the utility will prompt you for administrative credentials when launched.

To enable trace logging:

1. Launch `TraceController.exe`.

2. If prompted, enter the credentials of an account with administrative privileges.

3. Select **Capture Events** from the **File** menu. The **Capture** window appears.
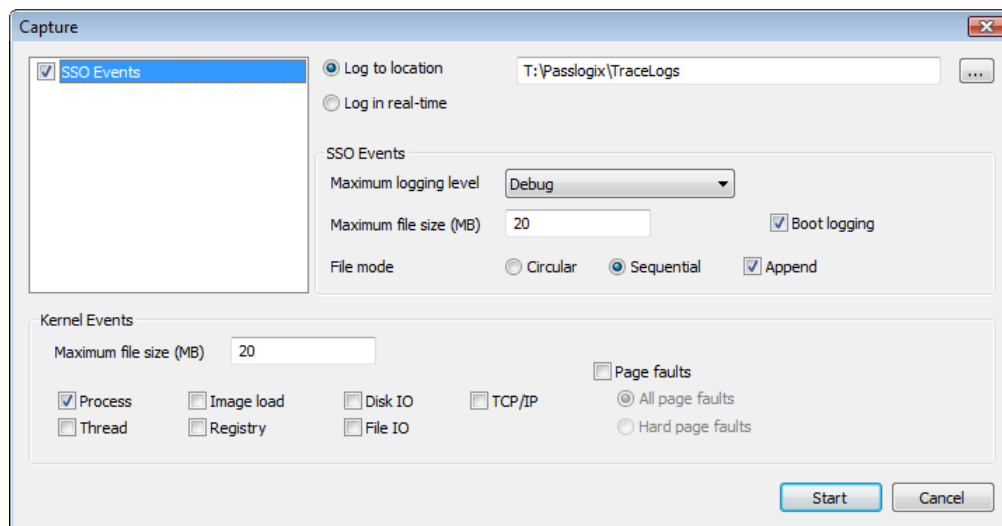
4. In the **Capture** window, do the following:

a. Select the provider whose events you want to log. By default, SSO Events, the main Logon Manager logging provider, is selected.

b. Select whether you would like to log events to a file or display them in real-time. If logging to a file, click the **Browse (…)** button and specify the path and file to which you want to log.

c. Specify the **Maximum logging level** for the SSO Events provider. See Command Line Switch Reference for a list of available logging levels)

d. Specify the **Maximum file size** for the SSO Events provider. The default value is 20MB.

e. Select the desired log file write mode:

Circular. After the maximum log file size is reached, the utility begins overwriting old data in chronological order. The log is cleared each time logging is started.

Sequential. After the maximum log file size is reached, the utility stops logging. The log is cleared each time logging is started, unless you select the **Append** check box.

f. If you want logging to begin at boot time, select the **Boot logging** check box. When this feature is enabled, events will be logged as soon as Windows completes startup and will not require a user logon.

g. For the **Kernel Events provider**, select the types of events you would like to log, and the maximum log file size (the default value is 20MB). In most cases, only kernel process events should be logged for Logon Manager troubleshooting.

5. Click **Start** to begin logging events. Note the following:

- Logging will remain enabled until you explicitly disable it.

- When the Trace Controller utility is running, its system tray icon animates to indicate events are being captured.

Note: After you have configured your initial capture settings, you can configure the Trace Controller utility to start and stop event capture using hot keys. To set up the hot keys, see Configuring Event Capture Hot Keys.

7.2.17.2 Viewing Logged Events

To view events logged to a file, do the following in the Trace Controller utility:

1. Open the desired log file:

a. From the **File** menu, select **Open Events**.

b. Browse to the desired provider's log file and click **Open**. The events stored in the log file are displayed as a list in chronological order.

c. If you want to view events from multiple log files simultaneously, repeat steps 1a and 1b for each additional file you want to open. The events from all open log files are displayed in the list in chronological order.
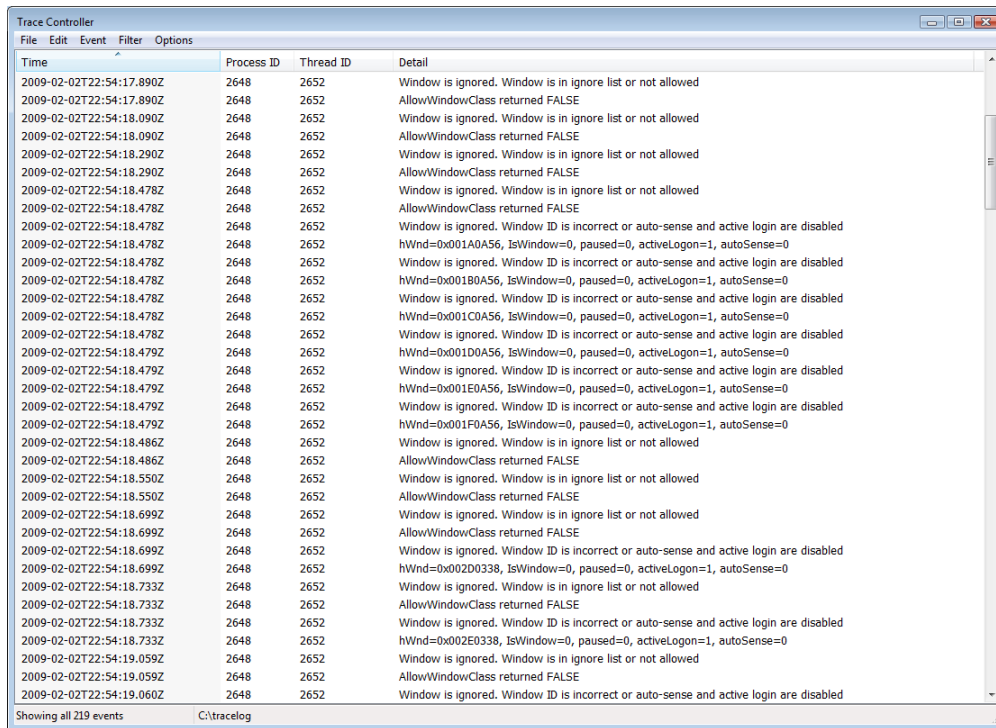
> **Note:** To reverse the sort order, click the **Time** column header. An arrow in the header indicates the currently selected sort direction.

2. To view details for a specific event, navigate to it in the list and double-click it. The details are displayed in a pop-up window.
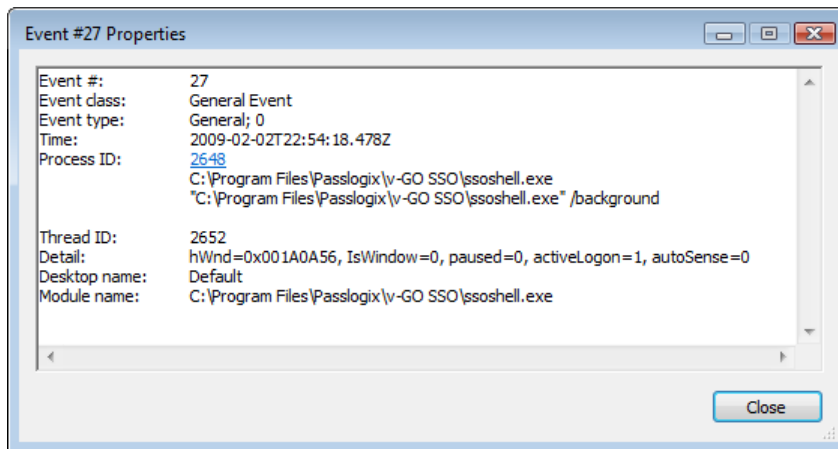
When you are finished viewing the event details, click **Close** to return to the event list.

> **Note:** If you are viewing events from multiple log files, you can see which log files are currently open by selecting **Show Open Log Files** from the **File** menu.

7.2.17.3 Customizing the Event List View

You can customize the following aspect of the event list:

- Event list columns

- Event filter

- Font style and size

- Timestamp format

7.2.17.3.1 Customizing Event List Columns You can select which columns will be displayed in the event list and in what order as follows:

1. Select **Choose Details** from the **Options** menu.

   The **Choose Details** window appears.
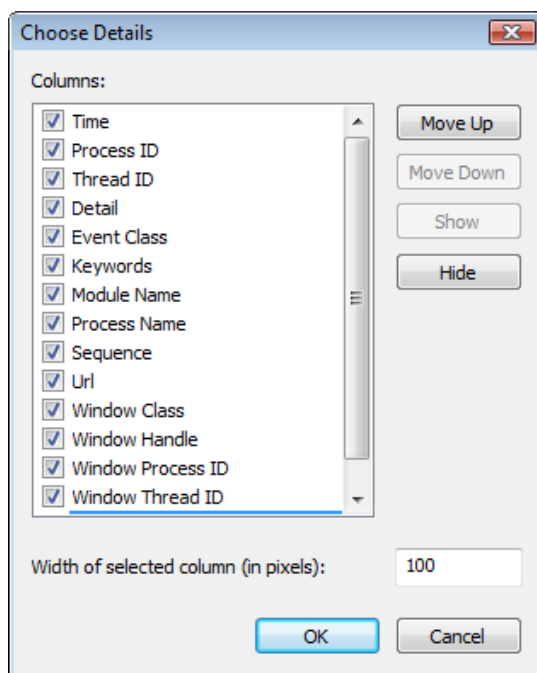
2. In the **Columns** list, select the check box next to each column you want to be visible; deselect the check box to hide the column.

3. To move a column left in the event list, select it in the **Columns** list and click **Move Up**; to move a column right, select it and click **Move Down**.

4. To set a column's width, select it in the **Columns** list and enter the desired width (in pixels) into the **Width of selected column** field.

5. When you have finished, click **OK** to save your changes.

7.2.17.3.2 Filtering Events The Trace Controller utility allows you to filter the displayed events by one or more criteria of your choice. To enable filtering, do the following:

1. From the **Filter** menu, select **Filter**.

2. In the window that appears, configure your first criterion as follows:

   a. Select the parameter to filter against.

   b. Select the operator (is, is not, less than, greater than, and so on).

   c. Enter the value to match the parameter against. Plain text strings as well as regular expressions are supported.

   d. Select whether this criterion should include or exclude matches from the results.

   e. Click **Add**.

3. Repeat the previous step to add criteria.

4. When you are finished, click **OK**. Your results are updated to reflect the filtering criteria you have configured.

> **Note:** The Advanced Filter option is a special feature reserved for developers. Use the standard filter to filter your event list.

7.2.17.3.3 Customizing the Timestamp Format You can customize the event timestamp format as follows:

1. From the **Options** menu, select **Date/Time Format**.

The **Date/Time Format** window appears.
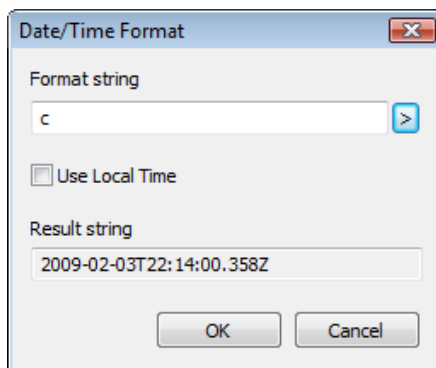
2. Select or enter the desired timestamp format string as follows:

- If you want to choose one of the preset timestamp formats, click the arrow button to the right of the Format string field and select it from the upper section of the menu.

- If you want to enter a custom string, click the arrow button to the right of the **Format string field** and examine the legend in the lower section of the menu, then construct your custom string using the building blocks of your choice.

c Coordinated universal time (yyyy-MM-ddTHH:mm:ss.fffK)

u Universal sortable date time (yyyy-MM-dd HH:mm:ssK)

s Sortable date time (yyyy-MM-ddTHH:ss:mm)

o yyyy-MM-ddTHH:mm:ss.fffffffzz

r RFC1123 date time (ddd, dd MMM yyyy HH:mm:ss GMT)

y Year

M Month

d Day of month

H Hours; 24-hour clock

h Hours; 12-hour clock

m Minutes

s Seconds

f Fractions of a second; Shows 0

F Fractions of a second; does not show 0

K Time zone designator

z Time zone designator

t Time marker string

g Period/era string

3. When you have finished, click **OK** to save your changes.

7.2.17.3.4 Customizing the Event List Font You can customize the font used to display the events in the list as follows:

1. From the **Options** menu, select **Font**.

The **Font** window appears.
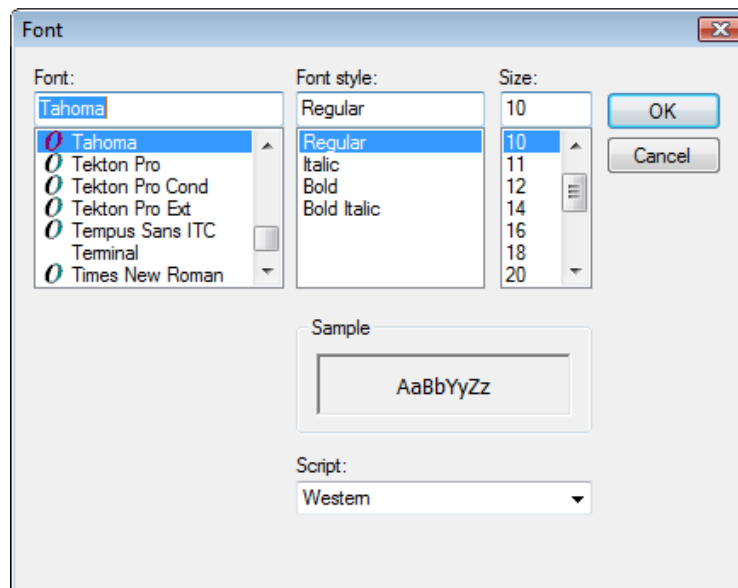
2. In the **Font** window, make your changes, then click **OK**.

7.2.17.4 Configuring Event Capture Hot Keys

You can configure the Trace Controller utility to start and stop event capture using hot keys as follows:

1. From the **Options** menu, select **Hot Keys**. The **Hot Keys** window appears:
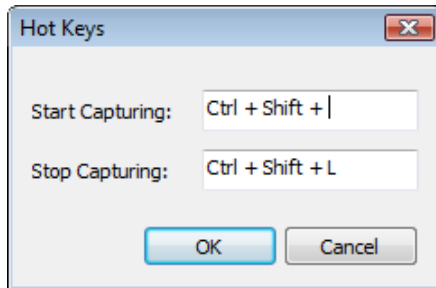
2. Configure the **Start Capturing** hot key:

   a. Click within the **Start Capturing** field.

   b. Press the desired key combination. The combination will appear in the field.

3. Configure the **Stop Capturing** hot key:

   a. Click within the **Stop Capturing** field.

   b. Press the desired key combination. The combination will appear in the field.

4. Click **OK** to save your changes.

7.2.17.5 Using the Trace Controller Utility in Command Line Mode

The Trace Controller utility can be launched and configured from the command line without the need to interact with its graphical interface. This section explains the command-line syntax accepted by the utility.

7.2.17.5.1 Command Line Switch Reference The Trace Controller utility accepts the following command-line switches. Required switches are shown in bold; non-bold switches are optional.

Switch	Purpose
/start	Start logging
/stop	Start logging
/boot	Start logging on boot
/noui	Start in silent mode (suppress graphical interface)
/path	Specifies the path in which log files will be stored in the following format: /path "<path_to_log_files>. If not specified, log files will be written to %SYSTEMROOT%\System32\LogFiles\Vgo. (This default folder is only accessible to users with administrative privileges.)
/event	Specifies the event type(s) to log in the following format: /event "EventType1 "[*verbosity level*] [*write mode*] [log file size] If omitted, events of all currently supported types (except kernel) will be logged.

Switch	Purpose
/level	Specifies the maximum logging verbosity level in the following format:
	/level *x*
	where *x* is an integer from 1 - 5. The available verbosity levels are:
	1 - Critical, 2 - Error, 3 - Warning, 4 - Information, 5 - Debug
	(The default verbosity level is 4.)
/circular	Specifies the log file write mode to be circular. In this mode, once the maximum log file size is reached, the utility begins overwriting old data in chronological order.
	The log is cleared each time logging is started. This is the default mode.
/sequential	Specifies the log file write mode to be sequential. In this mode, once the maximum log file size is reached, the utility stops logging. The log is cleared each time logging is started, unless you also specify the /append switch.
/append	If /sequential is used, the utility will continue writing to the log file at the end of the existing data instead of clearing it.
/fsize	Specifies the maximum size of the log file in megabytes in the following format:
	/fsize *x* (The default size is 20MB.
filename	Specifies the log file name to open for viewing in the following format:
	TraceController.exe "<path_to_log_file>\<log_file_name>"

7.2.17.5.2 Command-Line Use Examples The following are examples of operating the Trace Controller utility from the command line.

Starting Logging

To start logging, use the /start switch, plus one of the optional startup switches.

```
TraceController.exe /start [/noui] [/boot] [/path "<log_file_path>"]
```

For most troubleshooting scenarios, you will want to log all supported event types at the debug verbosity level and using Oracle-specified defaults for all other configuration options:

```
TraceController.exe /start /level 5
```

Specifying Logging Options for Multiple Event Types

When specifying more than one event type, you have the option to specify custom logging options for each individual type, as shown below. You can also specify them globally after specifying the event types, in which case all event types will be logged with the same configuration options.

Custom configuration options for each event type:

```
TraceController.exe /start /noui /path "T:\Oracle\TraceLogs"
```

```
/event "EventType1" /level 2 /circular /fsize:10 /event "EventType2"
/level 3 /sequential /append
```

Global configuration options for all event types:

```
TraceController.exe /start /noui /path "T:\Oracle\TraceLogs"
```

```
/level 2 /circular /fsize 10 /event "EventType1" /event "EventType2"
```

Stopping Logging

To stop logging, use the /stop switch:

```
TraceController.exe /stop
```

Viewing a Log File

You can open one or more log files for viewing as follows:

```
TraceController.exe "logfile1" "logfile2" … "logfile3"
```

7.2.18 Authentication Manager Error Messages

This section lists the messages logged in Authentication Manager during smart card authentication.

7.2.18.1 Warning Level Messages

Event Message	Description
Failed to retrieve the random password from the registry	This message can be ignored if the user has just completed the First Time Use (FTU) process, otherwise this indicates that information expected to be in the registry is missing. Check previous logs to ensure the random password was successfully saved and verify that synchronization process has completed successfully.
Failed to retrieve the PIN from the registry	This message can be ignored if the user has just completed the FTU process, or the first time after configuration was changed to store the PIN. Otherwise this indicates that information expected to be in the registry is missing. Check previous logs to ensure the PIN was successfully saved and verify that synchronization process has completed successfully.
Failed to retrieve the certificate passphrase from the registry	This message can be ignored if the user has just completed the FTU process, otherwise this indicates that information expected to be in the registry is missing. Check previous logs to ensure the passphrase was successfully saved and verify that synchronization process has completed successfully.

7.2.18.2 Error Level Messages

Event	Description
Smart card selection failed	Either the user canceled out of the smart card selection dialog, or the inserted smart card was not recognized by the system. Check to ensure that the proper middleware for the smart card is installed and configured correctly.
Exporting session key failed	Could not export a session key off of the smart card. Verify that the "SmartcardAPI" console setting is configured properly for the middleware. Some middleware may not support exporting session keys.
Importing session key failed	Could not import a session key onto the smart card. Verify that the "SmartcardAPI" console setting is configured properly for the middleware and verify that synchronization process has completed successfully.
Failed to set application data on the smart card	Application data could not be stored on the smart card. This message can be ignored if Kiosk Manager is not in use. Verify that the middleware includes support for PKCS #11 and the smart card is not "read only."
Failed to get application data from the smart card	This error message is usually encountered when application data could not be successfully stored on the smart card.

Event	Description
Failed to get the smart card serial number	The middleware does not support retrieving the smart card serial number. This message can be ignored if Kiosk Manager is not in use.
Failed to enumerate encryption certificate key containers	The Cryptographic Service Provider (CSP) installed by the middleware does not support enumerating key containers on the smart card.
Failed to locate logon certificate	A smart card logon certificate could not be located on the card. Verify that the logon certificate is present on the card and is the default certificate.
Failed to locate encryption certificate	If this error is encountered during FTU, no encryption certificates could be located on the card. The smart card logon certificate cannot be used for this purpose. Verify that a separate, non-logon encryption certificate is present on the card.
	If this error is encountered after successful FTU, verify that the encryption certificate used during FTU is present on the card and available for use.
Failed to obtain exchange key	The exchange key could not be obtained for use. If configured for logon certificates, verify that the certificate is available on the card for use. If SSO keys are configured, verify that the SSO container has been created on the card and contains keys.
Failed to create session key	A session key could not be created on the card. Verify that the "SmartcardAPI" console setting is configured properly for the middleware and the smart card is not "read only."

7.2.19 Regular Expression Syntax

The following operators and meta-characters can be used to specify a text string pattern that the Agent uses to detect specific application windows. See Section 2.13.4.13, "Add or Edit a Title on the Windows Matching Tab" for more information.

The following explanations are adapted for the .NET regular expression reference. The complete description and syntax of regular expressions can be found on the Microsoft Developer Network website (www.msdn.microsoft.com).

Symbol	Grouping
[ ]	Indicates a character class that matches any character inside the brackets.
	Example: [abc] matches "a," "b," and "c."
( )	Indicates a character grouping operator.
	Example: (\d+,)*\d+ matches a list of numbers separated by commas (such as "1" or "1,23,456").
{ }	Indicates a match group.
	Example: {0-9+}-{0-9+} matches "100-1234," where the two match groups are "100" and "1234," respectively.
|	Separates two expressions, exactly one of which matches.
	Example, T|the matches "The" or "the").

Symbol	Matching
.	Matches any single character.

Symbol	Matching
^	If ^ occurs at the start of a character class, it negates the character class. A negated character class matches any character except those inside the brackets. Example, `[^abc]` matches all characters except "a", "b,",and "c."
	If ^ is at the beginning of the regular expression, it matches the beginning of the input.
	Example, `^[abc]` will only match input that begins with "a," "b," or "c".
$	At the end of a regular expression, $ matches the end of the input. Example: `[0-9]$` matches a digit at the end of the input.
-	In a character class, a hyphen indicates a range of characters.
	Example: `[0-9]` matches any of the digits "0" through "9."

Symbol	Repeat Operation
!	Negates the expression that follows.
?	Indicates that the preceding expression is optional: it matches once or not at all.
	Example: [0-9][0-9]? matches "2" and "12").
+	Indicates that the preceding expression matches one or more times.
	Example: `[0-9]+` matches "1," "13," "666," and so on.
*	Indicates that the preceding expression matches zero or more times.
??, +?, *?	"Non-greedy" versions of ?, +, and *. These match as little as possible, unlike the greedy versions which match as much as possible.
	Example: given the input "<abc><def>," `<.*?>` matches "<abc>" while `<.*>` matches "<abc><def>."

Escape and Abbreviation

\   Escape character that forces the next character to be interpreted literally. Example: `[0-9]+` matches one or more digits, but `[0-9]\+` matches a digit followed by a plus character).

If \ is followed by a number n, it matches the nth match group (starting from 0).

Example: `<{.*?}>.*?</\0>` matches "<head>Contents</head>"

The \ is also used for abbreviations as described in the table below.

Abbreviation	Meaning	Matches
\a	Any alphanumeric character	`[a-z A-Z 0-9]`
\b	White space (blank)	`[ \\t]`
\c	Any alphabetic character	`[a-z A-Z]`
\d	Any decimal digit	`[0-9]`
\h	Any hexadecimal digit	`[0-9 a-f A-F]`
\n	New line	`\r|\r?\n`
\q	A quoted string	`\"[^\"]*\"|\'[^\']*\'`
\w	A simple word	`[a-z A-Z]+`
\z	An integer	`[0-9]+`

7.2.20 Command-Line Options

You can invoke Logon Manager from the command line to perform certain tasks.

Note: Items in [brackets] are optional in this section only.

Task	Use/Description	
Backup	`ssoshell.exe/mobility /backup [path] /silent [confirm]`	
	Example: `[path]`	The actual path to the directory where the backup file is placed. (Default: the last directory in which a command line backup file was stored, or where `Shell:AutoBackupPath` points.)
	Example: `silent`	Do not show the Backup/Restore Wizard when performing the backup.
	Example: `[confirm]`	Show all dialogs. When doing a silent backup where the confirm switch is not present, the user does not see the Yes/No dialog and the Agent defaults to Yes. (Example of a confirm dialog: "Overwrite backup file?")
Logon Manager	`ssoshell.exe`	
	Example	Show Logon Manager
No FTU	`ssoshell.exe/background /noftu`	
	Description	Prevents the Agent from starting twice when logging on to the computer. Enable in the `Userinit` registry key, which is located in `HKLM\Software\Microsoft\ Windows NT\Current Version\Winlogon`.
	Description	Prevents the Agent from starting twice when logging on to the computer. Enable in the `Userinit` registry key, which is located in `HKLM\Software\Microsoft\ Windows NT\Current Version\Winlogon`.
	Description	Using `/noftu` ensures that the Agent does not run for users who do not have it in their Windows Startup folder. This allows the administrator to roll out Logon Manager to only specific (not all) users of a particular computer.
Options	`ssoshell.exe/options`	
	Example	Show the Settings property page.
Restore	`ssoshell.exe/mobility /restore [path] /silent [confirm]`	
	Example:`[path]`	The actual path to the directory where the backup file exists. (Default: the last directory to which a command line backup file was stored, or where `Shell:AutoBackupPath` points.)
	Example: `silent`	Do not show the Backup/Restore Wizard when performing the backup.

Task	Use/Description	
	Example: `[confirm]`	Show all dialogs. When doing a silent backup and the confirm switch is not present, the user will not see the Yes/No dialog and the Agent will default to Yes. (Example of a confirm dialog: "Backup file has been restored")
	Example: `Notes`	The restore password submitted by default is the Windows password. The restore command is executed with a startup task (see Section 2.17.9, "Custom Actions Settings").
Setup	`ssoshell.exe/setupmgr`	
	Example	Show the Setup Wizard.
Shutdown	`ssoshell.exe/shutdown`	
Startup	`ssoshell.exe/background`	
Synchronize	`ssoshell.exe/syncmgr /sync`	Execute synchronization with the first synchronizer in the Sync Order list (see Section 2.17.7, "Synchronization Settings"; displays a logon to connect to the first-listed synchronizer.

7.2.21 Character Codes and Keys

This section lists the various codes and keys used to send keystrokes to Logon Manager.

7.2.21.1 Codes for VTabKeyN (Windows)

Code	Meaning
`` `DELAY=N` ``	`N` is the number of milliseconds to delay
`` `VKEY=N` ``	`N` is the virtual key code to send

Example sending a Tab, End, Space, a 1.5 second delay, Logon username , Space, the username/ID, Home, a 0.35 second delay, Tab, and then the password:

```
VTabKey1=`VKEY=9``VKEY=35` `DELAY=1500`Logon username`VKEY=32`
```

```
VTabKey2=`VKEY=36``DELAY=350``VKEY=9`
```

7.2.21.2 Codes for VirtualKeyCode and VKEY (Windows)

These codes are used in the application configuration file (`entlist.ini`) to send specific keystrokes to Windows logon or password change form fields. They are listed here for reference only. Use the **SendKeys (Windows)** dialog to specify keystrokes for a Windows application. See Chapter 2.12.3, "Adding Windows Applications" for more information.

Key	Code	Key	Code	Key	Code	Key	Code
Break	3	5	53	V	86	F5	116
Backspace	8	6	54	W	87	F6	117

Key	Code	Key	Code	Key	Code	Key	Code
Tab	9	7	55	X	88	F7	118
Clear	12	8	56	Y	89	F8	119
Enter	13	9	57	Z	90	F9	120
Shift	16	A	65	Left Windows	91	F10	121
Ctrl	17	B	66	Right Windows	92	F11	122
Alt	18	C	67	NumPad 0	96	F12	123
Caps Lock	20	D	68	NumPad 1	97	F13	124
Esc	27	E	69	NumPad 2	98	F14	125
Spacebar	32	F	70	NumPad 3	99	F15	126
Page Up	33	G	71	NumPad 4	100	F16	127
Page Down	34	H	72	NumPad 5	101	F17	128
End	35	I	73	NumPad 6	102	F18	129
Home	36	J	74	NumPad 7	103	F19	130
Left	37	K	75	NumPad 8	104	F20	131
Up	38	L	76	NumPad 9	105	F21	132
Right	39	M	77	Asterisk (*)	106	F22	133
Down	40	N	78	Plus (+)	107	F23	134
Print Scrn	44	O	79	Minus (-)	109	F24	135
Help	47	P	80	Period (.)	110	Num Lock	144
0	48	Q	81	Slash (/)	111	Scroll Lock	145
1	49	R	82	F1	112	Left Shift	160
2	50	S	83	F2	113	Right Shift	161
3	51	T	84	F3	114	Left Ctrl	162
4	52	U	85	F4	115	Right Ctrl	163

7.2.21.3 Codes for PreKey and TabKey (Host/HLLAPI)

These codes are used in the application configuration file (`entlist.ini`) to send specific keystrokes to HLLAPI-enabled Mainframe/Host logon or password change form fields. They are listed here for reference only. Use the **SendKeys (Host/Mainframe)** dialog to specify keystrokes for a host application. See Section 2.12.5, "Adding Host/Mainframe Applications" for more information.

Char/Cmd	Code	Char/Cmd	Code	Char/Cmd	Code
Alt Cursor	@$	Local Print	@P	PF12/F12	@c
Backspace	@<	Reset	@R	PF13/F13	@d
@	@@	Shift	@S	PF14/F14	@e

Char/Cmd	Code	Char/Cmd	Code	Char/Cmd	Code
Alt	@A	Dup	@S@x	PF15/F15	@f
Field -	@A@-	Field Mark	@S@y	PF16/F16	@g
Field +	@A@+	Tab (Right Tab)	@T	PF17/F17	@h
Field Exit	@A@E	Cursor Up	@U	PF18/F18	@i
Alt Cursor	@$	Cursor Down	@V	PF19/F19	@j
Erase Input	@A@F	Cursor Left	@L	PF20/F20	@k
Sys Request	@A@H	Cursor Right	@Z	PF21/F21	@l
Insert Toggle	@A@I	Page Up	@u	PF22/F22	@m
Cursor Select	@A@J	Page Down	@v	PF23/F23	@n
Attention	@A@Q	End	@q	PF24/F24	@o
Print Screen	@A@T	Home	@0	PA1	@x
Hexadecimal	@A@X	PF1/F1	@1	PA2	@y
Cmd/Func Key	@A@Y	PF2/F2	@2	PA3	@z
Print (PC)	@A@t	PF3/F3	@3	PA4	@+
Back/Left Tab	@B	PF4/F4	@4	PA5	@%
Clear	@C	PF5/F5	@5	PA6	@&
Delete	@D	PF6/F6	@6	PA7	@'
Enter	@E	PF7/F7	@7	PA8	@(
Erase EOF	@F	PF8/F8	@8	PA9	@)
Help	@H	PF9/F9	@9	PA10	@*
Insert	@I	PF10/F10	@a		
New Line	@N	PF11/F11	@b		

7.2.21.4 ftulist.ini Keys

ftulist.ini determines special actions the Agent will take the first time a user starts it. The file can exist as a local file or as a directory server or database object. If it is deployed using synchronization, ftulist.ini is placed in the %AppData/Passlogix% directory.

> **Note:**   All Logon Manager configuration files (including entlist.ini and ftulist.ini) can only be created and edited using the Administrative Console. The information in the topics listed below is provided only for reference.

The following tables list the keys and acceptable values for each section of ftulist.ini:

- Root Keys for ftulist.ini
- Password Windows Section Keys
- My Logons Section Keys
- Bulk Add Logon Section Keys

7.2.21.4.1 Root Keys These settings are used strictly within the [FTU] section and are required.

Example

```
[FTU]

Ver=20020523

Step1=Password Windows

Step2=My Logons
```

First-Time Use Keys	Description	Acceptable values
`Ver = %s`	Required. String of the date of the last `ftulist.ini` file. If the value of this key is higher (newer) than the decimal value in the user's registry (in `HKCU\&\Extensions\SetupManager:Completed`), then the user will see the bulk add list the next time the user starts up the Agent. Example: 20020523	`%s` = string representing the decimal equivalent of a date in yyyymmdd (year-month-date) format, as in 20130523 for May 23, 2013.
`Step1 = %s`	Required, do not alter. Calls the section that launches Primary Logon Method. This module forces the user to select an authenticator.	`%s` = "Password Windows"
`Step2 = %s`	Required, do not alter. Calls the section that launches Access Manager. This module enables bulk adding of credentials.	`%s` = "My Logons"

7.2.21.4.2 Password Windows Section Keys These settings are required and used strictly within the Password Windows section.

Example

```
[Password Windows]

ExtensionName=<core>

Action1=Password Window
```

First-Time Use Keys	Description	Acceptable values
`ExtensionName = %s`	Required, do not alter. Internal name of the extension module.	`%s` = "<core>"
`Action1 = %s`	Required, do not alter. Launches primary logon method. This module forces the user to select an authenticator.	`%s` = "Password Window"

7.2.21.4.3 My Logons Section Keys These settings are required and used strictly within the [My Logons] section.

Example 1

```
[My Logons]
ExtensionName=AccessManager
Section1=Corporate Win App
Section2=Intranet
&
```

First-Time Use Keys	Description	Acceptable values
ExtensionName = %s	Required, do not alter. Internal name of the extension module.	%s = "AccessManager"
Section%d = %s	Required, do not alter. Specifies logons to include in the bulk add wizard.	%d = consecutive integers %s = application logon section name; link to relevant logon class section

7.2.21.4.4   Bulk Add Logon Section Keys These settings are required and used in each bulk-add logon section.

Example 1

```
[My Logons]
ExtensionName=AccessManager
Section1=Corporate Win App
Section2=Intranet
```

Example 2

```
[Intranet]
ConfigKey=*Other Webs
ConfigName=Corporate Intranet
FTU_NeedID=0
FTU_NeedOther=0
FTU_NeedPwd=1
FTU_CONFIRMID=0
FTU_CONFIRMOTHER=0
FTU_CONFIRMPASSWORD=1
URL=Corp Intranet
&
```

First-Time Use Keys	Description	Acceptable Values
ConfigKey = %s	Link to logon configuration in entlist.ini	%s = application logon section name in entlist.ini or applist.ini. Use [*Mainframe] for host/mainframe logons, [*Other Webs] for Web logons, [*Online Services] for Online service logons, and [*Other Apps] for other Windows application logons.
ConfigName = %s	The name to use in the First-Time Use Wizard to describe the logon.	%s = application logon name
Description = %s	The name to use in Logon Manager to describe the logon.	%s = application logon name
FTU_CONFIRMID = %b	Flag indicating if the First-Time Use Wizard will require the user to confirm username/ID (optional).	%b = 0, user will not have to confirm username/ID (default) %b = 1, user will have to confirm username/ID
FTU_CONFIRMOTHER = %b	Flag indicating if the First-Time Use Wizard will require the user to confirm a third field, if one exists (optional).	%b = 0, user will not have to confirm third field (default) %b = 1, user will have to confirm third field

First-Time Use Keys	Description	Acceptable Values
`FTU_CONFIRMPASSWORD = %b`	Flag indicating if the First-Time Use Wizard will require the user to confirm password (optional).	`%b = 0`, user will not have to confirm password (default)
		`%b = 1`, user will have to confirm passwo
`FTU_NeedID = %b`	Flag to indicate whether the application requires a username/ID.	`%b = 0`, application does not require a username/ID
		`%b = 1`, logon requires a username/ID (default)
`FTU_NeedOther = %b`	Flag to indicate whether the application requires a third field (optional).	`%b = 0`, application does not require a thi field (default)
		`%b = 1`, application requires a third field
`FTU_NeedPwd = %b`	Flag to indicate whether the application requires a password.	`%b = 0`, application does not require a password
		`%b = 1`, logon requires a password (default)
`URL = %s`	Section name in `entlist.ini` for a Web or Host application, or URL for a Web site that is not predefined in `entlist.ini`.	`%s =` Web/Host section name or Web UR

7.2.21.5 entlist.ini Keys

The administrator designates the directory where the `entlist.ini` file resides. In most instances, this should be a subdirectory under the Logon Manager program directory.

> **Note:** All Logon Manager configuration files (including `entlist.ini` and `ftulist.ini`) can only be created and edited using the Administrative Console. The information in the topics listed below is provided only for reference.

This is also the format for synchronizer objects that override local `entlist.ini` files.

> **Note:** A directory-based object causes the Agent to ignore any local `entlist.ini` file. The remote object (if it exists) overwrites a local `entlist.ini` file when downloaded.

Then, `entlist.ini` is merged with `applist.ini` to create a new file (`aelist.ini`) in the `%AppData%\Passlogix` directory. The `aelist.ini` file is overwritten periodically, including when Logon Manager launches, when it re-merges `applist.ini` and `entlist.ini`. The Agent then uses `aelist.ini` to detect known applications.

The tables in the following topics list the keys and acceptable values for each section of `entlist.ini`.

- Root Keys for `entlist.ini`
- Windows Application Keys
- Web Application Keys
- Host/Mainframe Application Keys
- Password Policy Keys

7.2.21.5.1 Root Keys These settings are used strictly within the `[*Root]` section.

Example 1

```
[*Root]
Section1=*Other Apps
Section2=*Other Webs
Section3=*Mainframe
AppsMaxRetry=1
WebMaxRetry=3
HostMaxRetry=2
WebTimeout=90
&
```

Global Application Keys	Description	Acceptable values
`[*Root]`	Root section, from which application types (logon classes) are derived.	N/A
`AppsHideConfirmPW = %b`	Indicates whether to hide the password confirmation field in the Logon Error dialog for all Windows applications.	`%b = 0`; do not hide confirmation field (default)
		`%b = 1`; hide confirmation field
`AppsMaxRetry = %d`	Indicates the number of logon retries for all Windows applications the Agent makes before displaying the Logon Error dialog.	`%d` = the number of retries (default: 0)
`AppsTimeout = %d`	Indicates the maximum time between successive logon attempts that will trigger Error Loop detection for all Windows applications.	`%d` = amount of time in seconds (default: 30)
`MainframeHideConfirmPW = %b`	Indicates whether to hide the password confirmation field in the Logon Error dialog for all Host applications.	`%b = 0`; do not hide confirmation field (default)
		`%b = 1`; hide confirmation field
MainframeMaxRetry = %d	Indicates the number of logon retries for all Host applications the Agent makes before displaying the Logon Error dialog.	`%d` = the number of retries (default: 0)
MainframeTimeout = %d	Indicates the maximum time between successive logon attempts that will trigger Error Loop detection for all Host applications.	`%d` = amount of time in seconds (default: 30)
Section%d = %s	Declaration of supported subsections.	`%d` = consecutive integers
	Because *Other Webs, *Online Services, and *Other Apps are defined in `applist.ini`, they need not be defined in `[*Root]` in `entlist.ini`.	`%s` = *Other Apps: (Windows applications)
		`%s` = *Mainframe: (Host/Mainframe applications)
		`%s` = *Other Webs: (Predefined Web applications)
		`%s` = *Online Services
WebHideConfirmPW = %b	Indicates whether to hide the password confirmation field in the Logon Error dialog for all Web applications.	`%b = 0`; do not hide confirmation field (default)
		`%b = 1`; hide confirmation field
WebMaxRetry = %d	Indicates the number of logon retries for all Web applications the Agent makes before displaying the Logon Error dialog.	`%d` = the number of retries (default: 0)

Global Application Keys	Description	Acceptable values
WebTimeout = %d	Indicates the maximum time between successive logon attempts that will trigger Error Loop detection for all Web applications.	%d = amount of time in seconds (default: 30)

7.2.21.5.2 Application Type Section Keys These settings are used for the Windows, Web, and Host application sections that delineate the list of predefined applications.

Example 1

```
[*Other Apps]
Section1=Corporate WinApp
&
[*Other Webs]
Section1=Corporate Intranet
&
[*Mainframe]
Section1=Corporate Mainframe
```

Global Application Keys	Description	Acceptable Values	
[%s]	Section heading that identifies an application category section.	%s = [*Other Apps]:	(Windows applications)
		%s = [*Mainframe]:	(Host/Mainframe applications)
		%s = [*Other Webs]:	(Predefined Web applications)
Section%d = %s	Declaration of application sections.	%d = consecutive integers	
		%s = section name	

7.2.21.5.3 Windows Application Keys These settings are used within applications delineated in the [*Other Apps] section.

Example 1

```
[*Other Apps]
Section1=Corporate WinApp
&
[Corporate WinApp]
(the keys below)
```

Windows Application Keys	Description	Acceptable Values
AllowReveal = %b	Flag that enables or disables the Reveal button for password in Wizards and property pages.	%b = 0; disabled %b = 1; enabled (default)

Windows Application Keys	Description	Acceptable Values
`AppPathKey%d = %s`	Windows registry key identifying the application associated with a logon to match against running processes. Used in combination with the WindowTitle for exact matching of logon requests. `%d` is replaced with a number, starting at `1`, so that multiple registry keys can be associated with a single logon.	`%d` = consecutive integers `%s` = application name string used in Windows registry (typically corresponds to executable name)
`AutoOK = %b`	Flag instructs the Agent to automatically select OK for this application logon after insertion of logon data.	`%b` = `0`; disabled `%b` = `1`; enabled (default)
`ChangeTitle%d = %s`	Text matched against password change window titles to identify password change requests. `%d` is replaced with a number, starting at `1`, so that multiple windows can be identified for a single password change request. There must be a duplicate WindowTitle entry for each ChangeTitle entry.	`%d` = consecutive integers `%s` = window title string
`ChgCtrl0 = %d`	Control ID used to identify the username/ID field in a password-change request window.	`%d` = `-1`; change request does not require a username/ID `%d` = `1`; change request requires a username/ID, but it will be sent to the application using Send Keys. If this value is `1`, all other Control IDs (`IDCtrl`, `PassKeyCtrl`, `OtherCtrl1`, `OtherCtrl2`, `OKCtrl`, `ChgCtrl1`, `ChgCtrl2`, and `ChgCtrl3`) must also be `1` or `-1`. `%d` = `2 - 99,999`; Control ID value
`ChgCtrl1 = %d`	Control ID used to identify the old password field in a password change request window.	`%d` = `-1`; change request does not require an old password `%d` = `1`; change request requires a password, but it will be sent to the application using Send Keys. If this value is `1`, all other Control IDs must also be `1` or `-1`. `%d` = `2 - 99,999`; Control ID value
`ChgCtrl2 = %d`	Control ID used to identify the new password field in a password change request window.	`%d` = `-1`; change request does not require a new password. `%d` = `1`; change request requires a password, but it will be sent to the application using Send Keys. If this value is `1`, all other Control IDs must also be `1` or `-1`. `%d` = `2 - 99,999`; Control ID value

Windows Application Keys	Description	Acceptable Values
`ChgCtrl3 = %d`	Control ID used to identify the password confirmation field in a password change request window.	`%d = -1`; change request does not require a "confirm new password" entry. `%d = 1`; change request requires a "confirm new password" entry, but it will be sent to the application using SendKeys. If this value is `1`, all other Control IDs must also be `1` or `-1`. `%d = 2 - 99,999`; Control ID value
`ConfigName = %d`	Control ID identifying the control that contains the text used to create the initial configuration name when the user adds this logon.	`%d = 1 - 99,999`; Control ID value
`CPWFlag = %d`	Determines the behavior of the Password Change Wizard, for specific applications, when a user encounters a password-change request. This key is specified in the application's root section, not in a password-change subsection. **Note:** This setting can also be set globally, for all applications, via the Registry.	`%d = 1`; Prompts user with Password Change Wizard (default). `%d = 2`; Prompts user to manually enter a new password, but also provides the option of having the Agent automatically generate the password. `%d = 4`; Generates the new password automatically, but also provides the option of manually creating the new password. `%d = 10`; Prompts user to manually enter a new password, without providing the option of having the Agent automatically generate the password. `%d = 12`; Generates the new password automatically, without providing the option of manually creating the new password.
`CtrlOrder = %s1, %s2, %s3&`	Determines the order in which fields are sent when `UseSendKeys` is enabled. For example, specifying `CtrlOrder = OtherCtrl1, IDCtrl, PassKeyCtrl` tells the Agent that the tab order in the dialog should be `OtherCtrl1`, then `IDCtrl`, followed by `PassKeyCtrl`. For logons, the default order is `IDCtrl, PassKeyCtrl, OtherCtrl1, OtherCtrl2`. For password changes, the default order is `ChgCtrl0, ChgCtrl1, ChgCtrl2, ChgCtrl3`. **Note:** This setting applies only when `UseSendKeys` is enabled and works only with Windows applications.	`%s1` = The first field sent `%s2` = The second field sent `%s3` = The third field sent etc.

Windows Application Keys	Description	Acceptable Values
Description = %s	Text describing this application, also stored in the Description field in Logon Manager.	%s = any string
ExtMap = %s	Windows file extension associated with a logon. Allows the Agent to map an icon to the configuration.	%s = three-character string for file extension
ForceReauth = %b	Force the user to reauthenticate before providing credentials to this application. **Note:** Applies to all subsections; the user would have to reauthenticate multiple times in a multiple-section password change scenario.	%b = 0; do not require reauthentication (default) %b = 1; require reauthentication
Group = %s	Group section name that this application is a part of. Used when configuring for credential sharing groups. Special values include: ■ **LDAP:** Application uses LDAP Directory Server authenticator password. ■ **Domain:** Application uses the Windows authenticator password. **Note:** Must set Windows Registry entry PWSEnable=1 to enable Groups.	%s = the section name of the application group that the application belongs to.
HideConfirmPW = %b	Determines whether to hide the password confirmation field in the Logon Error dialog.	%b = 0; do not hide confirmation field (default) %b = 1; hide confirmation field
IDCtrl = %d	Identifies the username/ID control field and/or the mechanism to provide the username/ID data to the appropriate username/ID control.	%d = 0; the user must use the Agent's "teaching tool" mechanism during application setup (default) %d = -1; application does not require a username/ID %d = 1; application requires a username/ID, but it will be sent to the application using Send Keys. If this value is set to 1, all other Control IDs (PassKeyCtrl, OtherCtrl1, OtherCtrl2, OKCtrl, ChgCtrl0, ChgCtrl1, ChgCtrl2, and ChgCtrl3) must also be 1 or -1. %d = 2 - 99,999; username/ID Control ID value
IDCtrlType = %d	Identifies the control type of the username/ID control field.	%d = 0; edit control (default) %d = 1; combobox control %d = 2; listbox control

Windows Application Keys	Description	Acceptable Values
IgnoreClassName = %s	Identifies the class name of the logon or password-change window that should be ignored when submitting credentials. Used in cases where an application contains a second, hidden logon or password-change window.	%s = class name string
InteractionMode = %b	Prevents the Agent from attaching to the application's window's message queue.	%b = 0; disabled (default) %b = 1; enabled
Match%d = %s	Maps to a matching section for the application. Use this method if the same application has multiple logon and password change screens. This is most useful when one set of user credentials is for multiple screens within an application. By using this method, the matching sections could be set up for logons, password change (pick and manual), and ignores.	%d = consecutive integers %s = application logon name (logon definition sections)
MaxRetry = %d	Determines the number of logon retries the Agent makes before displaying the Logon Error dialog.	%d = the number of retries (default: 0)
ModuleName%d = %s	Application module name associated with a logon to match against running processes. Used in conjunction with WindowTitle key to identify a specific application logon or password-change request. %d is replaced with a number, starting at 1, so that multiple application modules can be associated with a single logon.	%d = consecutive integers %s = application name string (typically corresponds to executable name)
OKCtrl = %d	Identifies the Control ID of the **OK** button for this application.	%d = 1; use the Agent's internal logic (default) %d = 2 - 99,999; **OK** button Control ID %d = -1; requires the user to manually select **OK**
OtherCtrl1 = %d	Identifies the Control ID of a third logon field and/or the mechanism to provide the additional field data to the appropriate control.	%d = -1; application does not require a third field %d = 1; application requires a third field, but it will be sent to the application using Send Keys. If this value is set to 1, all other Control IDs must also be 1 or -1. %d = 2 - 99,999; third field Control ID value; can be any value if Send Keys is used
OtherCtrl1Type = %d	Identifies the control type of a third logon field.	%d = 0; edit control (default) %d = 1; combobox control %d = 2; listbox control

Windows Application Keys	Description	Acceptable Values
`OtherCtrl2 = %d`	Identifies the Control ID of a fourth logon field and/or the mechanism to provide the additional field data to the appropriate control.	`%d = -1`; application does not require a fourth field
		`%d = 1`; application requires a fourth field, but it will be sent to the application using Send Keys. If this value is set to 1, all other Control IDs must also be 1 or -1.
		`%d = 2 - 99,999`; fourth field Control ID value; can be any value if Send Keys is used
`OtherCtrl2Type = %d`	Identifies the control type of a fourth logon field.	`%d = 0`; edit control (default)
		`%d = 1`; combobox control
		`%d = 2`; listbox control
`OtherLabel1 = %s`	The text label used by the Agent when displaying a third logon field.	`%s` = the text the Agent will display
`OtherLabel2 = %s`	The text label used by the Agent when displaying a fourth logon field.	`%s` = the text the Agent will display
`ParentKey1 = %s`	Maps a subsection to its parent section.	`%s` = parent application/section name
`PassKeyCtrl = %d`	Identifies the password control field and/or the mechanism to provide the password data to the appropriate password control.	`%d = 0`; the user must use the Agent's "teaching tool" mechanism during application setup
		`%d = -1`; application does not require a password
		`%d = 1`; application requires a password, but it will be sent to the application using Send Keys. If this value is set to 1, all other Control IDs must also be 1 or -1.
		`%d = 2 - 99,999`; password Control ID value; can be any value if Send Keys is used
`PassKeyCtrlType = %d`	Identifies the control type of the password control field.	`%d = 0`; edit control (default)
		`%d = 1`; combobox control
		`%d = 2`; listbox control
`PassPolicy = %s`	Identifies which password policy section to associate with this application logon configuration.	`%s` = Policy Section Name
`PresetFocusAll = %b`	Specifies whether to set the focus to a logon field before the Agent actually places data in that field.	`%b = 0`; disabled (default)
		`%b = 1`; enabled
`QuietGenerator = %b`	When set, this flag instructs the Agent to handle password change requests automatically and not inform the user that a password change request has been handled.	`%b = 0`; do not use quiet generator, use standard password change process with user intervention (default)
		`%b = 1`; use quiet generator
`Section%d = %s`	Declaration of application subsections.	`%d` = consecutive integers
		`%s` = subsection name

Windows Application Keys	Description	Acceptable Values
`SystemLogon = %b`	RESERVED. Flag identifying if a logon section is a system logon section.	`%b = 0`; not a system logon section (default) `%b = 1`; system logon section
`Timeout = %d`	Determines the maximum time period between successive logon attempts that will trigger Error Loop detection.	`%d` = amount of time in seconds (default: 30)
`UseSendKeys = %b`	Send fields via keystrokes to the application. If UseSendKeys is selected, then `IDCtrl`, `PassKeyCtrl`, `OtherCtrl1`, `OtherCtrl2`, and (if present) `ChgCtrl0`, `ChgCtrl1`, `ChgCtrl2`, and `ChgCtrl3` variables must all be set to `1`, if needed.	`%b = 0`; do not use Send Keys; use Control IDs (default) `%b = 1`; use Send Keys
`VTabKey%d0 = %d1`	Specifies the character/delay sequence to send before/after each credential field. **Note:** Fields are sent in the order specified by `CtrlOrder`. `UseSendKeys` must also be enabled. To send nothing for the specified value, specify a value of `` `` `` (two back-quotes in a row).	`%d0 = 1`; sequence to send before the first credential field `%d0 = 2`; sequence to send after the first field, before the second - so on; `%d` is not bound. `%d1` = Code sequence to send (see) (default: standard tab key)
`VTabKeyPWC%d0 = %d1`	Specifies the character/delay sequence to send before/after each credential field. **Note:** Fields are sent in the order specified by `CtrlOrder`. `UseSendKeys` must also be enabled. To send nothing for the specified value, specify a value of `` `` `` (two back-quotes).	`%d0 = 1`; sequence to send before the first credential field `%d0 = 2`; sequence to send after the first field, before the second - so on; `%d` is not bound. `%d1` = Code sequence to send (see) (default: standard Tab key)
`WindowTitle%d = %s`	Text matched against logon window titles to identify logon requests. `%d` is replaced with a number, starting at `1`, so that multiple windows can be identified for a single logon.	`%d` = consecutive integers `%s` = window title string

7.2.21.5.4 Windows Application Keys for SectionN Subsection These settings are used within subsections delineated by `SectionN`.

Example 1

```
[Corporate WinApp]
Section1=~Corporate WinApp Logon
Section2=~Corporate WinApp Password Change
&
[~Corporate WinApp Logon]
(the keys below)
```

Windows Application Keys	Description	Acceptable values
`AppPathKey%d = %s`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`ChangeTitle%d = %s`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`ChgCtrl0 = %d`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`ChgCtrl1 = %d`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`ChgCtrl2 = %d`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`ChgCtrl3 = %d`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`CtrlOrder = %s1, %s2, %s3&`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`IDCtrl = %d`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`IDCtrlType = %d`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`IgnoreClassName = %s`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`InteractionMode = %b`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`Match%d = %s`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`ModuleName%d = %s`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`OKCtrl = %d`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`OtherCtrl1 = %d`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`OtherCtrl1Type = %d`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`OtherCtrl2 = %d`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`OtherCtrl2Type = %d`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`ParentKey1 = %s`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`PassKeyCtrl = %d`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`PassKeyCtrlType = %d`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`VTabKey%d0 = %d1`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`VTabKeyPWC%d0 = %d1`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`UseSendKeys = %b`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`WindowTitle%d = %s`	(See Windows Application Keys, above)	(See Windows Application Keys, above)

7.2.21.5.5 Windows Application Keys for MatchN Subsection These settings are used within subsections delineated by `MatchN`.

Example 1
```
[Corporate WinApp
Section1=~Whatever subsection
Match1=~Corporate WinApp Logon Match
Match2=~Corporate WinApp Ignore Match
&
[~Corporate WinApp Ignore Match]
(the keys below)
```

Match Section Keys	Description	Acceptable values
`ChangeTitle%d = %s`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`ChgCtrl0 = %d`	(See Windows Application Keys, above)	(See Windows Application Keys, above)

Match Section Keys	Description	Acceptable values
`ChgCtrl1 = %d`	(See Windows Application Keys, above)	(See Windows Application Keys, abov
`ChgCtrl2 = %d`	(See Windows Application Keys, above)	(See Windows Application Keys, abov
`ChgCtrl3 = %d`	(See Windows Application Keys, above)	(See Windows Application Keys, abov
`Field%d0 = %d1,%s1,%s2,%s3`	The match criteria for the fields. `%d1` is replaced with a number, starting at `1`, so that multiple matching criteria could be set up for one screen. `%d2` is replaced with the Control ID of the matching criteria. `%s1` is replaced with the control type. `%s2` is replaced with the comparison operator. `%s3` is replaced with the compare value.	`%d0` = consecutive integers `%d1` = Control ID of the matching criteria `%s1` = the control type could be the following, with the appropriate value `%s3`: `Text`: actual text from the control `Style`: numerical value for the style the control `Class`: the class of the control, usuall Edit or Static. `Edit`: edit or combo box controls. `Static`: static controls (for example, text labels). `%s2` = the comparison operator could the following: `EQ`: equals `NE`: not equal `%s3` = compared value
`IDCtrl = %d`	(See Windows Application Keys, above)	(See Windows Application Keys, abov
`OKCtrl = %d`	(See Windows Application Keys, above)	(See Windows Application Keys, abov
`OtherCtrl1 = %d`	(See Windows Application Keys, above)	(See Windows Application Keys, abov
`OtherCtrl2 = %d`	(See Windows Application Keys, above)	(See Windows Application Keys, abov
`ParentKey1 = %s`	(See Windows Application Keys, above)	(See Windows Application Keys, abov
`PassKeyCtrl = %d`	(See Windows Application Keys, above)	(See Windows Application Keys, abov
`Type = %s`	The type of event.	`%s` = `string` for the type: ■ `Logon`: logon events. ■ `Change`: password change events ■ `Confirm`: confirms the new password. ■ `Ignore`: bypass all events for the application.
`WindowTitle%d = %s`	(See Windows Application Keys, above)	(See Windows Application Keys, abov

7.2.21.5.6 Host/Mainframe Application Keys These settings are used within applications delineated in the [*Mainframe] section.

For all keys below that have row/column values, the row/column value starts at 1 (that is, top-left is 1,1).

Note: For Telnet the value must be 1,1.

Example 1

```
[*Mainframe]
Section1=Corporate Mainframe
&
[Corporate Mainframe]
(the keys below)
```

Host Application Keys	Description	Acceptable values
`AllowReveal = %b`	Flag that enables or disables the **Reveal** button for password in Wizards and property pages.	`%b = 0`; disabled `%b = 1`; enabled (default)
`AltTabKey = %d`	Flag to indicate how to send credentials to the host emulator. Normally, credentials are sent through a direct HLLAPI call but this setting specifies using another method. If this is set to 1, then Enter is pressed in between two fields. This is usually used for password change screens that separate the new password and confirmation password into two screens. **Note:** `%d=1` is usually used for password-change scenarios that separate the new-password field and confirm-password into two screens.	`%d = 0`; Use HLLAPI to submit credentials directly to the credential fields (default). `%d = 1`; Replace the Tab key with the Enter key between two fields. `%d = 2`; Use HLLAPI SendKeys and enable support for `CtrlOrder`, `PreKey`, and `TabKeyN`. This is useful for logon scenarios with non-standard credential delimiters.
`AutoOK = %b`	Flag instructs the Agent to automatically send **Enter** for this application logon after insertion of logon data.	`%b = 0`; disabled `%b = 1`; enabled (default)
`CPWFlag = %d`	Determines the behavior of the **Password Change Wizard**, for specific applications, when a user encounters a password-change request. This key is specified in the application's root section, not in a password-change subsection. **Note:** This setting can also be set globally, for all applications, via the Registry.	`%d = 1`; Prompts user with **Password Change Wizard** (default). `%d = 2`; Prompts user to manually enter a new password, but also provides the option of having the Agent automatically generate the password. `%d = 4`; Generates the new password automatically, but also provides the option of manually creating the new password. `%d = 10`; Prompts user to manually enter a new password, without providing the option of having the Agent automatically generate the password. `%d = 12`; Generates the new password automatically, without providing the option of manually creating the new password.

Host Application Keys	Description	Acceptable values
CtrlOrder = %s1,%s2,%s3,%s4,%s5	Determines the order in which fields are sent when AltTabKey=2.	%s1 = The first field sent (default: IDField)
	For example, specifying CtrlOrder=OtherField1,IDField,PassField tells the Agent that the order in the dialog should be OtherField1, then IDField, followed by PassField.	%s2 = The second field sent (default: PassField)
		%s3 = The third field sent (default: OtherField1)
		%s4 = The fourth field sent (default: NewPWField)
		%s5 = The fifth field sent (default: NewPWField2)
		%s5 = The sixth field sent (default: OtherField2)
DelayField = %d	Numeric value in milliseconds for the Agent to delay between actions (entering value into a field).	%d = integer value in milliseconds
Description = %s	Text describing this application, also stored in the **Description** field in Logon Manager.	%s = any string
Field%d0 = %d1, %d2, %s	Strings to match against text fields as displayed on the screen for identifying a host/mainframe logon. %d0 is replaced with a number, starting at 1, so that multiple text strings can be used to uniquely identify a logon. For Telnet applications, the values must be 1,1.	%d0 = consecutive integers
		%d1 = row of first text string character
		%d2 = column of first text string character
		%s = text string
ForceReauth = %b	Force the user to reauthenticate before providing credentials to this application.	%b = 0; do not require reauthentication (default)
	Note: Applies to all subsections; the user would have to reauthenticate multiple times in a multiple-section password change scenario.	%b = 1; require reauthentication
Group = %s	Group section name that this application is a part of. Used when configuring for credential sharing groups. Special values include: ■ **LDAP:** Application uses LDAP Directory Server authenticator password. ■ **Domain:** Application uses the Windows authenticator password. **Note:** Must set Windows Registry entry PWSEnable=1 to enable Groups.	%s = the section name of the application group that the application belongs to.
HideConfirmPW = %b	Determines whether to hide the password confirmation field in the **Logon Error** dialog.	%b = 0; do not hide confirmation field (default)
		%b = 1; hide confirmation field
IDField = %d1, %d2	Location of first input character of username/ID field as displayed on a host/mainframe logon screen. For Telnet applications, this value is ignored and is optional. Set to 1,0 if the field is not present.	%d1 = row of first text string character
		%d2 = column of first text string character
MaxRetry = %d	Determines the number of logon retries the Agent makes before displaying the Logon Error dialog.	%d = the number of retries (default 0)
NewPWField = %d1,%d2	The key-value pair that identifies the location of the new password field.	%d1 = row of first text string character
		%d2 = column of first text string character

Host Application Keys	Description	Acceptable values
NewPWField2 = %d1,%d2	The key-value pair that identifies the location of the new password confirmation field. This is optional. This is not necessary if only one new password field is required.	%d1 = row of first text string character %d2 = column of first text string character
OtherField1 = %d1, %d2	Location of first input character of third logon field as displayed on a host/mainframe logon screen. For Telnet applications, this value is ignored and is optional.	%d1 = row of first text string character %d2 = column of first text string character
OtherField2 = %d1, %d2	Location of first input character of fourth logon field as displayed on a host/mainframe logon screen. For Telnet applications, this value is ignored and is optional.	%d1 = row of first text string character %d2 = column of first text string character
OtherLabel1 = %s	The label presented within the Agent for the third logon field.	%s = text string
OtherLabel2 = %s	The label presented within the Agent for the fourth logon field.	%s = text string
Page%d = %s	Pointer to subsections used for multiple pages for one host/mainframe application. One application logon may have multiple pages.	%d = consecutive integers %s = name of the subsection
ParentKey1 = %s	Maps a subsection to its parent section.	%s = parent application/section name
PassField = %d1, %d2	Location of first input character of password field as displayed on a host/mainframe logon screen. For Telnet applications, the values must be 1,1. Set to 1,0 if the field is not present.	%d1 = row of first text string character %d2 = column of first text string character
PassPolicy = %s	Identifies which password policy section to associate with this application logon configuration.	%s = Policy Section Name
PreKey = %d	A string of characters and mnemonics defining what should be sent prior to any credential submission.	Any combination of characters and/or ASCII mnemonics. Maximum length is 25 characters.
QuietGenerator = %b	When set, this flag instructs the Agent to handle password change requests automatically and not inform the user that a password change request has been handled.	%b = 0; do not use quiet generator, use standard password change process with user intervention (default) %b = 1; use quiet generator
TabKey1 = %d	A string of characters and mnemonics defining what should be sent after IDField is submitted.	Any combination of characters and/or ASCII mnemonics. Maximum length is 25 characters.
TabKey2 = %d	A string of characters and mnemonics defining what should be sent after PassField is submitted.	Any combination of characters and/or ASCII mnemonics. Maximum length is 25 characters.
TabKey3 = %d	A string of characters and mnemonics defining what should be sent after OtherField1 is submitted.	Any combination of characters and/or ASCII mnemonics. Maximum length is 25 characters.
TabKey4 = %d	A string of characters and mnemonics defining what should be sent after NewPWField is submitted.	Any combination of characters and/or ASCII mnemonics. Maximum length is 25 characters.
TabKey5 = %d	A string of characters and mnemonics defining what should be sent after NewPWField2 is submitted.	Any combination of characters and/or ASCII mnemonics. Maximum length is 25 characters.

Host Application Keys	Description	Acceptable values
TabKey6 = %d	A string of characters and mnemonics defining what should be sent after `OtherField2` is submitted.	Any combination of characters and/or ASCII mnemonics Maximu length is 25 characters.
Timeout = %d	Determines the maximum time period between successive logon attempts that will trigger error loop detection.	`%d` = amount of time in seconds (default: 30)

7.2.21.5.7 Host Applications: Keys for PageN Subsection These settings are used within subsections delineated by `PageN`.

Example 1

```
[Corporate Mainframe]
Page1=~Corporate Mainframe Logon
Page2=~Corporate Mainframe Password Change
[~Corporate Mainframe Logon]
(the keys below)
```

Host Application Keys	Description	Acceptable values
AllowReveal = %b	(See Windows Application Keys, above)	(See Windows Application Keys, above)
AltTabKey = %d	(See Windows Application Keys, above)	(See Windows Application Keys, above)
AutoOK = %b	(See Windows Application Keys, above)	(See Windows Application Keys, above)
CPWFlag = %d	(See Windows Application Keys, above)	(See Windows Application Keys, above)
CtrlOrder = %s1,%s2,%s3,%s4,%s5	(See Windows Application Keys, above)	(See Windows Application Keys, above)
DelayField = %d	(See Windows Application Keys, above)	(See Windows Application Keys, above)
Description = %s	(See Windows Application Keys, above)	(See Windows Application Keys, above)
Field%d0 = %d1, %d2, %s	(See Windows Application Keys, above)	(See Windows Application Keys, above)
ForceReauth = %b	(See Windows Application Keys, above)	(See Windows Application Keys, above)
Group = %s	(See Windows Application Keys, above)	(See Windows Application Keys, above)
HideConfirmPW = %b	(See Windows Application Keys, above)	(See Windows Application Keys, above)
IDField = %d1, %d2	(See Windows Application Keys, above)	(See Windows Application Keys, above)
MaskPW = %b	(See Windows Application Keys, above)	(See Windows Application Keys, above)
MaxRetry = %d	(See Windows Application Keys, above)	(See Windows Application Keys, above)
NewPWField = %d1,%d2	(See Windows Application Keys, above)	(See Windows Application Keys, above)
NewPWField2 = %d1,%d2	(See Windows Application Keys, above)	(See Windows Application Keys, above)
OtherField1 = %d1, %d2	(See Windows Application Keys, above)	(See Windows Application Keys, above)
OtherField2 = %d1, %d2	(See Windows Application Keys, above)	(See Windows Application Keys, above)
OtherLabel1 = %s	(See Windows Application Keys, above)	(See Windows Application Keys, above)
OtherLabel2 = %s	(See Windows Application Keys, above)	(See Windows Application Keys, above)
Page%d = %s	(See Windows Application Keys, above)	(See Windows Application Keys, above)
ParentKey1 = %s	(See Windows Application Keys, above)	(See Windows Application Keys, above)
PassField = %d1, %d2	(See Windows Application Keys, above)	(See Windows Application Keys, above)

Host Application Keys	Description	Acceptable values
PassPolicy = %s	(See Windows Application Keys, above)	(See Windows Application Keys, above)
PreKey = %d	(See Windows Application Keys, above)	(See Windows Application Keys, above)
QuietGenerator = %b	(See Windows Application Keys, above)	(See Windows Application Keys, above)
TabKey1 = %d	(See Windows Application Keys, above)	(See Windows Application Keys, above)
TabKey2 = %d	(See Windows Application Keys, above)	(See Windows Application Keys, above)
TabKey3 = %d	(See Windows Application Keys, above)	(See Windows Application Keys, above)
TabKey4 = %d	(See Windows Application Keys, above)	(See Windows Application Keys, above)
TabKey5 = %d	(See Windows Application Keys, above)	(See Windows Application Keys, above)
Timeout = %d	(See Windows Application Keys, above)	(See Windows Application Keys, above)

7.2.21.5.8 Web Application Keys These settings are used within applications delineated in the [*Other Webs] section.

Example 1

```
[*Mainframe]
Section1=Corporate Mainframe
&
[Corporate Mainframe]
(the keys below)
```

Web Application Keys	Description	Acceptable values
AllowReveal = %b	Flag that enables or disables the **Reveal** button for password in Wizards and property pages.	%b = 0; disabled %b = 1; enabled (default)
AutoOK = %b	Flag instructs the Agent to automatically send **Enter** for this application logon after insertion of logon data.	%b = 0; disabled %b = 1; enabled (default)
CPWFlag = %d	Determines the behavior of the **Password Change Wizard**, for specific applications, when a user encounters a password-change request. This key is specified in the application's root section, not in a password-change subsection. **Note:** This setting can also be set globally, for all applications, using the Registry.	%d = 1; Prompts user with **Password Change Wizard** (default). %d = 2; Prompts user to manually enter a new password, but also provides the option of having the Agent automatically generate the password. %d = 4; Generates the new password automatically, but also provides the option of manually creating the new password. %d = 10; Prompts user to manually enter a new password, without providing the option of having the Agent automatically generate the password. %d = 12; Generates the new password automatically, without providing the option of manually creating the new password.
Description = %s	Text describing this application, also stored in the **Description** field in Logon Manager.	%s = any string

Web Application Keys	Description	Acceptable values
ForceReauth = %b	Force the user to reauthenticate before providing credentials to this application. **Note:** Applies to all subsections; the user would have to reauthenticate multiple times in a multiple-section password change scenario.	%b = 0; do not require reauthentication (default) %b = 1; require reauthentication
Group = %s	Group section name that this application is a part of. Used when configuring for credential sharing groups. Special values include: ■ **LDAP:** Application uses LDAP Directory Server authenticator password. ■ **Domain:** Application uses the Windows authenticator password. **Note:** Must set Windows Registry entry PWSEnable=1 to enable Groups.	%s = the section name of the application group that the application belongs to.
HideConfirmPW = %b	Determines whether to hide the password confirmation field in the Logon Error dialog.	%b = 0; do not hide confirmation field (default) %b = 1; hide confirmation field
IDField = %s1,%s2,%s3,%s4	Identification of the field for entering a username/ID. **Note:** If a frame/form/field name consists solely of digits, the enumerated value must be used.	%s1 = Frame name/number %s2 = Form name/number %s3 = Field name/number %s4 = Field type (text/password)
MaxRetry = %d	Determines the number of logon retries the Agent makes before displaying the Logon Error dialog.	%d = the number of retries (default: 0)
NewPWField = %s1,%s2,%s3,%s4	Identification of the field for entering a new password.	%s1 = Frame name/number %s2 = Form name/number %s3 = Field name/number %s4 = Field type (text/password)
NewPWField2 = %s1,%s2,%s3,%s4	Identification of the field for confirming a new password.	%s1 = Frame name/number %s2 = Form name/number %s3 = Field name/number %s4 = Field type (text/password)
OtherField1 = %s1,%s2,%s3,%s4	Identification of the third logon field.	%s1 = Frame name/number %s2 = Form name/number %s3 = Field name/number %s4 = Field type (text/password)
OtherField2 = %s1,%s2,%s3,%s4	Identification of the fourth logon field.	%s1 = Frame name/number %s2 = Form name/number %s3 = Field name/number %s4 = Field type (text/password)
OtherLabel1 = %s	The label presented within the Agent for a third logon field.	%s = text string
OtherLabel2 = %s	The label presented within the Agent for a fourth logon field.	%s = text string

Web Application Keys	Description	Acceptable values
`ParentKey1 = %s`	Maps a subsection to its parent section.	`%s` = parent application/section name
`PassField = %s1,%s2,%s3,%s4`	Identification of the field for entering the password.	`%s1` = Frame name/number `%s2` = Form name/number `%s3` = Field name/number `%s4` = Field type (text/password)
`PassPolicy = %s`	Identifies which password policy section to associate with this application logon configuration.	`%s` = Policy Section Name
`QuietGenerator = %b`	When set, this flag instructs the Agent to handle password change requests automatically and not inform the user that a password change request has been handled.	`%b` = `0`; do not use quiet generator, use standard password change process with user intervention (default) `%b` = `1`; use quiet generator
`Section%d = %s`	Declaration of application subsections.	`%d` = consecutive integers `%s` = subsection name
`StrictURLCheck = %b`	Determines whether to require an exact (case-insensitive) URL match or to use substring matching.	`%b` = `0`; use substring matching (default) `%b` = `1`; use precise matching
`SubmitField = %s1,%s2,%s3,%s4`	Identification of the **Submit** button (or equivalent). The value format is frame name/number, form name/number, field name/number/URL, and Field type. If the field type is image, the field name must be the entire/exact URL. **Note:** This entry is optional. If not specified, the Agent uses its own internal search logic to locate and press this button.	`%s1` = Frame name/number `%s2` = Form name/number `%s3` = Field name/number/URL `%s4` = Field type (submit/image)
`Timeout = %d`	Determines the maximum time period between successive logon attempts that will trigger Error Loop detection.	`%d` = amount of time in seconds (default: 30)
`URL%d = %s`	The address(es) of a Web site's logon page(s). **Note:** If the web address consists of spaces or special characters, use the URL quoting method (RFC 2396) to define the web address. This means substituting `%20` for each space in the URL and substituting similar "`%`"-escaped ASCII hexadecimal values for all characters other than the following: `:  /  ,  .  =  ?  @`	`%d` = consecutive integers starting with 1 `%s` = Web URL

7.2.21.5.9 Web Application Keys for SectionN Subsection These settings are used within subsections delineated by `SectionN`.

Example 1

```
[Corporate WebApp]
Section1=~Corporate Intranet Logon #1
Section2=~Corporate Intranet Logon #2
&
[~Corporate Intranet Logon #1]
```

```
                    (the keys below)
```

Web Application Keys	Description	Acceptable values
`IDField = %s1,%s2,%s3,%s4`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`NewPWField = %s1,%s2,%s3,%s4`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`NewPWField2 = %s1,%s2,%s3,%s4`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`OtherField1 = %s1,%s2,%s3,%s4`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`OtherField2 = %s1,%s2,%s3,%s4`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`ParentKey1 = %s`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`PassField = %s1,%s2,%s3,%s4`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`SubmitField = %s1,%s2,%s3,%s4`	(See Windows Application Keys, above)	(See Windows Application Keys, above)
`URL%d = %s`	(See Windows Application Keys, above)	(See Windows Application Keys, above)

7.2.21.5.10 Password Policy Keys These settings are used within subsections delineated by SectionN in the `[*PasswordPolicies]` section.

Example 1

```
[*PasswordPolicies
Section1=A policy
Section2=PIN
Section3=Windows
&
[A policy]
(the keys below)
```

Password Policy Keys	Description	Acceptable Values
`ALPHA = %s`	Flag instructing the Agent to use alphabetic characters when generating a password.	`%s = U`; use upper case alphabetic characters only
		`%s = L`; use lower case alphabetic characters only
		`%s = UL`; use upper and lower characters (default)
		`%s` = (nothing); use no alphabetic characters
`NAME = %s`	Descriptive name of this password policy.	`%s` = any string
`NUMCONSMAX = %d`	Number of times a given character can be repeated consecutively (adjacent to itself).	`%d = 0-127` (default: 8)
`NUMERIC = %b`	Flag instructing the Agent to use numeric characters when generating a password.	`%b = 0`; do not use numeric characters (default)
		`%b = 1`; use numeric characters

Password Policy Keys	Description	Acceptable Values
`NUMFLAGFIRST = %b`	Flag indicating if a numeric character can start a password.	`%b = 0`; numeric character cannot start (default)
		`%b = 1`; numeric character can start
`NUMFLAGLAST = %b`	Flag indicating if a numeric character can end a password.	`%b = 0`; numeric character cannot end (default)
		`%b = 1`; numeric character can end
`NUMRPTMAX = %d`	Number of times a character can be repeated in a password.	`%d = 0-127` (default: 8)
`NUMSIZE = %d`	Maximum number of numeric characters.	`%d = 0-128` (default: 0)
`NUMSIZEMIN = %d`	Minimum number of numeric characters.	`%d = 0-128` (default: 0)
`SBYE = %s`	List of special characters to exclude when generating this password.	`%s` = any string of special characters, to exclude, such as:
		`!@#$`
		The Windows registry key pair that holds the list of special characters normally used, but which can be excluded, is `AccessManager:SpecialChars`.
`SCHARFLAGFIRST = %b`	Flag specifying if a special character can start a password.	`%b = 0`; special character cannot start (default)
		`%b = 1`; special character can end
`SCHARFLAGLAST = %b`	Flag specifying if a special character can end a password.	`%b = 0`; special character cannot end (default)
		`%b = 1`; special character can start
`SCHARS = %b`	Flag instructing the Agent to use special characters when generating a password.	`%b = 0`; do not use special characters (default)
		`%b = 1`; use special characters
`SCHARSIZE = %d`	Maximum number of special characters.	`%d =0-128` (default: 0)
`SCHARSIZEMIN = %d`	Minimum number of special characters.	`%d =0-128` (default: 0)
`SIZE = %d`	Maximum total length of a password.	`%d = 1-255` (default: 8)
`SIZEMIN = %d`	Minimum total length of a password.	`%d = 1-255` (default: 8)

7.2.22 Kiosk Manager .NET API Sample

Example 1 .NET API Sample C# code with properties for the "User Change" event

```csharp
using System;
using System.Collections.Generic;
using System.Text;
using System.Windows.Forms;
namespace ClassLibraryTest
{
    public class TestClass
```

```
        {
                private string m_userName;
                private string m_domainName;
                public string UserName
                {
                    set
                    {
                        m_userName = value;
                    }
                    get
                    {
                        return m_userName;
                    }
        }
        public string DomainName
        {
                    set
                    {
                        m_domainName = value;
                    }
                    get
                    {
                        return m_domainName;
                    }
        }          public void UserChange()
                {
                    MessageBox.Show("UserChange called with user: " + DomainName + "\\" +
        UserName);
                }
                public void SessionStart()
                {
                MessageBox.Show("SessionStart called");
                }
                public void SessionEnd()
                {
                    MessageBox.Show("SessionEnd called");
                }
                public void SessionLocked()
                {
                    MessageBox.Show("SessionLocked called");
                }
                public void SessionUnlocked()
                {
                    MessageBox.Show("SessionUnlocked called");
                }
                public void PreSessionUnlocked()
                {
                    MessageBox.Show("PreSessionUnlocked called");
                }
                public void AuthLogon()
                {
                    MessageBox.Show("AuthLogon called");
                }
                public void AuthTimeout()
                {
                    MessageBox.Show("AuthTimeout called");
                }
                public void DeviceIn()
                {
                    MessageBox.Show("DeviceIn called");
```

```
            }
            public void DeviceOut()
            {
                MessageBox.Show("DeviceOut called");
            }
            public void GracePeriod()
            {
                MessageBox.Show("GracePeriod called");
            }
        }
    }
```

7.3 Password Reset

This section contains information applicable specifically to Password Reset.

7.3.1 Understanding Password Reset Data Structures

When you initialize the database schema, several database tables are created. Password Reset uses these tables to store data during its operation. This section discusses the database tables and how Password Reset uses them.

The schema contain data in the following tables:

- Main Configuration Data (SYSTEMPARAMETERS Table)
- Logging Configuration Data (SYSTEMPARAMETERS Table)
- System Challenge Question Data (SYSTEMPARAMETERS Table)
- User Enrollment Data (ENROLLMENTINFORMATION, USERQUESTIONS, and USER Tables)
- Password Reset Data (RESETINFORMATION Table)
- Log Message Data (SYSLOG)

> **Note:** This information is intended as a reference only and does not provide the actual configuration steps whose results are illustrated in the examples shown. For information on how to access the configuration forms and settings described in this guide, see the *Oracle Enterprise Single Sign-On Suite Installation Guide*.

7.3.1.1 Main Configuration Data (SYSTEMPARAMETERS Table)

In the following example, we configure Password Reset and submit the changes to the server.

When you click **Submit**, the following data is written to the SYSTEMPARAMETERS table as an XML string:

Example 1 System Parameters XML String

```
AuthSuccessLevel="150"
AuthFailureLevel="-150"
EnrollLevel="200"
UserQuestionCorrectResponseWeight="0"
UserQuestionWrongResponseWeight="0"
MinUserDefinedQuestions="0"
MaxUserDefinedQuestions="0"
AdminServiceStatus="0"
OperationalServiceState="0"
UserLockoutCount="3"
UserLockoutHours="24"
ByPassForceEnrollment="3"
ExcludedUsers=""
UserEmailRequired="0"
UserEmailFormat="[A-Za-z0-9._\-]+@[A-Za-z0-9._\-]+[.][A-Za-z][A-Za-z][A-Za-z]?"
ShowUnlockOption="false"
EnableTempPasswordMode="false"
```

Additionally, the following logging configuration data is written to the SYSTEMPARAMETERS table as an XML string:

Example 1 System Paramaters Table Entry

```
EventFilter="0"
SyslogPort="514"
EventFilter="0"
```

7.3.1.2 Logging Configuration Data (SYSTEMPARAMETERS Table)

In the following example, we configure Password Reset logging and submit the changes to the server.

When you click Submit, the following data is written to the SYSTEMPARAMETERS table as an XML string:

Example 1 Logging Configuration Table Entry

```
SyslogEnable="true"
SyslogServer="cmdemo.sedemo.passlog"
SyslogPort="514"
EventFilter="2031623"
```

7.3.1.3 System Challenge Question Data (SYSTEMPARAMETERS Table)

In the following example, we configure Password Reset system challenge questions and submit the changes to the server.

When you click **Submit**, the following data is written to the SYSTEMPARAMETERS table as XML strings:

Field	String
QUID	99a96ea2-671c-4db6-941c-058a6986123b
QUESTION	QuestionText="What is your favorite hockey team?"
	AnswerSource="1"
	CorrectResponseWeight="50"
	DisableState="1"
	Required="true"
	SystemQUID="99a96ea2-671c-4db6-941c-058a6986123b"
	QUID="99a96ea2-671c-4db6-941c-058a6986123b"
	WrongResponseWeight="-50"
	Flags="1"
	Language=""
	MinLength="4"
	RegExp=""

A new row is added for each system challenge question created.

7.3.1.4 User Enrollment Data (ENROLLMENTINFORMATION, USERQUESTIONS, and USER Tables)

The following example illustrates the data written to the database during user enrollment.

1. User accesses the enrollment page via the following URL:

   ```
   http://<hostname>:<port>/vgoselfservicereset/enrollmentclient/
   enrolluser.aspx
   ```

   The Password Reset enrollment page is displayed.
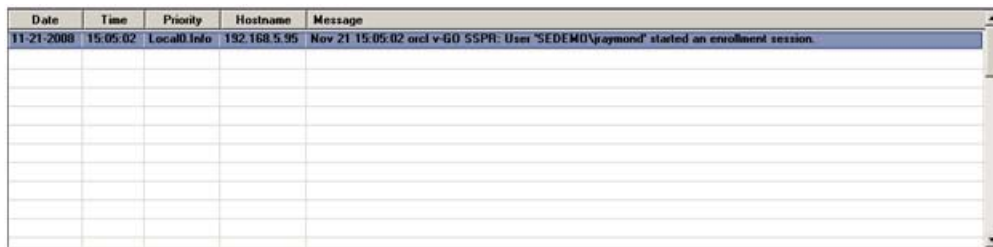
2. User clicks **Start**. A new row with the following data (in XML string format) is written to the USER table:

Field	String
USER.USERSID	S-1-5-21-1607104245-2398925301-1456127008-1137
USER.ENROLLED	FALSE
USER.USERINFORMATION	UserName="SEDEMO\jraymond"
	strSid="S-1-5-21-1607104245-2398925301-1456127008-1137"
	bEnrolled="false"
	LockOutTime="0001-01-01T00:00:00-05:00"
	LockoutCount="0"
	Email=""
	EnrollmentByPassCount="0"
	<Language />
	<ConnectorUsername />

3. When the user answers the required challenge question, a confirmation screen is displayed and a row with the following data is added to the `ENROLLMENTINFORMATION` table:

Field	String
USERSID	S-1-5-21-1607104245-2398925301-1456127008-1137
ENROLLMENTINFORMATION	StartTime="2008-11-21T15:05:02.8386162-05:00"
	EndTime="0001-01-01T00:00:00-05:00"
	Weight="0"
	Activity="1"
	State="2"
	UserNameSelect="SEDEMO\jraymond"
	GUID="d9d3c610-dd78-4292-924c-f21f9c9b9217"
CREATETIME	21- NOV-08
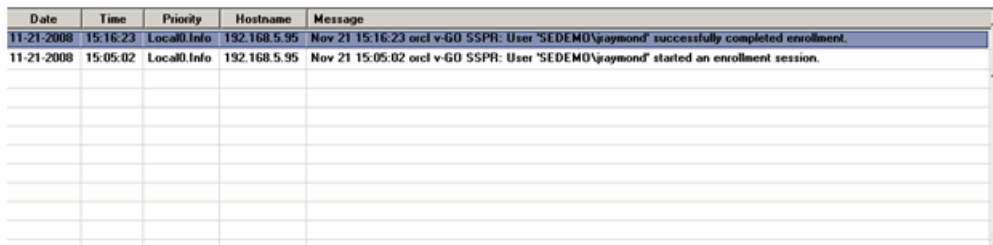
4. When the user clicks **Next** to begin answering the optional challenge questions, the following message is logged:

When the user has answered the optional questions (six in our example), the **Enrollment Finished** screen appears.

5. When the user clicks **Close**, the following events occur:

    a. A message is logged:

    b. A row for each answered question is added to the `USERQUESTIONS` table with the following data:

Field	String
USERSID	S-1-5-21-1607104245-2398925301-1456127008-1137
QUID	53412afd-af16-4a1a-9ddb-ecdf5414ff51

Field	String
USERQUESTIONS	QuestionAnswer="BoNGMYmBe5KUp5Zqzu5QtOGylJl6QJtnupKIkQ8Tx SnQGIU0" SystemQuestion="true"
	SystemQUID="99a96ea2-671c-4db6-941c-058a6986123b"
	QUID="53412afd-af16-4a1a-9ddb-ecdf5414ff51"

c. The following data is written to the USER table:

Field	String
USER.USERSID	S-1-5-21-1607104245-2398925301-1456127008-1137
USER.ENROLLED	TRUE
USER.USERINFORMATION	UserName="SEDEMO\jraymond"
	Sid="S-1-5-21-1607104245-2398925301-1456127008-1137" Enrolled="true"
	LockOutTime="0001-01-01T00:00:00-05:00"
	LockoutCount="0"
	Email=""
	EnrollmentByPassCount="0"
	Language />
	ConnectorUsername />

d. The following data is written to the ENROLLMENTINFORMATION table:

Field	String
USERSID	S-1-5-21-1607104245-2398925301-1456127008-1137
ENROLLMENTINFORMATION	StartTime="2008-11-21T15:05:02.8386162-05:00"
	EndTime="2008-11-21T15:16:23.1736578-05:00"
	Weight="200"
	Activity="1"
	State="6"
	UserNameSelect="SEDEMO\jraymond"
	GUID="71c2739f-b192-42b3-a326-271bec9323da"
CREATETIME	21- NOV-08

7.3.1.5 Password Reset Data (RESETINFORMATION Table)

The following example illustrates the data written to the database during password reset.

1. User accesses the password reset page via the following URL:

http://<hostname>:<port>/vgoselfservicereset/resetclient/default.aspx

The Password Reset logon page appears.

2. When the user enters the required information and waits too long before clicking the **OK** button, the **Session is invalid** screen appears, providing a link allowing the user to reset the enrollment session. At this point, the following message is logged:

3. When the user retries the reset procedure and arrives at the password reset page, the following data is written to the RESETINFORMATION table:

Field	String
USERSID	S-1-5-21-1607104245-2398925301-1456127008-1137
RESETINFORMATION	StartTime="2008-11-21T15:59:38.436503-05:00"
	EndTime="2008-11-21T16:00:40.5771384-05:00"
	Weight="0"
	State="2"
	HostAddress="192.168.5.101"
CREATETIME	21-NOV-08

At this point, the following message is logged:

4. When the user has successfully reset the password, Password Reset displays a message confirming the successful password reset and the following data is written to the RESETINFORMATION table:

Field	String
USERSID	S-1-5-21-1607104245-2398925301-1456127008-1137
RESETINFORMATION	StartTime="2008-11-21T16:10:43.7618874-05:00"
	EndTime="0001-01-01T00:00:00-05:00"
	Weight="100"
	State="6"
	HostAddress="192.168.5.101"
CREATETIME	21-NOV-08

At this point, the following message is logged:

7.3.1.6 Log Message Data (SYSLOG)

When enabled, the logging feature of Password Reset will write the following data to SYSLOG:

- Date
- Time
- Priority
- Host name
- Message

The following are examples of typical log messages generated by Password Reset during normal operation.

Example 1 Logging Configuration Table Entry

```
Nov 21 16:21:46 orcl v-GO SSPR: User 'SEDEMO\lchristine' started an enrollment
session.
Nov 21 16:22:42 orcl v-GO SSPR: User 'SEDEMO\lchristine' cancelled the enrollment
session.
Nov 21 15:16:23 orcl v-GO SSPR: User 'SEDEMO\jraymond' successfully completed
enrollment
```

Example 2 Example Password Reset Log Messages

```
Nov 21 16:10:43 orcl v-GO SSPR: User 'SEDEMO\jraymond' started a reset session.
Nov 24 11:21:51 orcl v-GO SSPR: User 'SEDEMO\jraymond' cancelled the reset
session.
Nov 21 16:11:17 orcl v-GO SSPR: User 'SEDEMO\jraymond' successfully reset his/her
password.
Nov 24 09:43:08 orcl v-GO SSPR: User 'SEDEMO\jraymond' failed the reset quiz.
Nov 24 10:00:15 orcl v-GO SSPR: User 'SEDEMO\jraymond' has been locked out!
Nov 21 16:06:20 orcl v-GO SSPR: User 'SEDEMO\jraymond' timed out the reset
session.
Nov 24 10:13:28 orcl v-GO SSPR: User 'SEDEMO\jraymond' successfully unlocked
his/her account.
```

For additional information on logging see Chapter 4, "Using the Administrative Console to Configure Password Reset" in this guide.

7.3.2 Schema Diagram

This diagram shows the object classes that Password Reset adds when extending the schema.

- Each box represents a class.
- The class name is displayed in the top of the box.
- The attributes the class can have are displayed in the bottom of the box.

■ Each link represents the child classes that a class can contain.
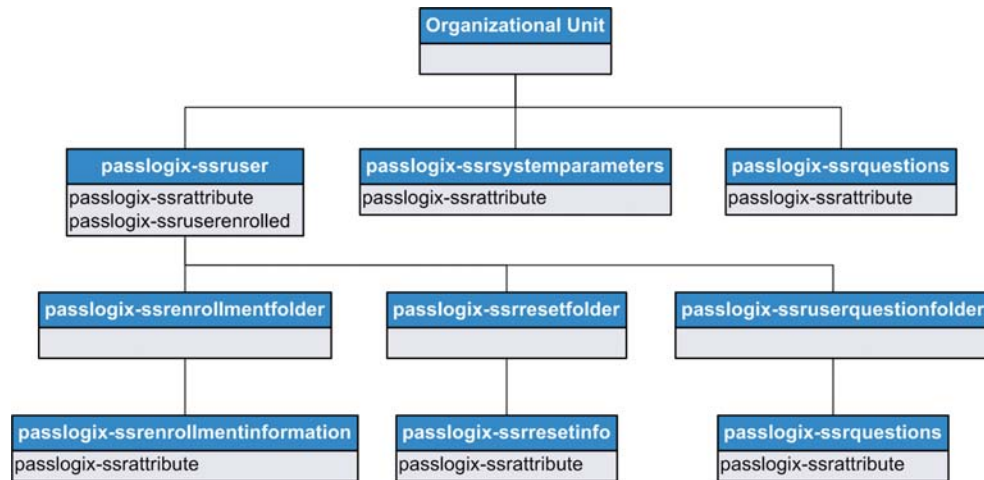
7.3.2.1 Rights and Security

At a minimum, the Password Reset Web Service account requires permission to create, delete, and modify the classes shown in the schema diagram. These permissions should be granted for the OU=SSPR organizational unit and be inherited to all child objects.

7.3.2.2 Object Classes

Following are definitions of the schema's object classes.

7.3.2.2.1 passlogix-ssruser This class contains enrollment, reset, and question response objects, and serves as a container to hold all the information about an Password Reset user. An instance of this class will be created for each user under OU=SSPR, OU=Users. The instance name will be the user's SID.

Attribute Name	Syntax	Flag
passlogix-ssrattribute	Case Ignore String	Single Valued
passlogix-ssruserenrolled	Cast Ignore String	Single Valued
Other optional attributes	cn, dn	

7.3.2.2.2 passlogix-ssrenrollmentfolder This class contains passlogix-ssrenrollmentinformation objects, and can only exist as a child of a passlogixssruser object.

Attribute Name	Syntax	Flag
Other optional attributes	cn, dn	

7.3.2.2.3 passlogix-ssrenrollmentinformation This class stores information about an enrollment event, and typically exists as a child of passlogix-ssrenrollmentfolder. The instance name will be a randomly generated GUID.

Attribute Name	Syntax	Flag
passlogix-ssrattribute	Case Ignore String	Single Valued

Attribute Name	Syntax	Flag
Other optional attributes	cn, dn	

7.3.2.2.4   passlogix-ssruserquestionfolder   This class containspasslogix-ssrquestions objects, and can only exist as a child of a `passlogix-ssruser` object.

Attribute Name	Syntax	Flag
Other optional attributes	cn, dn	

7.3.2.2.5   passlogix-ssrquestions   This class stores information about a question or a response, and typically exists as a child of `passlogixssruserquestionfolder` if it represents the user answer to a question. If it represents a system question, it will exist under `OU=SSPR,OU=SystemQuestions`. The instance name will be a randomly generated GUID.

Attribute Name	Syntax	Flag
passlogix-ssrattribute	Case Ignore String	Single Valued
Other optional attributes	cn, dn	

7.3.2.2.6   passlogix-ssrresetfolder   This class containspasslogix-ssrresetinfoobjects, and can only exist as a child of a `passlogix-ssruserobject`.

Attribute Name	Syntax	Flag
Other optional attributes	cn, dn	

7.3.2.2.7   passlogix-ssrresetinfo   This class stores information about a reset event, and typically exists as a child of `passlogix-ssrresetfolder`. The instance name will be a randomly generated GUID.

Attribute Name	Syntax	Flag
passlogix-ssrattribute	Case Ignore String	Single Valued
Other optional attributes	cn, dn	

7.3.2.2.8   passlogix-ssrsystemparameters   This class stores Password Reset system settings information. An instance of this class is typically created under `OU=SSPR` and will be named `CN=SystemParameters`.

Attribute Name	Syntax	Flag
passlogix-ssrattribute	Case Ignore String	Single Valued
Other optional attributes	cn, dn	

7.3.2.3 Attributes
Following are definitions of the schema's attribute objects.

7.3.2.3.1   passlogix-ssrattribute   This attribute provides data storage for a Password Reset object. Generally, this data will be an XML-formatted string.

7.3.2.3.2 passlogix-ssruserenrolled This attribute indicates if the user is currently enrolled in Password Reset. It will be set to either TRUE or FALSE.

7.3.3 Configuring Password Reset for Data Storage in an Oracle Database

Follow the guidelines below when preparing your Oracle database instance for Password Reset:

- Create a dedicated simple tablespace in a simple database instance with initial size of 200MB and auto-extend enabled.

- Create a dedicated application user whose only role is to allow Password Reset to connect to and store data in the database. Do not use the SYSTEM user for interfacing Password Reset with the database.

> **Note:** The specifics of configuring your Oracle database are beyond the scope of this document. Oracle highly recommends that you engage your organization's DBA team to determine how to integrate Password Reset into your existing Oracle database infrastructure.

7.3.3.1 Configuring the Database Schema for Password Reset Data

Complete the steps below to configure the database schema for Password Reset:

1. Locate the Password Reset DDL script file:

   ```
   %PROGRAM FILES%\Passlogix\v-GO SSPR\WebServices\OracleTables.txt
   ```

2. If you have not already done so, replace all instances of the SYSTEM user in the OracleTables.txt script with the dedicated Password Reset application user you created when preparing your Oracle database instance.

3. Launch the Oracle SQL*Plus client and log on to the Password Reset database instance.

4. Execute theOracleTables.txtscript create the required data structures:

   ```
   @ "<ESSO-PR_server_install_path>\WebServices\OracleTables.txt"
   ```

7.3.3.2 Configuring Password Reset to Store Data in the Database

1. Log in to the Administrative Console by pointing your Web browser at the following URL:

   ```
   http://<hostname>:<port>/vGoSelfServiceReset/ManagementClient/storage.a
   spx
   ```

   > **Note:** If you have configured Password Reset to accept SSL connections, replace http with https in the above URL.

   ---

2. In the left hand pane, click **Storage**.

3. On the **Storage** page, do the following:

   a. From the **Storage Type** drop-down list, select **Oracle Database**.

   b. In the **Connection String** field, enter the connection string for the target database instance, then click **Add**. The syntax is as follows (on a single line):

```
Provider=OraOLEDB.Oracle;Data Source=<datasource>;User Id=<user_
id>;Password=<password>
```

Where:

*<datasource>*is the name of the data source for the target instance,

<user_id> is the ID of the dedicated application user account you created in your database instance for Password Reset,

<password> is the password for the user chosen above.

c. In the **Database Timeout** field, enter a desired value in seconds. Oracle recommends 60 seconds as a default.

d. Click **Submit**.

Password Reset is now configured for storing its data in the selected database instance. See Understanding Password Reset Data Structures for more information on, and examples of, the data Password Reset stores in the database, and how this data is organized.

7.3.4 Password Reset Client-Side Registry Settings

This section describes registry settings governing the behavior of the Password Reset client.

7.3.4.1 Under HKLM\Software\Passlogix\SSPR

Key	Value Name	Data Type	Data [URLRoot] : http://[host]/vgoselfservicereset
WindowsInterface	EnrollURL	string (REG_SZ)	URL of the Enrollment service default page: [URLroot]/enrollmentclient/enrolluser.aspx
	ResetURL	string (REG_SZ)	URL of the reset service default page: [URLroot]/resetclient/default.aspx
	StatusURL	string (REG_SZ)	URL of the checkstatus page (notifies reset client that reset service is available: [URLroot]/resetclient/checkstatus.aspx
	CheckEnrollURL	string (REG_SZ)	URL of Enrollment check service (checks if user is enrolled in service): [URLroot]/resetclient/checkenrollment.aspx
	AutomaticEnroll	dword (REG_DWORD)	Set to a non-zero value to offer enrollment option to enroll user at next logon. Set to 0 (default) not to offer enrollment upon logon.
	ForceEnrollment	dword (REG_DWORD)	Set to a non-zero value to require unenrolled user to enroll at next logon. Set to 0 (default) not to require enrollment upon logon.
	CheckForceEnrollment	string (REG_SZ)	URL of force enrollment check service (checks the number of times user can defer Enrollment): [URLroot]/resetclient/checkforceenrollment .aspx
	WindowHeight	dword (REG_DWORD)	Adjusts the Password Reset browser window height.
	WindowWidth	dword (REG_DWORD)	Adjusts the Password Reset browser window width.
	IgnoreCertRevocation Errors	dword (REG_DWORD)	Set to a non-zero value to ignore certificate revocation errors. Set to 0 (default) or leave empty to recognize those errors.

Key	Value Name	Data Type	Data [URLRoot] : http://[host]/vgoselfservicereset
WindowsInterface\xx (where xx is the two-letter language code*)	LinkText	string (REG_SZ)	Enter desired text to instruct the user to click to reset password (Windows 7 only).
	WindowTitle	string (REG_SZ)	Enter desired text for the Enrollment and Reset Interface window titles.
WindowsInterface\	UseSeparateTile	string (REG_DWORD)	Set to any non-zero number to eliminate the "Forgot your password?" link under the user's default Windows 7 logon tile, and create a separate password reset tile and text, on the logon screen. Set to 0 to disable the additional tile. Default is 0.
WindowsInterface\xx\	TileText	string (REG_SZ)	Text to display under the replacement Password Reset tile, where xx is the language of the text.
WindowsInterface\xx\	TileImage	string (REG_SZ)	Full path to a bitmap file to use for the replacement Password Reset tile.

7.3.4.2 Language Codes for WindowsInterface\xx

Language	Code	Language	Code
English (default)	en-US	Norwegian	no
Brazilian Portuguese	pt-BR	Polish	pl
Czech	cs	Portuguese	pt
Danish	da	Romanian	ro
Dutch	nl	Russian	ru
Finnish	fi	Simplified Chinese	zh-CN
French	fr	Slovak	sk
German	de	Spanish	es
Greek	el	Swedish	sv
Hungarian	hu	Thai	th
Italian	it	Traditional Chinese zh	zh
Japanese	ja	Turkish	tr
Korean ko	ko		

7.3.5 Password Reset Server-Side Registry Settings

This section describes the registry settings governing the behavior of the Password Reset Server application.

7.3.5.1 Under HKLM\Software\Passlogix\SSPR

Key	Value Name	Data Type	Data
SSPRService	CacheEnabled	dword REG_DWORD	Set to 1 (default) to allow the server to cache user information. Set to 0 to disable caching user information. This setting specifically addresses a configuration with more than one Web server. For such configurations, use the 0 value to prevent user information from synchronizing incorrectly.
SSPRService	Reset_ShowIntroduction	dword REG_DWORD	Set to 1 to display the reset prompt. Set to 0 (default) to suppress the reset prompt.
SSPRService	Reset_CustomizedErrorMsg	dword REG_DWORD	Set to 1 to activate customizable reset error messages. Set to 0 (default) to use the built-in reset error messages.
SSPRService	SessionTimeoutMessage	dword REG_DWORD	Set to 1 to activate a message notifying the user that the session will timeout within a specified period of time. Set to 0 (default) if you do not want this message to display.

7.3.5.2 Under HKLM\Software\Passlogix\SSPR\Storage\Extensions\

Key	Value Name	Data Type	Data
ADAM	Root	string (REG_SZ)	AD LDS (ADAM) partition root
	Classname	string (REG_SZ)	Adam

7.3.5.3 Under HKLM\Software\Passlogix\SSPR\Storage\Extensions\ADAM\

Key	Value Name	Data Type	Data
Servers	Server1	string (REG_SZ)	server:port (of the AD LDS (ADAM) instance)

7.3.5.4 Under HKLM\Software\Passlogix\SSPR\Storage\Extensions\

Key	Value Name	Data Type	Data
AD	Root	string (REG_SZ)	AD root
	Classname	string (REG_SZ)	AD

7.3.5.5 Under HKLM\Software\Passlogix\SSPR\Storage\Extensions\AD\

Key	Value Name	Data Type	Data
Servers	Server1	string (REG_SZ)	server:port

7.4 Reporting

This section contains information applicable specifically to the Reporting tool.

7.4.1 Reporting Event Definition Table

This section describes the reporting event table and the values contained therein. Because field population depends on the product and context in which the event was generated, events will not always have every field populated. All fields are textual in nature, with the exception of time stamps and any fields specific to Oracle use. Some entries have specific enumerated values; these are included under the description when applicable.

Following is the SQL Server Script used to create the event log table.

```
CREATE TABLE [dbo].[tblEventsLog](
    [ID]                    [int] IDENTITY(1,1) NOT FOR REPLICATION NOT NULL,
    [GUID]                  [varchar](400) NOT NULL,
    [ProductName]           [varchar](400) NULL,
    [ProductVersion]        [varchar](400) NULL,
    [HostName]              [varchar](400) NULL,
    [LogonMethod]           [varchar](400) NULL,
    [CredentialType]        [varchar](400) NULL,
    [Operation]             [varchar](400) NULL,
    [SSOUserId]             [varchar](400) NULL,
    [WindowsUserName]       [nvarchar](400) NULL,
    [ApplicationName]       [nvarchar](400) NULL,
    [ApplicationReference]  [nvarchar](400) NULL,
    [ApplicationUserId]     [nvarchar](400) NULL,
    [ApplicationThirdField] [nvarchar](400) NULL,
    [ApplicationFourthField] [nvarchar](400) NULL,
    [SAMAccountName]        [nvarchar](400) NULL,
    [Comment]               [nvarchar](max) NULL,
    [EventtimeClient]       datetime NULL,
    [EventtimeServer]       datetime NULL,
    [HashType]              [tinyint] NOT NULL,
    [HashValue]             [varchar](400) NOT NULL,
    [HostFingerprint]       [nvarchar](max)
CONSTRAINT [PK_tblEventsLog] PRIMARY KEY CLUSTERED
(
    [ID] ASC
)WITH (PAD_INDEX = OFF, STATISTICS_NORECOMPUTE = OFF,
IGNORE_DUP_KEY = OFF,
ALLOW_ROW_LOCKS = ON,
ALLOW_PAGE_LOCKS = ON, FIsLLFACTOR = 90) ON [PRIMARY]
) ON [PRIMARY]
```

7.4.1.1 Definitions

- GUID

  A Globally Unique Identifier. Every event generated has an identifier that is unique to that specific event.

  > **Note:** This field is generally not needed for reporting purposes but may be useful for accounting purposes.

- ProductName

  The name of the Oracle Enterprise Single Sign-On Suite component that generated the event.

Current Values	
SSO_Server	SM
SSO_Client	UAM
SAM_Server	ODE
SAM_Client	NotificationService
PM_Server	ReportingService
PM_Client	DC_Client
SSPR	OPAM_Client
AM	

- ProductVersion

  The version of the Oracle Enterprise Single Sign-On Suite Plus product that generated the event.

- HostName

  The name of the host or machine that generated the event.

- LogonMethod

- The logon method that was used if applicable for the given event.

  Current Values:

  - WinAuth

  - MsAuth

  - LDAPv1

  - LDAPv2

  - MultiAuth

- CredentialType

  Denotes the type of credential if available.

  Current Values:

  - Standard

  - Shared

- Operation

  This defines the nature of the event generated by a given Oracle Enterprise Single Sign-On Suite product.

Current Values

Login	SM_MachineShutdown
CredentialChange_Username	SM_MachineRestart
CredentialChange_Password	SM_ManagerExit
CredentialChange_Third	SM_SpecialActionExec
CredentialChange_Fourth	SM_RunListExecNet
Pause	SM_TerminateListExec
Shutdown_Manual	SM_TerminateListExec
Shutdown_Programmatic	Enrollment
Resume	PasswordReset_Success
FirstTimeUse	PasswordReset_Fail
CredentialAdded	Re-enrollment
CredentialDeleted	PM_CredentialAdded
CredentialAddAborted	PM_CredentialDeleted
Auth_Failure	PM_CredentialModified
Auth_Success	DC_DelegationAccepted
Auth_Enrollment	DC_DelegationRevoked
Auth_Unenrollment	DC_DelegationModified
Start	DC_DelegationDeclined
SM_AuthenticatorLogon	DC_DelegationEndedTimeExceeded
SM_SessionStart	DC_DelegationEndedManual
SM_SessionLock	OPAM_CheckOut
SM_SessionUnlock	OPAM_CheckIn_User
SM_SessionEnd	OPAM_CheckIn_External
SM_SessionExpiration	OPAM_CheckIn_Expire

- SSOUserId

  This is the User ID that Logon Manager uses for synchronization with the corporate repository, such as Active Directory or LDAP. If the generated event is from another Oracle Enterprise Single Sign-On Suite product or a repository not in use, this field will be the user's Windows Logon name, for example <domain>\<user>.

- WindowsUserName

  This is the Windows logon name for the system that generated the event, for example <domain>\<user>. This may or may not be the same as SSOUserId.

- ApplicationName

  This is the name of the application that was the target of event generation, such as an Logon Manager logon to Outlook, AIM etc.

- ApplicationReference

The application template reference for the credential used, if available.

■ ApplicationUserId

The User ID for the application this credential belongs to.

■ ApplicationThirdField

This field will be populated with the Third Field if the credential used contains additional information.

> **Note:** If the template is masked by definition, this field will contain "<masked>" to avoid exposing sensitive information.

■ ApplicationFourthField

This field will be populated with the Fourth Field if the credential used contains additional information.

> **Note:** If the template is masked by definition, this field will contain "<masked>" to avoid exposing sensitive information.

■ SAMAccountName

If this event was generated from a Shared Account, this will contain the name of that Shared Account.

■ Comment

Additional (and optional) information regarding this event.

■ EventtimeClient

This is the time (in GMT) format when the event was created on the local system.

> **Note:** This time is sourced from the local system; while stored in GMT format, if the local system time is incorrect, it will be reflected/stored in this field.

■ EventtimeServer

This is the time (in GMT) format that the event was stored in the database.

> **Note:** This field is sourced from the system that contains the database. The database itself creates this timestamp when the event is stored.

■ EventtimeEnrollment

This field is the time (in GMT format) that the user's cryptographic key was generated or updated. The cryptographic key is used to encrypt credentials when a user enrolls to an authenticator or changes the enrollment. This field is set only for the Auth_Enrollment and Auth_Unenrollment events.

■ HashType

Oracle internal use only.

- `HashValue`

  Oracle internal use only.

- `HostFingerprint`

  Oracle internal use only.

7.5 Universal Authentication Manager Registry Settings

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

- Setting Logon Method Display Order
- Global Universal Authentication Manager Settings
- Global Branding Settings

> **Note:** Keep in mind the distinction between registry paths for 32-bit and 64-bit operating systems.
>
> The path for a 32-bit OS registry key begins with "`HKEY_LOCAL_MACHINE\SOFTWARE\...`".
>
> The equivalent registry key path for a 64-bit OS begins with "`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\...`".

7.5.1 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.

> **Note:** 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
32-bit OS:
`HKEY_LOCAL_MACHINE\Software\Passlogix\UAM\Authenticators\{16627EE1-FAE3-43B5-B884-D3661649B97D}`

64-bit OS:
`HKEY_LOCAL_`

```
MACHINE\Software\Wow6432Node\Passlogix\UAM\Authenticators\{16627EE1-FAE3-4
3B5-B884-D3661649B97D}
```

Order `REG_DWORD 100`

Proximity Card

32-bit OS:
```
HKEY_LOCAL_
MACHINE\Software\Passlogix\UAM\Authenticators\{4A8F93E4-2328-44CA-8DBE-FBF
A4E5FD334}
```

64-bit OS:
```
HKEY_LOCAL_
MACHINE\Software\Wow6432Node\Passlogix\UAM\Authenticators\{4A8F93E4-2328-4
4CA-8DBE-FBFA4E5FD334}
```

Order `REG_DWORD 500`

Smart Card

32-bit OS:
```
HKEY_LOCAL_
MACHINE\Software\Passlogix\UAM\Authenticators\{A1B34553-8D40-42A9-8ED5-F70
E3497E138}
```

64-bit OS:
```
HKEY_LOCAL_
MACHINE\Software\Wow6432Node\Passlogix\UAM\Authenticators\{A1B34553-8D40-4
2A9-8ED5-F70E3497E138}
```

Order `REG_DWORD 600`

Challenge Questions

32-bit OS:
```
HKEY_LOCAL_
MACHINE\Software\Passlogix\UAM\Authenticators\{393D4B53-EC46-4A38-9E9E-3D6
B5141DD34}
```

64-bit OS:
```
HKEY_LOCAL_
MACHINE\Software\Wow6432Node\Passlogix\UAM\Authenticators\{393D4B53-EC46-4
A38-9E9E-3D6B5141DD34}
```

Order `REG_DWORD 900`

Windows Password

32-bit OS:
```
HKEY_LOCAL_
MACHINE\Software\Passlogix\UAM\Authenticators\{0C29417D-8A20-48B7-8CC4-D94
8D384E9B2}
```

64-bit OS:
```
HKEY_LOCAL_
MACHINE\Software\Wow6432Node\Passlogix\UAM\Authenticators\{0C29417D-8A20-4
8B7-8CC4-D948D384E9B2}
```

Order `REG_DWORD 999`

> **Note:** If the Order key does not exist, the default is 800.

7.5.2 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	DWORD	ClientMode	Enterprise Client Mode (1) (default) or Local Client Mode (0)	Client Mode may be set to Local or Enterprise during install.	32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM 64-bit OS: HKEY_LOCAL_ MACHINE\ SOFTWARE\Wow643 2Node\Passlogix\UA M
Framework	Logging	DWORD	SimpleLoggerOn	Yes (1) or No (0) (default)	Turn auditing and debug logging on or off.	32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix 64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix
Framework	Logging	DWORD	SimpleLogger Level	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.	32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix 64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix
Framework	Logging	SZ	SimpleLoggerPath	Default is c:\uamlog.txt	Specify debug log path and filename.	32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix 64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix
Framework	Logging	SZ	SimpleLoggerAudi tPath	Default is c:\uamadt.txt	Specify audit log path and filename.	32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix 64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix

Target	Category	Type	Name	Values	Description	Path

Framework	Logging	SZ	`SimpleLogger ProcShow`	N/A	Regular expression to only show matching log entries by process name. Default is to show all entries.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix`

Framework	Logging	SZ	`SimpleLogger ProcHide`	N/A	Regular expression to hide matching log entries by process name. Default is to show all entries.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix`

Framework	Logging	SZ	`SimpleLogger FileHide`	N/A	Regular expression to hide matching log entries by source filename. Default is to show all entries.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix`

Framework	Logging	SZ	`SimpleLoggerMsgS how`	N/A	Regular expression to only show matching log entries by log entry contents. Default is to show all entries.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix`

Framework	Logging	SZ	`SimpleLoggerMsgH ide`	N/A	Regular expression to hide matching log entries by log entry contents. Default is to show all entries.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix`

Framework	Logging	DWORD	`SimpleLoggerRemo te`	Disabled (0) or Enabled (1)	If enabled, add extra columns for console session ID, remote session state and application vs. service process.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix`

Framework	Logging	DWORD	`SimpleLoggerForm at`	TXT (0) or CSV (1)	Controls how the logging file is formatted. Note: Audit log is always in CSV format.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix`

Target	Category	Type	Name	Values	Description	Path

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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM`

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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM`

Target	Category	Type	Name	Values	Description	Path

Framework	Enrollment	DWORD	`PromptToken Description`	Prompt User for Description (1) (default) or Do Not Prompt User for Description (0)	Ask user to enter a token description during enrollment. If not prompted, the default description is automatically used.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM`

Framework	Enrollment	DWORD	`JitEnrolllPrompt Mode`	Ask - Prompt User with Yes/No Dialog (0) (default), Force - force enrollment with a message (1), Silent - Silently initiate enrollment (2), None - Disable just-in-time enrollment / Fail authentication (3)	Configure if just-in-time enrollment will be permitted during ESSO-LM reauthentication, and whether the user will be prompted or automatically forced to enroll.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM`

Framework	Enrollment	DWORD	`JitEnrollForceRe auth`	Disabled (0) (default), Enabled (1)	Control whether just-in-time enrollment during ESSO-LM reauthentication will suppress the second authentication prompt. If enabled, the user will have to authenticate twice.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM`

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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM`

Framework	Reauthentication	DWORD	`HideAlways UseMethod`	Hide Checkbox (1) or Show Checkbox (0) (default)	Hide or show the **Always Use Method** checkbox.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM`

Target	Category	Type	Name	Values	Description	Path
Synchroniz ation	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.	32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ SyncManager 64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix\UAM\ SyncManager
Synchroniz ation	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.	32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ SyncManager 64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix\UAM\ SyncManager
Synchroniz ation	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.	32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ SyncManager 64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix\UAM\ SyncManager
Synchroniz ation	Per-Logon Sync	DWORD	SyncData AuthAsync	Asynchronous Update (1) (default), or Synchronous Update (0)	Sync user data at logon synchronously or asynchronously.	32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ SyncManager 64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix\UAM\ SyncManager
Synchroniz ation	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.	32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ SyncManager 64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix\UAM\ SyncManager
Synchroniz ation	Per-Logon Sync	DWORD	SyncPolicy AuthAsync	Asynchronous Update (1) (default), or Synchronous Update (0)	Sync user policy at logon synchronously or asynchronously.	32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ SyncManager 64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\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.	`32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ SyncManager`
						
						`64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\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	`32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\ UAM\ SyncManager`
						
						`64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\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.	`32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\ UAM\Client`
						
						`64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix\ UAM\Client`

Logon	General	DWORD	`RemoteSupportLog on`	Enabled (1) (default), Disabled (0)	Turn Remote Desktop support on or off in the logon application. Framework support must also be enabled.	`32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM`
						
						`64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix\UAM`

Logon	General	REG_SZ	`DefaultAuthentic ator`	None (default), Fingerprint, Proximity Card, Smart Card, Challenge Questions, Windows Password
				
				The actual values are the GUIDs of the respective logon methods (available in the Config Editor).
					Default authenticator to use in preference to remembering the last used method.	`32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\Crede ntialProviders`
						
						`64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix\UAM\Cre dentialProviders`

Logon	Filters	DWORD	`Disable`	Enabled (visible) (0), Disabled (filtered) (1) (default)	Enable or disable the Microsoft Windows Password Credential Provider (Windows 7).	`32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\Crede ntialProviders\{6f4 5dc1e-5384-457a-bc1 3-2cd81b0d28ed}`
						
						`64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix\UAM\Cre dentialProviders\{6 f45dc1e-5384-457a-b c13-2cd81b0d28ed}`

Target	Category	Type	Name	Values	Description	Path

Logon	Filters	DWORD	`Disable`	Enabled (visible) (0), Disabled (filtered) (1) (default)	Enable or disable the Microsoft Windows Smart Card Credential Provider (Windows 7).	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM\Crede`
						`ntialProviders\{8bf`
						`9a910-a8ff-457f-999`
						`f-a5ca10b4a885}`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\Cre`
						`dentialProviders\{8`
						`bf9a910-a8ff-457f-9`
						`99f-a5ca10b4a885}`

Logon	Filters	DWORD	`Disable`	Enabled (visible) (0), Disabled (filtered) (1) (default)	Enable or disable the Microsoft Windows Biometric Credential Provider (Windows 7).	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM\Crede`
						`ntialProviders\{ac3`
						`ac249-e820-4343-a65`
						`b-377ac634dc09}`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\Cre`
						`dentialProviders\{a`
						`c3ac249-e820-4343-a`
						`65b-377ac634dc09}`

Logon	Filters	DWORD	`Disable`	Enabled (visible) (0), Disabled (filtered) (1) (default)	Enable or disable the Microsoft Windows Password Credential Provider (Windows 8).	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM\Crede`
						`ntialProviders\{60b`
						`78e88-ead8-445c-9cf`
						`d-0b87f74ea6cd}`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\Cre`
						`dentialProviders\{6`
						`0b78e88-ead8-445c-9`
						`cfd-0b87f74ea6cd}`

Logon	Filters	DWORD	`Disable`	Enabled (visible) (0), Disabled (filtered) (1) (default)	Enable or disable the Microsoft Windows Smart Card Credential Provider (Windows 8).	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM\Crede`
						`ntialProviders\{{8f`
						`d7e19c-3bf7-489b-a7`
						`2c-846ab3678c96}`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\Cre`
						`dentialProviders\{8`
						`fd7e19c-3bf7-489b-a`
						`72c-846ab3678c96}`

Target	Category	Type	Name	Values	Description	Path
Logon	Filters	DWORD	`Disable`	Enabled (visible) (0), Disabled (filtered) (1) (default)	Enable or disable the Microsoft Windows Biometric Credential Provider (Windows 8).	`32-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\` `Passlogix\UAM\Crede` `ntialProviders\{bec` `09223-b018-416d-a0a` `c-523971b639f5}` `64-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\Wow6432Nod` `e\Passlogix\UAM\Cre` `dentialProviders\{b` `ec09223-b018-416d-a` `0ac-523971b639f5}`
Logon	Filters	DWORD	`Disable`	Enabled (visible) (0), Disabled (filtered) (1) (default)	Enable or disable the Microsoft Windows PIN Credential Provider (Windows 8).	`32-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\` `Passlogix\UAM\Crede` `ntialProviders\{{cb` `82ea12-9f71-446d-89` `e1-8d0924e1256e}` `64-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\Wow6432Nod` `e\Passlogix\UAM\Cre` `dentialProviders\{c` `b82ea12-9f71-446d-8` `9e1-8d0924e1256e}`
Logon	Filters	DWORD	`Disable`	Enabled (visible) (0), Disabled (filtered) (1) (default)	Enable or disable the Microsoft Windows Picture Credential Provider (Windows 8).	`32-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\` `Passlogix\UAM\Crede` `ntialProviders\{213` `5f72a-90b5-4ed3-a7f` `1-8bb705ac276a}` `64-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\Wow6432Nod` `e\Passlogix\UAM\Cre` `dentialProviders\{2` `135f72a-90b5-4ed3-a` `7f1-8bb705ac276a}`
Logon	Filters	DWORD	`Disable`	Enabled (visible) (0), Disabled (filtered) (1) (default)	Enable or disable the Microsoft Windows Microsoft Account (Windows Live ID) Credential Provider (Windows 8).	`32-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\` `Passlogix\UAM\Crede` `ntialProviders\{f8a` `0b131-5f68-486c-804` `0-7e8fc3c85bb6}` `64-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\Wow6432Nod` `e\Passlogix\UAM\Cre` `dentialProviders\{f` `8a0b131-5f68-486c-8` `040-7e8fc3c85bb6}`

Target	Category	Type	Name	Values	Description	Path
Proximity Card	General	DWORD	InsertionDelay	Default is 0 ms Allowed range is 1-2147483646 ms	Rest period between accepting consecutive proximity token insertions.	32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {4A8F93E4- 2328-44CA-8DBE- FBFA4E5FD334}\ Settings 64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\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.	32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {4A8F93E4- 2328-44CA-8DBE- FBFA4E5FD334}\ Settings 64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\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.	32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {4A8F93E4- 2328-44CA-8DBE- FBFA4E5FD334}\ Settings 64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM\`
						`Authenticators\`
						`{4A8F93E4-`
						`2328-44CA-8DBE-`
						`FBFA4E5FD334}\`
						`Settings`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM\`
						`Authenticators\`
						`{4A8F93E4-`
						`2328-44CA-8DBE-`
						`FBFA4E5FD334}\`
						`Settings`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM\`
						`Authenticators\`
						`{4A8F93E4-`
						`2328-44CA-8DBE-FBFA`
						`4E5FD334}\Settings`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\`
						`Authenticators\`
						`{4A8F93E4-`
						`2328-44CA-8DBE-FBFA`
						`4E5FD334}\Settings`

Target	Category	Type	Name	Values	Description	Path
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.	`32-bit OS:` `HKEY_LOCAL_` `MACHINE\SOFTWARE\Pa` `sslogix\UAM\` `Authenticators\{A1B` `34553-8D40-42A9-8ED` `5-F70E3497E138}\Set` `tings` `64-bit OS:` `HKEY_LOCAL_` `MACHINE\SOFTWARE\Wo` `w6432Node\Passlogix` `\UAM\` `Authenticators\{A1B` `34553-8D40-42A9-8ED` `5-F70E3497E138}\Set` `tings`
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.	`32-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\` `Passlogix\UAM\` `Authenticators\` `{A1B34553-` `8D40-42A9-8ED5F70E3` `497E138}\` `Providers\BaseCSP` `64-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\Wow6432Nod` `e\Passlogix\UAM\` `Authenticators\` `{A1B34553-` `8D40-42A9-8ED5F70E3` `497E138}\` `Providers\BaseCSP`
Smart Card	Microsoft Base CSP Provider	DWORD	`SessionKeyUseKey` `CipherCerts`	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.	`32-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\Passlogix\` `UAM\Authenticators\` `{A1B34553-8D40-42A9` `-8ED5-F70E3497E138}` `\Providers\BaseCSP` `64-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\Wow6432Nod` `e\Passlogix\UAM\Aut` `henticators\{A1B345` `53-8D40-42A9-8ED5-F` `70E3497E138}\Provid` `ers\BaseCSP`
Smart Card	Microsoft Base CSP Provider	DWORD	`SessionKeyUseSma` `rtCardCerts`	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.	`32-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\Passlogix\` `UAM\Authenticators\` `{A1B34553-8D40-42A9` `-8ED5-F70E3497E138}` `\Providers\BaseCSP` `64-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\Wow6432Nod` `e\Passlogix\UAM\Aut` `henticators\{A1B345` `53-8D40-42A9-8ED5-F` `70E3497E138}\Provid` `ers\BaseCSP`

Target	Category	Type	Name	Values	Description	Path

Smart Card	Microsoft Base CSP Provider	DWORD	`SessionKeyStrict KeyCipher`	Disabled (0) (default), Enabled (1)	Card PIN type only. If enabled, ignore certificates and key pairs without Key Cipher usage (whether Smart Card Usage or not).	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Passlogix\`
						`UAM\Authenticators\`
						`{A1B34553-8D40-42A9`
						`-8ED5-F70E3497E138}`
						`\Providers\BaseCSP`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\Aut`
						`henticators\{A1B345`
						`53-8D40-42A9-8ED5-F`
						`70E3497E138}\Provid`
						`ers\BaseCSP`

Smart Card	Microsoft Base CSP Provider	DWORD	`SessionKeyUseEss oKeyPair`	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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Passlogix\`
						`UAM\Authenticators\`
						`{A1B34553-8D40-42A9`
						`-8ED5-F70E3497E138}`
						`\Providers\BaseCSP`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\Aut`
						`henticators\{A1B345`
						`53-8D40-42A9-8ED5-F`
						`70E3497E138}\Provid`
						`ers\BaseCSP`

Smart Card	Microsoft Base CSP Provider	DWORD	`SessionKeyRegene rateEssoKeyPair`	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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Passlogix\`
						`UAM\Authenticators\`
						`{A1B34553-8D40-42A9`
						`-8ED5-F70E3497E138}`
						`\Providers\BaseCSP`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\Aut`
						`henticators\{A1B345`
						`53-8D40-42A9-8ED5-F`
						`70E3497E138}\Provid`
						`ers\BaseCSP`

Smart Card	Microsoft Base CSP Provider	DWORD	`SessionKeyEssoKe yPairBits`	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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Passlogix\`
						`UAM\Authenticators\`
						`{A1B34553-8D40-42A9`
						`-8ED5-F70E3497E138}`
						`\Providers\BaseCSP`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\Aut`
						`henticators\{A1B345`
						`53-8D40-42A9-8ED5-F`
						`70E3497E138}\Provid`
						`ers\BaseCSP`

Target	Category	Type	Name	Values	Description	Path

Smart Card	Microsoft Base CSP Provider	DWORD	`SessionKeyPrefer SmartCardCert`	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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Passlogix\`
						`UAM\Authenticators\`
						`{A1B34553-8D40-42A9`
						`-8ED5-F70E3497E138}`
						`\Providers\BaseCSP`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\Aut`
						`henticators\{A1B345`
						`53-8D40-42A9-8ED5-F`
						`70E3497E138}\Provid`
						`ers\BaseCSP`

Smart Card	Microsoft Base CSP Provider	DWORD	`SessionKeyPrefer EssoKeyPair`	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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Passlogix\`
						`UAM\Authenticators\`
						`{A1B34553-8D40-42A9`
						`-8ED5-F70E3497E138}`
						`\Providers\BaseCSP`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\Aut`
						`henticators\{A1B345`
						`53-8D40-42A9-8ED5-F`
						`70E3497E138}\Provid`
						`ers\BaseCSP`

Smart Card	Microsoft Base CSP Provider	DWORD	`SessionKeyPrompt IfMultipleCerts`	Enabled (1) (default), or Disabled (0)	Card PIN mode only. If disabled, choose a certificate at random (will attempt to use newest certificate).	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Passlogix\`
						`UAM\Authenticators\`
						`{A1B34553-8D40-42A9`
						`-8ED5-F70E3497E138}`
						`\Providers\BaseCSP`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\Aut`
						`henticators\{A1B345`
						`53-8D40-42A9-8ED5-F`
						`70E3497E138}\Provid`
						`ers\BaseCSP`

Smart Card	Microsoft Base CSP Provider	DWORD	`SessionKeyPrompt Always`	Enabled (1) (default), or Disabled (0)	Card PIN mode only. If enabled, always prompt to confirm certificate selection even if only a single certificate is available.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Passlogix\`
						`UAM\Authenticators\`
						`{A1B34553-8D40-42A9`
						`-8ED5-F70E3497E138}`
						`\Providers\BaseCSP`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\Aut`
						`henticators\{A1B345`
						`53-8D40-42A9-8ED5-F`
						`70E3497E138}\Provid`
						`ers\BaseCSP`

Target	Category	Type	Name	Values	Description	Path

Smart Card	Microsoft Base CSP Provider	DWORD	`SessionKeyPrompt EssoKeyPair`	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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Passlogix\`
						`UAM\Authenticators\`
						`{A1B34553-8D40-42A9`
						`-8ED5-F70E3497E138}`
						`\Providers\BaseCSP`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\Aut`
						`henticators\{A1B345`
						`53-8D40-42A9-8ED5-F`
						`70E3497E138}\Provid`
						`ers\BaseCSP`

Smart Card	Microsoft Base CSP Provider	DWORD	`SessionKeyAllowA esKeys`	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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Passlogix\`
						`UAM\Authenticators\`
						`{A1B34553-8D40-42A9`
						`-8ED5-F70E3497E138}`
						`\Providers\BaseCSP`
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\Aut`
						`henticators\{A1B345`
						`53-8D40-42A9-8ED5-F`
						`70E3497E138}\Provid`
						`ers\BaseCSP`

Smart Card	Microsoft Base CSP Provider	DWORD	`SessionKeyAllowD esKeys`	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).	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Passlogix\`
						`UAM\Authenticators\`
						`{A1B34553-8D40-42A9`
						`-8ED5-F70E3497E138}`
						`\Providers\BaseCSP`
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\Aut`
						`henticators\{A1B345`
						`53-8D40-42A9-8ED5-F`
						`70E3497E138}\Provid`
						`ers\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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Passlogix\`
						`UAM\Authenticators\`
						`{A1B34553-8D40-42A9`
						`-8ED5-F70E3497E138}`
						`\Providers\BaseCSP`
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\Aut`
						`henticators\{A1B345`
						`53-8D40-42A9-8ED5-F`
						`70E3497E138}\Provid`
						`ers\BaseCSP`

Target	Category	Type	Name	Values	Description	Path

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).	`32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\ UAM\Authenticators\ {A1B34553-8D40-42A9 -8ED5-F70E3497E138} \Providers\BaseCSP`
						
						`64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix\UAM\Aut henticators\{A1B345 53-8D40-42A9-8ED5-F 70E3497E138}\Provid ers\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.	`32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\ UAM\Authenticators\ {A1B34553-8D40-42A9 -8ED5-F70E3497E138} \Providers\BaseCSP`
						
						`64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix\UAM\Aut henticators\{A1B345 53-8D40-42A9-8ED5-F 70E3497E138}\Provid ers\BaseCSP`

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.	`32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\ UAM\Authenticators\ {A1B34553-8D40-42A9 -8ED5-F70E3497E138} \Providers\BaseCSP`
						
						`64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix\UAM\Aut henticators\{A1B345 53-8D40-42A9-8ED5-F 70E3497E138}\Provid ers\BaseCSP`

Smart Card	PKCS#11 Provider	DWORD	`Enabled`	Enabled (1), or Disabled (0) (default)	Enable or disable smart card authenticator support for PKCS#11.	`32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553- 8D40-42A9-8ED5-F70E 3497E138}\Providers \PKCS#11`
						
						`64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix\UAM\ Authenticators\ {A1B34553- 8D40-42A9-8ED5-F70E 3497E138}\Providers \PKCS#11`

Target	Category	Type	Name	Values	Description	Path

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.	`32-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\` `Passlogix\UAM\` `Authenticators\` `{A1B34553-` `8D40-42A9-8ED5-F70E` `3497E138}\Providers` `\PKCS#11`
						
						`64-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\Wow6432Nod` `e\Passlogix\UAM\` `Authenticators\` `{A1B34553-` `8D40-42A9-8ED5-F70E` `3497E138}\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.	`32-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\` `Passlogix\UAM\` `Authenticators\` `{A1B34553-` `8D40-42A9-8ED5-F70E` `3497E138}\Providers` `\PKCS#11`
						
						`64-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\Wow6432Nod` `e\Passlogix\UAM\` `Authenticators\` `{A1B34553-` `8D40-42A9-8ED5-F70E` `3497E138}\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.	`32-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\` `Passlogix\UAM\` `Authenticators\` `{A1B34553-8D40-42A9` `-8ED5-F70E3497E138}` `\Providers\PKCS#11`
						
						`64-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\Wow6432Nod` `e\Passlogix\UAM\` `Authenticators\` `{A1B34553-8D40-42A9` `-8ED5-F70E3497E138}` `\Providers\PKCS#11`

Target	Category	Type	Name	Values	Description	Path

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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM\Authe`
						`nticators\`
						`{A1B34553-8D40-42A9`
						`-8ED5-F70E3497E138}`
						`\Settings`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\Aut`
						`henticators\`
						`{A1B34553-8D40-42A9`
						`-8ED5-F70E3497E138}`
						`\Settings`

Smart Card	PKCS#11 Provider	DWORD	`SerialTimeout`	Default is 500 ms
				
				Allowed range is 0-5000 ms
					Max time to wait for a PKCS#11 module to report serial information for an inserted card.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM\`
						`Authenticators\`
						`{A1B34553-8D40-`
						`42A9-8ED5-F70E3497E`
						`138}\Settings`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\`
						`Authenticators\`
						`{A1B34553-8D40-`
						`42A9-8ED5-F70E3497E`
						`138}\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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM\`
						`Authenticators\`
						`{A1B34553-8D40-`
						`42A9-8ED5-F70E3497E`
						`138}\Settings`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\`
						`Authenticators\`
						`{A1B34553-8D40-`
						`42A9-8ED5-F70E3497E`
						`138}\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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM\`
						`Authenticators\`
						`{A1B34553-`
						`8D40-42A9-8ED5-F70E`
						`3497E138}\Providers`
						`\PKCS#11`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\`
						`Authenticators\`
						`{A1B34553-`
						`8D40-42A9-8ED5-F70E`
						`3497E138}\Providers`
						`\PKCS#11`

Target	Category	Type	Name	Values	Description	Path

Smart Card	PKCS#11 Provider	DWORD	`ExternalAuthDial og`	Hide Status Dialog (0) (default), Show Status Dialog (1)	Show or hide status dialog when performing external authentication.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM\`
						`Authenticators\`
						`{A1B34553-`
						`8D40-42A9-8ED5-F70E`
						`3497E138}\Providers`
						`\PKCS#11`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\`
						`Authenticators\`
						`{A1B34553-`
						`8D40-42A9-8ED5-F70E`
						`3497E138}\Providers`
						`\PKCS#11`

Smart Card	PKCS#11 Provider	DWORD	`ExternalEnrollMo de`	Auth Mode Reauthentication (0) (default), PIN + Morpho Fingerprint Enroll (1), Force Smart Card PIN Auth (2)	Smart card enrollment behavior.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM\`
						`Authenticators\`
						`{A1B34553-`
						`8D40-42A9-8ED5-F70E`
						`3497E138}\Providers`
						`\PKCS#11`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\`
						`Authenticators\`
						`{A1B34553-`
						`8D40-42A9-8ED5-F70E`
						`3497E138}\Providers`
						`\PKCS#11`

Smart Card	PKCS#11 Provider	DWORD	`SessionKeyUseCsp ForPki`	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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM\`
						`Authenticators\`
						`{A1B34553-`
						`8D40-42A9-8ED5-F70E`
						`3497E138}\Providers`
						`\PKCS#11`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\`
						`Authenticators\`
						`{A1B34553-`
						`8D40-42A9-8ED5-F70E`
						`3497E138}\Providers`
						`\PKCS#11`

Target	Category	Type	Name	Values	Description	Path
Smart Card	PKCS#11 Provider	DWORD	`SessionKeyUseKey CipherCerts`	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.	`32-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\` `Passlogix\UAM\` `Authenticators\` `{A1B34553-` `8D40-42A9-8ED5-F70E` `3497E138}\Providers` `\PKCS#11`
						`64-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\Wow6432Nod` `e\Passlogix\UAM\` `Authenticators\` `{A1B34553-` `8D40-42A9-8ED5-F70E` `3497E138}\Providers` `\PKCS#11`
Smart Card	PKCS#11 Provider	DWORD	`SessionKeyUseSma rtCardCerts`	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.	`32-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\` `Passlogix\UAM\` `Authenticators\` `{A1B34553-` `8D40-42A9-8ED5-F70E` `3497E138}\Providers` `\PKCS#11`
						`64-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\Wow6432Nod` `e\Passlogix\UAM\` `Authenticators\` `{A1B34553-` `8D40-42A9-8ED5-F70E` `3497E138}\Providers` `\PKCS#11`
Smart Card	PKCS#11 Provider	DWORD	`SessionKeyStrict KeyCipher`	Disabled (0) (default), Enabled (1)	Card PIN type only. If enabled, ignore certificates and key pairs without Key Cipher usage (whether Smart Card Usage or not).	`32-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\` `Passlogix\UAM\` `Authenticators\` `{A1B34553-` `8D40-42A9-8ED5-F70E` `3497E138}\Providers` `\PKCS#11`
						`64-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\Wow6432Nod` `e\Passlogix\UAM\` `Authenticators\` `{A1B34553-` `8D40-42A9-8ED5-F70E` `3497E138}\Providers` `\PKCS#11`

Target	Category	Type	Name	Values	Description	Path

Smart Card	PKCS#11 Provider	DWORD	`SessionKeyUseEss oKeyPair`	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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM\`
						`Authenticators\`
						`{A1B34553-`
						`8D40-42A9-8ED5-F70E`
						`3497E138}\Providers`
						`\PKCS#11`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\`
						`Authenticators\`
						`{A1B34553-`
						`8D40-42A9-8ED5-F70E`
						`3497E138}\Providers`
						`\PKCS#11`

Smart Card	PKCS#11 Provider	DWORD	`SessionKeyRegene rateEssoKeyPair`	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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM\`
						`Authenticators\`
						`{A1B34553-`
						`8D40-42A9-8ED5-F70E`
						`3497E138}\Providers`
						`\PKCS#11`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\`
						`Authenticators\`
						`{A1B34553-`
						`8D40-42A9-8ED5-F70E`
						`3497E138}\Providers`
						`\PKCS#11`

Smart Card	PKCS#11 Provider	DWORD	`SessionKeyEssoKe yPairBits`	1024-4096 bits. Default is 2048 bits.	Card PIN mode only.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM\`
						`Authenticators\`
						`{A1B34553-`
						`8D40-42A9-8ED5-F70E`
						`3497E138}\Providers`
						`\PKCS#11`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\`
						`Authenticators\`
						`{A1B34553-`
						`8D40-42A9-8ED5-F70E`
						`3497E138}\Providers`
						`\PKCS#11`

Target	Category	Type	Name	Values	Description	Path

Smart Card	PKCS#11 Provider	DWORD	`SessionKeyPrefer SmartCardCert`	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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM\`
						`Authenticators\`
						`{A1B34553-`
						`8D40-42A9-8ED5-F70E`
						`3497E138}\Providers`
						`\PKCS#11`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\`
						`Authenticators\`
						`{A1B34553-`
						`8D40-42A9-8ED5-F70E`
						`3497E138}\Providers`
						`\PKCS#11`

Smart Card	PKCS#11 Provider	DWORD	`SessionKeyPrefer EssoKeyPair`	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.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM\`
						`Authenticators\`
						`{A1B34553-`
						`8D40-42A9-8ED5-F70E`
						`3497E138}\Providers`
						`\PKCS#11`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\`
						`Authenticators\`
						`{A1B34553-`
						`8D40-42A9-8ED5-F70E`
						`3497E138}\Providers`
						`\PKCS#11`

Smart Card	PKCS#11 Provider	DWORD	`SessionKeyPrompt IfMultipleCerts`	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).	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\`
						`Passlogix\UAM\`
						`Authenticators\`
						`{A1B34553-`
						`8D40-42A9-8ED5-F70E`
						`3497E138}\Providers`
						`\PKCS#11`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Nod`
						`e\Passlogix\UAM\`
						`Authenticators\`
						`{A1B34553-`
						`8D40-42A9-8ED5-F70E`
						`3497E138}\Providers`
						`\PKCS#11`

Target	Category	Type	Name	Values	Description	Path

Smart Card	PKCS#11 Provider	DWORD	`SessionKeyPrompt Always`	Enabled (1) (default), or Disabled (0)	Card PIN mode only. If enabled, always prompt to confirm certificate selection even if only a single certificate is available.	`32-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\` `Passlogix\UAM\` `Authenticators\` `{A1B34553-` `8D40-42A9-8ED5-F70E` `3497E138}\Providers` `\PKCS#11`
						
						 `64-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\Wow6432Nod` `e\Passlogix\UAM\` `Authenticators\` `{A1B34553-` `8D40-42A9-8ED5-F70E` `3497E138}\Providers` `\PKCS#11`

Smart Card	PKCS#11 Provider	DWORD	`SessionKeyPrompt EssoKeyPair`	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.	`32-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\` `Passlogix\UAM\` `Authenticators\` `{A1B34553-` `8D40-42A9-8ED5-F70E` `3497E138}\Providers` `\PKCS#11`
						
						 `64-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\Wow6432Nod` `e\Passlogix\UAM\` `Authenticators\` `{A1B34553-` `8D40-42A9-8ED5-F70E` `3497E138}\Providers` `\PKCS#11`

Smart Card	PKCS#11 Provider	DWORD	`SessionKeyAllowA esKeys`	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.	`32-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\` `Passlogix\UAM\` `Authenticators\` `{A1B34553-` `8D40-42A9-8ED5-F70E` `3497E138}\Providers` `\PKCS#11` `64-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\Wow6432Nod` `e\Passlogix\UAM\` `Authenticators\` `{A1B34553-` `8D40-42A9-8ED5-F70E` `3497E138}\Providers` `\PKCS#11`

Target	Category	Type	Name	Values	Description	Path
Smart Card	PKCS#11 Provider	DWORD	SessionKeyAllowD esKeys	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).	32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553- 8D40-42A9-8ED5-F70E 3497E138}\Providers \PKCS#11 64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix\UAM\ Authenticators\ {A1B34553- 8D40-42A9-8ED5-F70E 3497E138}\Providers \PKCS#11
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.	32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553- 8D40-42A9-8ED5-F70E 3497E138}\Providers \PKCS#11 64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix\UAM\ Authenticators\ {A1B34553- 8D40-42A9-8ED5-F70E 3497E138}\Providers \PKCS#11
Smart Card	PKCS#11 Provider	DWORD	SessionKeyCertCh eckTime	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).	32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\ Authenticators\ {A1B34553- 8D40-42A9-8ED5-F70E 3497E138}\Providers \PKCS#11 64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Nod e\Passlogix\UAM\ Authenticators\ {A1B34553- 8D40-42A9-8ED5-F70E 3497E138}\Providers \PKCS#11

Target	Category	Type	Name	Values	Description	Path
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.	`32-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\` `Passlogix\UAM\` `Authenticators\` `{A1B34553-` `8D40-42A9-8ED5-F70E` `3497E138}\Providers` `\PKCS#11` `64-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\Wow6432Nod` `e\Passlogix\UAM\` `Authenticators\` `{A1B34553-` `8D40-42A9-8ED5-F70E` `3497E138}\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.	`32-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\` `Passlogix\UAM\` `Authenticators\` `{A1B34553-` `8D40-42A9-8ED5-F70E` `3497E138}\Providers` `\PKCS#11` `64-bit OS:` `HKEY_LOCAL_MACHINE\` `SOFTWARE\Wow6432Nod` `e\Passlogix\UAM\` `Authenticators\` `{A1B34553-` `8D40-42A9-8ED5-F70E` `3497E138}\Providers` `\PKCS#11`

7.5.3 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	`32-bit OS:` `HKEY_LOCAL_` `MACHINE\SOFTWARE\` `Passlogix\UAM\Branding` `64-bit OS:` `HKEY_LOCAL_` `MACHINE\SOFTWARE\Wow64` `32Node\Passlogix\UAM\B` `randing`
Framework	Common	SZ	`STR:Framework:137`	Oracle Enterprise Single Sign-On Universal Authentication Manager	Product Long Name	`32-bit OS:` `HKEY_LOCAL_` `MACHINE\SOFTWARE\` `Passlogix\UAM\Branding` `64-bit OS:` `HKEY_LOCAL_` `MACHINE\SOFTWARE\Wow64` `32Node\Passlogix\UAM\B` `randing`

Target	Category	Type	Name	Values	Description	Path
Framework	Reauthentication	SZ	`BMP:Framework:112`	N/A	Reauthentication Banner (500x75)	32-bit OS: `HKEY_LOCAL_MACHINE\ SOFTWARE\ Passlogix\UAM\Branding` 64-bit OS: `HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Node\P asslogix\UAM\Branding`
Framework	Reauthentication	SZ	`BMP:Framework:111`	N/A	Reauthentication Band (500x2)	32-bit OS: `HKEY_LOCAL_ MACHINE\SOFTWARE\ Passlogix\UAM\Branding` 64-bit OS: `HKEY_LOCAL_ MACHINE\SOFTWARE\Wow64 32Node\Passlogix\UAM\B randing`
Fingerprint	General	SZ	`STR:BiometricAuth:107`	Fingerprint	Authenticator Name	32-bit OS: `HKEY_LOCAL_ MACHINE\SOFTWARE\ Passlogix\UAM\ Authenticators\ {16627EE1-FAE3-43B5-B8 84-D3661649B97D}\Brand ing` 64-bit OS: `HKEY_LOCAL_ MACHINE\SOFTWARE\Wow64 32Node\Passlogix\UAM\ Authenticators\ {16627EE1-FAE3-43B5-B8 84-D3661649B97D}\Brand ing`
Fingerprint	General	SZ	`ICO:BiometricAuth:103`	N/A	Authenticator Icon (24x24)	32-bit OS: `HKEY_LOCAL_ MACHINE\SOFTWARE\ Passlogix\UAM\ Authenticators\ {16627EE1-FAE3-43B5-B8 84-D3661649B97D}\Brand ing` 64-bit OS: `HKEY_LOCAL_ MACHINE\SOFTWARE\Wow64 32Node\Passlogix\UAM\ Authenticators\ {16627EE1-FAE3-43B5-B8 84-D3661649B97D}\Brand ing`
Fingerprint	General	SZ	`ICO:BiometricAuth:109`	N/A	Authenticator Icon (48x48)	32-bit OS: `HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM \Authenticators\ {16627EE1- FAE3-43B5-B884-D366164 9B97D}\Branding` 64-bit OS: `HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Node\P asslogix\UAM\Authentic ators\ {16627EE1- FAE3-43B5-B884-D366164 9B97D}\Branding`

Target	Category	Type	Name	Values	Description	Path

Fingerprint	General	SZ	`ICO:Biometri cAuth:112`	N/A	Authenticator Icon (128x128)	`32-bit OS:`
						`HKEY_LOCAL_`
						`MACHINE\SOFTWARE\Passl`
						`ogix\UAM\Authenticator`
						`s\{16627EE1-FAE3-43B5-`
						`B884-D3661649B97D}\Bra`
						`nding`
						
						`64-bit OS:`
						`HKEY_LOCAL_`
						`MACHINE\SOFTWARE\Wow64`
						`32Node\Passlogix\UAM\A`
						`uthenticators\{16627EE`
						`1-FAE3-43B5-B884-D3661`
						`649B97D}\Branding`

Proximity Card	Sound Effects	SZ	`WAV:ProxCard Auth:113`	N/A	Omnikey: Undefined = default sound; Blank = disabled. RFIdeas: Disabled by default; use "DEFAULT" to enable.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Passlogix\UAM`
						`\Authenticators\`
						`{4A8F93E4-2328-44CA-8D`
						`BE-FBFA4E5FD334}\Brand`
						`ing`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Node\P`
						`asslogix\UAM\Authentic`
						`ators\`
						`{4A8F93E4-2328-44CA-8D`
						`BE-FBFA4E5FD334}\Brand`
						`ing`

Proximity Card	Sound Effects	SZ	`WAV:ProxCard Auth:110`	N/A	Disabled by default; use "DEFAULT" to enable.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Passlogix\UAM`
						`\Authenticators\`
						`{4A8F93E4-2328-44CA-8D`
						`BE-FBFA4E5FD334}\Brand`
						`ing`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Node\P`
						`asslogix\UAM\Authentic`
						`ators\`
						`{4A8F93E4-2328-44CA-8D`
						`BE-FBFA4E5FD334}\Brand`
						`ing`

Proximity Card	Sound Effects	SZ	`WAV:ProxCard Auth:112`	N/A	Applies only to Omnikey, if MinPresence is enabled. Undefined = default sound; Blank = disabled.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Passlogix\UAM`
						`\Authenticators\`
						`{4A8F93E4-`
						`2328-44CA-8DBE-FBFA4E5`
						`FD334}\Branding`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Node\P`
						`asslogix\UAM\Authentic`
						`ators\ {4A8F93E4-`
						`2328-44CA-8DBE-FBFA4E5`
						`FD334}\Branding`

Target	Category	Type	Name	Values	Description	Path

Proximity Card	General	SZ	`STR:ProxCard Auth:101`	Proximity Card	Authenticator Name	`32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM \Authenticators\ {4A8F93E4-2328- 44CA-8DBE-FBFA4E5FD334 }\Branding`
						
						`64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Node\P asslogix\UAM\Authentic ators\ {4A8F93E4-2328- 44CA-8DBE-FBFA4E5FD334 }\Branding`

Proximity Card	General	SZ	`STR:ProxCard Auth:142`	N/ASZ	Default token description. Restricted to alphanumeric and space characters.	`32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM \Authenticators\ {4A8F93E4-2328- 44CA-8DBE-FBFA4E5FD334 }\Branding`
						
						`64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Node\P asslogix\UAM\Authentic ators\ {4A8F93E4-2328- 44CA-8DBE-FBFA4E5FD334 }\Branding`

Proximity Card	General	SZ	`ICO:ProxCard Auth:106`	N/A	Authenticator Absent Icon (24x24)	`32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM \Authenticators\ {4A8F93E4- 2328-44CA-8DBE-FBFA4E5 FD334}\Branding`
						
						`64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Node\P asslogix\UAM\Authentic ators\ {4A8F93E4- 2328-44CA-8DBE-FBFA4E5 FD334}\Branding`

Proximity Card	General	SZ	`ICO:ProxCard Auth:109`	N/A	Authenticator Absent Icon (48x48)	`32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM \Authenticators\ {4A8F93E4- 2328-44CA-8DBE-FBFA4E5 FD334}\Branding`
						
						`64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Node\P asslogix\UAM\Authentic ators\ {4A8F93E4- 2328-44CA-8DBE-FBFA4E5 FD334}\Branding`

Target	Category	Type	Name	Values	Description	Path
Proximity Card	General	SZ	ICO:ProxCard Auth:114	N/A	Authenticator Absent Icon (128x128)	32-bit OS: HKEY_LOCAL_ MACHINE\SOFTWARE\Passl ogix\UAM\ Authenticators\{4A8F93 E4-2328-44CA-8DBE-FBFA 4E5FD334\\Branding 64-bit OS: HKEY_LOCAL_ MACHINE\SOFTWARE\Wow64 32Node\Passlogix\UAM\ Authenticators\{4A8F93 E4-2328-44CA-8DBE-FBFA 4E5FD334\Branding
Proximity Card	General	SZ	ICO:ProxCard Auth:107	N/A	Authenticator Present Icon (24x24)	32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM \Authenticators\ {4A8F93E4- 2328-44CA-8DBE-FBFA4E5 FD334}\Branding 64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Node\P asslogix\UAM\Authentic ators\ {4A8F93E4- 2328-44CA-8DBE-FBFA4E5 FD334}\Branding
Proximity Card	General	SZ	ICO:ProxCard Auth:108	N/A	Authenticator Present Icon (48x48)	32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM \Authenticators\ {4A8F93E4- 2328-44CA-8DBE-FBFA4E5 FD334}\Branding 64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Node\P asslogix\UAM\Authentic ators\ {4A8F93E4- 2328-44CA-8DBE-FBFA4E5 FD334}\Branding
Proximity Card	General	SZ	ICO:ProxCard Auth:115	N/A	Authenticator Present Icon (128x128)	32-bit OS: HKEY_LOCAL_ MACHINE\SOFTWARE\Passl ogix\UAM\ Authenticators\{4A8F93 E4-2328-44CA-8DBE-FBFA 4E5FD334}\Branding 64-bit OS: HKEY_LOCAL_ MACHINE\SOFTWARE\Wow64 32Node\Passlogix\UAM\ Authenticators\{4A8F93 E4-2328-44CA-8DBE-FBFA 4E5FD334}\Branding

Target	Category	Type	Name	Values	Description	Path

Smart Card	General	SZ	`STR:SmartCar dAuth:101`	Smart Card	Authenticator Name	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Passlogix\UAM`
						`\Authenticators\`
						`{A1B34553-`
						`8D40-42A9-8ED5-F70E349`
						`7E138}\Branding`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Node\P`
						`asslogix\UAM\Authentic`
						`ators\ {A1B34553-`
						`8D40-42A9-8ED5-F70E349`
						`7E138}\Branding`

Smart Card	General	SZ	`STR:SmartCar dAuth:173`	My smart card	Default token description. Restricted to alphanumeric and space characters.	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Passlogix\UAM`
						`\Authenticators\`
						`{A1B34553-`
						`8D40-42A9-8ED5-F70E349`
						`7E138}\Branding`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Node\P`
						`asslogix\UAM\Authentic`
						`ators\ {A1B34553-`
						`8D40-42A9-8ED5-F70E349`
						`7E138}\Branding`

Smart Card	General	SZ	`ICO:SmartCar dAuth:103`	N/A	Authenticator Absent Icon (24x24)	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Passlogix\UAM`
						`\Authenticators\`
						`{A1B34553-`
						`8D40-42A9-8ED5-F70E349`
						`7E138}\Branding`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Node\P`
						`asslogix\UAM\Authentic`
						`ators\ {A1B34553-`
						`8D40-42A9-8ED5-F70E349`
						`7E138}\Branding`

Smart Card	General	SZ	`ICO:SmartCar dAuth:110`	N/A	Authenticator Absent Icon (48x48)	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Passlogix\UAM`
						`\Authenticators\`
						`{A1B34553-`
						`8D40-42A9-8ED5-F70E349`
						`7E138}\Branding`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\`
						`SOFTWARE\Wow6432Node\P`
						`asslogix\UAM\Authentic`
						`ators\ {A1B34553-`
						`8D40-42A9-8ED5-F70E349`
						`7E138}\Branding`

Target	Category	Type	Name	Values	Description	Path

Smart Card	General	SZ	`ICO:SmartCardAuth:112`	N/A	Authenticator Absent Icon (128x128)	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix\UAM\Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}\Branding`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Passlogix\UAM\Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}\Branding`

Smart Card	General	SZ	`ICO:SmartCardAuth:108`	N/A	Authenticator Present Icon (24x24)	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix\UAM\Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}\Branding`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Passlogix\UAM\Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Branding`

Smart Card	General	SZ	`ICO:SmartCardAuth:109`	N/A	Authenticator Present Icon (48x48)	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix\UAM\Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}\Branding`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Passlogix\UAM\Authenticators\ {A1B34553-8D40-42A9-8ED5-F70E3497E138}\Branding`

Smart Card	General	SZ	`ICO:SmartCardAuth:113`	N/A	Authenticator Present Icon (128x128)	`32-bit OS:`
						`HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix\UAM\Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}\Branding`
						
						`64-bit OS:`
						`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Passlogix\UAM\Authenticators\{A1B34553-8D40-42A9-8ED5-F70E3497E138}\Branding`

Target	Category	Type	Name	Values	Description	Path

Challenge Questions	General	SZ	`ICO:Passphra seAuth:101`	Challenge Questions	Authenticator Name	`32-bit OS:` `HKEY_LOCAL_ MACHINE\SOFTWARE\Passl ogix\UAM\ Authenticators\{393D4B 53-EC46-4A38-9E9E-3D6B 5141DD34}\Branding`
						
						 `64-bit OS:` `HKEY_LOCAL_ MACHINE\SOFTWARE\Wow64 32Node\Passlogix\UAM\ Authenticators\{393D4B 53-EC46-4A38-9E9E-3D6B 5141DD34}\Branding`

Challenge Questions	General	SZ	`ICO:Passphra seAuth:103`	N/A	Authenticator Icon (24x24)	`32-bit OS:` `HKEY_LOCAL_ MACHINE\SOFTWARE\Passl ogix\UAM\ Authenticators\{393D4B 53-EC46-4A38-9E9E-3D6B 5141DD34}\Branding`
						
						 `64-bit OS:` `HKEY_LOCAL_ MACHINE\SOFTWARE\Wow64 32Node\Passlogix\UAM\ Authenticators\{393D4B 53-EC46-4A38-9E9E-3D6B 5141DD34}\Branding`

Challenge Questions	General	SZ	`ICO:Passphra seAuth:105`	N/A	Authenticator Icon (48x48)	`32-bit OS:` `HKEY_LOCAL_ MACHINE\SOFTWARE\Passl ogix\UAM\ Authenticators\{393D4B 53-EC46-4A38-9E9E-3D6B 5141DD34}\Branding`
						
						 `64-bit OS:` `HKEY_LOCAL_ MACHINE\SOFTWARE\Wow64 32Node\Passlogix\UAM\ Authenticators\{393D4B 53-EC46-4A38-9E9E-3D6B 5141DD34}\Branding`

Challenge Questions	General	SZ	`ICO:Passphra seAuth:106`	N/A	Authenticator Icon (128x128)	`32-bit OS:` `HKEY_LOCAL_ MACHINE\SOFTWARE\Passl ogix\UAM\ Authenticators\{393D4B 53-EC46-4A38-9E9E-3D6B 5141DD34}\Branding`
						
						 `64-bit OS:` `HKEY_LOCAL_ MACHINE\SOFTWARE\Wow64 32Node\Passlogix\UAM\ Authenticators\{393D4B 53-EC46-4A38-9E9E-3D6B 5141DD34}\Branding`

Target	Category	Type	Name	Values	Description	Path
Windows Password	General	SZ	STR:WinPwdAuth:101	Windows Password	Authenticator Name	32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM \Authenticators\ {0C29417D-8A20-48B7-8CC4-D948D38 4E9B2}\Branding
						64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Node\P asslogix\UAM\Authentic ators\ {0C29417D-8A20-48B7-8CC4-D948D38 4E9B2}\Branding
Windows Password	General	SZ	ICO:WinPwdAuth:104	N/A	Authenticator Icon (24x24)	32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM \Authenticators\ {0C29417D-8A20-48B7-8CC4-D948D38 4E9B2}\Branding
						64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Node\P asslogix\UAM\Authentic ators\ {0C29417D-8A20-48B7-8CC4-D948D38 4E9B2}\Branding
Windows Password	General	SZ	ICO:WinPwdAuth:103	N/A	Authenticator Icon (48x48)	32-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Passlogix\UAM \Authenticators\ {0C29417D-8A20-48B7-8CC4-D948D38 4E9B2}\Branding
						64-bit OS: HKEY_LOCAL_MACHINE\ SOFTWARE\Wow6432Node\P asslogix\UAM\Authentic ators\ {0C29417D-8A20-48B7-8CC4-D948D38 4E9B2}\Branding
Windows Password	General	SZ	ICO:WinPwdAuth:105	N/A	Authenticator Icon (128x128)	32-bit OS: HKEY_LOCAL_ MACHINE\SOFTWARE\Passl ogix\UAM\ Authenticators\{0C2941 7D-8A20-48B7-8CC4-D948 D384E9B2}\Branding
						64-bit OS: HKEY_LOCAL_ MACHINE\SOFTWARE\Wow64 32Node\Passlogix\UAM\ Authenticators\{0C2941 7D-8A20-48B7-8CC4-D948 D384E9B2}\Branding

8

Troubleshooting

This section contains solutions to the most common problems encountered when installing, configuring, and deploying Oracle Enterprise Single Sign-On Suite. For in-depth discussion and best practices for administering the suite, see *Oracle Enterprise Single Sign-On Suite Installation Guide*, *Deploying Logon Manager with a Directory-Based Repository*, and *Configuring and Diagnosing Logon Manager Application Templates*.

8.1 Installation

Following are solutions to the most common installation scenario problems.

8.1.1 Authenticators

An authenticator is not installed when selected

By default, the installer does not install authenticators that will not work on the system. For example, if the Entrust Entelligence client is not installed, then the authenticator for the Entrust PKI will not be installed (Entrust Entelligence is available with Authentication Manager only).

8.1.2 Synchronizer Extensions

The Microsoft Active Directory extension is not installed when selected

By default, the installer does not install synchronizer extensions that will not work on the system. For example, if the Microsoft Active Directory client is not installed, then the synchronizer extension for the Microsoft Active Directory Server will not be installed.

8.1.3 Uninstalling

User credentials remain after uninstall

- Only the current user's credentials can be removed by the standard uninstall. A simple batch file can handle removing other credentials. For example:

  ```
  CD /D %UsersProfile%

  CD .

  For /D %Z in (*.*) do Del /F/S/Q "%Z\Application Data\SSO"
  ```

- You will need to manually delete registry entries for other users. This can be done in `RegEdit` or `RegEdit32` (`RegEdt32.exe`), or you can push the following `*.reg` file to each user:

Windows Registry Editor Version 5.00

```
HKey_Current_User\Software\Passlogix]
```

8.1.4 Agent Performance/Application Response

The Agent responds slowly, applications are slowed, or specific functions within applications are slowed, when the Agent is running.

- Some antiviral software programs check Agent modules too aggressively. To resolve this, disable checks of `ssoshell.exe` and/or of the `%ProgramFiles%\Passlogix\v-GO SSO` directory tree.

- Some antiviral software programs check `*.ini` files too aggressively. The Agent stores user credentials in `*.ini` files. To resolve this, disable checks of `*.ini` files, of the file `%UserName% aml.ini`, and/or of files in the `%AppData%\Passlogix` directory.

8.1.5 Authentication

Following are solutions to problems associated specifically with authentication.

8.1.5.1 Initial Authentication

User logs onto a computer with different domain/workgroup accounts but sees the same credentials.

The problem is that the local computer's Windows account provides the user's Registry Hive (`HKCU`), not the domain/workgroup account. There are two workarounds: use the `CleanupOnShutdown` feature or use a different Windows account for each domain/workgroup logon.

8.1.5.2 Reauthentication

Users are never asked to reauthenticate.

Make sure `Extensions\AccessManager:AutoLogin` is set to the desired value. The value is in milliseconds; a value of 900000 (default for client-side installations) is 15 minutes.

Users have to reauthenticate too frequently.

- Make sure `Extensions\AccessManager:AutoLogin` is set to the desired value. The value is in milliseconds; a value of 900000 (default for client-side installations) is 15 minutes.

- Make sure other force-reauth settings are set appropriately. These settings include:

  - Overriding settings: `Extensions\AccessManager:ReauthOnReveal`.

  - Application configuration settings: `ForceReauth`.

8.1.6 Application Configuration

Following are solutions to problems associated specifically with configuring Logon Manager's templates for any application.

8.1.6.1 All Applications

The Agent does not recognize pre-existing logon credentials after an upgrade

After an upgrade of the Agent, users report that applications for which they have previously provided credentials no longer function. Instead, a message box appears, advising that the credentials do not correspond to configured logons. The applications appear in Logon Manager in gray, italicized text.

Create a Bulk Add list to update the user's `entlist.ini`. Also note that in Logon Manager, preconfigured logons for Windows and Web applications are included in the Administrative Console templates, rather than in the Agent's `applist.ini`. Create the required application logons, using templates, then create the Bulk Add list to update the user's `entlist.ini`.

An application is not available in the list of predefined applications when you add credentials

Shut down the Agent making sure that no ssoshell.exe processes are running, and restart the Agent.

The Agent can be started and Logon Manager can be opened without the user authenticating

Shut down the Agent, kill any running ssoshell.exe or SSObho.exe processes, and restart the Agent.

8.1.6.2 Predefined Windows Applications

The Agent does not recognize a password change window –OR– The Agent does not respond to an application's configured password-change dialog

This can be remedied by adding the password-change form's window title to the main logon form's window-title matching list.

In the Administrative Console, select the application in the left pane and click the **General** tab. Double-click the **Password Change** form for the application to open the form configuration dialog. Note the Window Titles of the form, then click **Cancel**. Double-click the Logon form for the application and, under **Window Titles**, click **Add**. Enter the window title of the Password Change form, click **OK**, then click **OK** to close the form configuration dialog.

Double-Logon or Wrong Window

The Agent responds twice to an application or responds to a previously-invisible window or to the wrong window

- Use one or more (additional) Match sections and Field keys to specify more precise matching criteria.

- Specify the window class that should be ignored in **Ignore this Window Class** in the **Miscellaneous** tab on the application configuration.

The Agent does not respond to any Windows application

Shut down the Agent, kill any running `ssoshell.exe` or `SSObho.exe` processes, and restart the Agent.

The Agent does not respond to a specific Windows application
- Use fewer matching criteria.

- Check that the application configuration values that are numbers are in decimal, not hexadecimal.

- Check that the application configuration values that are strings are the exact ones in the application dialogs.

- If using multiple sections, try a test with just one section.

The Agent provides credentials but does not submit

Verify that **Auto Submit** is set in the **Miscellaneous** tab of the application configuration and **AutoOK** is set in the specific set of credentials.

8.1.6.3 All Web Applications

> **Note:** In order for Logon Manager to respond correctly to ActiveX-based logon forms, you must configure these forms as Windows applications, with the template targeting the Web browser window.
>
> Refer to *Configuring and Diagnosing Logon Manager Application Templates* for complete instructions.

The Agent does not detect or respond to a specific Web page

- Check that the page has a password field (Field Type of Password). Without it, the Agent will ignore the page.

- Check that SSObho.exe is running.

- Try disabling Java, JavaScript, and/or ActiveX support.

The Agent responds slowly to a specific Web page

- Check that the page has finished loading. The Agent does not respond to a page until the page finishes loading completely.

- Try turning off images.

- Try disabling Java, JavaScript, and/or ActiveX support.

The Agent doesn't respond to a loaded Web Application

1. Start the Agent, then trigger the Agent from the **Title Bar Button**.

2. Log On using Logon Manager.

3. Refresh the browser page.

The Agent doesn't respond to a selected logon using Logon Manager

There is a known issue in the Agent where it does not respond to Web Applications in this way. The Agent still responds via the other triggers.

> **Note:** If the browser is embedded within another application, the Agent might respond as if the browser is a Windows Application.

SSObho.exe does not run

If the Agent does not recognize web pages properly, make sure that SSObho.exe is running. If it is not, the Agent may think the user is in a Terminal Services session. To correct this:

1. Shut down the Agent. (Verify no SSO* tasks are running in Task Manager.)

2. Uninstall the Agent.

3. Make sure the following files are not present on the user's computer:

   - `SSOwts.exe`

   - `SSOwts.exe`

   - `SSOwts.exe`

4. Search using `RegEdit` in the system hives of the registry (for example, NOT in `HKEY_CURRENT_USER or HKEY_USERS`) for references to `SSO`, `vGO`, and `Passlogix`. Delete all inappropriate references, especially:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Passlogix` and its children

   `HKEY_LOCAL_ MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects\{04EB19CE-B3B3-11D2-8A09-006008C7059E}` and its children

   `HKEY_CLASSES_ROOT\CLSID\{04EB19CE-B3B3-11D2-8A09-006008C7059E}` and its children

   `HKEY_CLASSES_ROOT\AppID\SSO WTS.EXE` and its children

   `HKEY_CLASSES_ROOT\AppID\{6B9E3EFF-C54A-472C-821B-6FC464B58235}` and its children

   `HKEY_CLASSES_ROOT\SSObho.HelperObject` and its children

   `HKEY_CLASSES_ROOT\SSObho.HelperObject.1` and its children

5. Reinstall the Agent.

8.1.6.4 Web Applications That Are Predefined

The Agent provides credentials but does not submit
- If a Submit field is of type Image, make sure that the URL is exact, including the protocol.
- If a Submit field is not present, add one.

Instead of submitting the page, the Agent triggers a link to another page or some other action (for example, cancel/clear)
Add a Submit field to the application configuration.

The Web page uses more than three fields (for example, a Social Security # as three fields and a password)
Break the logon up into two (or more) logons. Then the user will select (via the Logon Chooser) first the credential lacking the password (with Auto Submit disabled) and then the credential with the password.

8.1.6.5 Web Applications That Are Not Predefined

The Agent provides credentials but does not submit

Keep the system focus on the window that is requesting the credentials; if you switch to another window, the Agent will supply the credentials but not tell the page to submit.

Instead of submitting the page, the Agent triggers a link to another page or some other action (for example, cancel/clear)

- Turn off Auto Submit for that credential, and manually trigger page submission.

- Predefine the page, specifying the Submit field.

When adding credentials, the window title is stored instead of the URL

Check that SSObho.exe is running. (See above.)

8.1.7 Host Applications

Following are solutions to problems particular to Logon Manager's response to Host/Mainframe applications.

8.1.7.1 Responding to All Host Applications

The Agent does not respond to any Host application

- Shut down the Agent, kill any running ssoshell.exe or SSObho.exe processes, and restart the Agent.

- Check that HLLAPI is properly enabled in the host emulator.

- Check that MFEnable=1.

- Check that the coordinates are relative to the top-left corner, where the top-left corner is (1,1) (row 1, column 1).

The Agent does not respond at all to any Telnet application

Check that the Host emulator supports Telnet through HLLAPI or through a scripting language.

> **Note:** The Agent supports Telnet through HLLAPI only for ScanPak Aviva and NetManage Rumba.

8.1.7.2 Responding to a Specific Host Application

One or more credential fields are not inserted, or are partially inserted

- Check that the coordinates are relative to the top-left corner, where the top-left corner is (1,1) (row 1, column 1).

- Check that application configuration coordinates are for the exact place where credentials are inserted; usually, there is a space after the field prompts (for example, "Username:Space"), and the credential field needs to be inserted after the space.

- If a special character sequence is used between fields, check that the sequence is valid, that **Delay Field** is set to a sufficiently high value.

The Agent does not respond at all to a specific Host application

- Check that the coordinates are relative to the top-left corner, where the top-left corner is (1,1) (row 1, column 1).

- Use fewer matching criteria.

The Agent does not respond at all to a specific Telnet application

Check that the coordinates for all fields are set to (1,1).

8.1.8 Event Logging

Following are solutions to problems associated with Event Logging with any extension.

8.1.8.1 All Extensions

No events are recorded

- The Filter setting is not set. For testing purposes, set to `0xFFFFFFFF` (to log all events) and restart the Agent.

- The Agent has not reached the Retry setting (default: 30 minutes). To change the value from the default, set `Extensions\EventManager:Retry` or `Extensions\EventManager\%Extension%:Retry` to a lower value. To verify that the Event Logging is occurring, open the user's `%UserName% AML.ini` file, look in the `SSOSection` column for entries with the name starting with `CacheItem` (for example, `CacheItem1`). These items are the events, cached until the retry time is reached. At the retry time, the cached events will be sent to the extension(s).

The wrong events are recorded

The Filter setting is set improperly. Review the Event Logging Filter, note the precise bit order and conversion from binary to hexadecimal/decimal.

8.1.8.2 Windows Event Viewer

Credentials do not arrive at the server

The server name is not properly set. Do not use leading "\\" characters. Specify the proper NetBIOS name (not the TCP/IP name).

Credentials on the server are missing data; category and event labels are only numbers and the Description is similar to "The description for Event ID (###) in Source (Logon Manager) cannot be found

- The local computer may not have the necessary registry information or message DLL files to display messages from a remote computer. The following information is part of the event:"

- The server is not properly configured. See Section 2.17.11.1, "Configuring the Windows Event Logging Server" extension for instructions on configuring the server.

8.1.9 Credential Sharing Groups

Credential Sharing Groups are not working

Make sure `Extensions\AccessManager:PWSEnable=1`.

A Password Change within an application in the Domain or LDAP groups does not notify the authenticator of the change

Make sure `AUI:ShareToAuth=1`.

8.1.10 All Synchronizer Extensions

Following are solutions to problems experienced when synchronizing to any type of directory.

8.1.10.1 All Directory Extensions User Connections

Cannot connect via SSL

Make sure the directory connection works without SSL.

A user cannot create an object on the directory

- Make sure the user is connecting to the directory.
- Make sure `UserPaths` points to a valid location.
- An `SSOlocator` object for the user does not exist, either specifically for the user or as a default object. Put a default object in the location `UserPaths` points to; if this works, you can move the default object up the tree or put a user-specific object on the tree.

8.1.10.2 Admin Objects

Admin objects (vGOAdminOverride, vGOentlist, vGOftulist) cannot be altered

Existing objects cannot be overwritten. Instead, delete the old objects and then push new ones.

8.1.10.3 File System Server User Connections

A user cannot create an object on the directory

Make sure the user can connect to the File System share directly (for example, in Explorer).

8.1.10.4 OpenLDAP Directory Server Repository

An error message appears when extending the Schema

In the **Connect to Repository** dialog, if OpenLDAP Directory Server is selected as the Repository Type and an Extend Schema Status error appears, the schema will have to be manually extended.

The Error message appears as follows:

```
============== ERROR ==============

Automated schema extension is not supported

by this server. Use the file located at

"C:\Program Files\Passlogix\v-GO SSO Console\

DirectorySchema\vgo\OLDAP\sso.schema"

to extend the schema manually.

Extend Schema ABORTED!
```

If you receive this error, follow these steps to extend the schema manually:

1. Copy the sso.schema file to the OpenLDAP server. The sso.schema file can be located in the following location: C:\Program Files\Passlogix\v-GO SSO Console\DirectorySchema\vgo\OLDAP\sso.schema

2. Place the sso.schema file in the following directory (or other schema directory for OpenLDAP configuration): /usr/local/etc/openldap/schema

3. The OpenLDAP configuration file must be modified to include the new schema file. Open the file, and add the following line: include <path>/sso.schema where <path> is the path specified in the previous step.

> **Note:** On UNIX machines, this file is called slapd.conf.

8.2 Troubleshooting a Universal Authentication Manager Deployment

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

8.2.1 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 Section 5.2.2.5, "Initializing Universal Authentication Manager Storage" to reconfigure Universal Authentication Manager to use the recreated account.

8.2.2 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 O**n 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**.

8.2.3 AutoLogon Condition Is Incorrectly Configured

If the AutoLogon condition is enabled but incorrectly configured, users logging on will see the Microsoft Logon dialog 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 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

8.2.4 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.

8.2.5 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.

8.2.6 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

8.2.7 Windows Password Logon and Unlock

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

8.2.7.1 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 credential provider. 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.

8.2.8 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 logon and unlock flows. Once installed, Universal Authentication Manager conforms to all Microsoft Active Directory security policies.

> **Note:** 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.

8.2.9 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.

8.2.10 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.

8.2.11 Changing User Passwords As the Administrator

If, as an administrator, you change a user's password, and the user then tries to log on 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.

> **Note:** 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.