Oracle® Enterprise Single Sign-on Logon Manager

Best Practices: Configuring the ESSO-LM Agent

Release 11.1.1.5.0

21004-01

March 2011

ORACLE

Oracle Enterprise Single Sign-on Logon Manager Best Practices: Configuring the ESSO-LM Agent

Release 11.1.1.5.0

21004-01

Table of Contents

Introduction

About This Guide

This guide describes best practices for configuring the ESSO-LM Agent via global Agent settings and administrative overrides. It is intended for installation engineers and administrators deploying ESSO-LM in the enterprise. By following the recommendations in this and other *ESSO-LM SSO Best Practices* guides, you will implement an optimal ESSO-LM configuration.

Note: This guide does not cover configuring ESSO-LM for synchronization with specific data repositories, such as Active Directory or a database. These steps are explained in separate *ESSO-LM Best Practices* guides.

Terms and Abbreviations

The following table describes the terms and abbreviations used throughout this guide:

Term or Acronym	Description
ESSO-LM	Oracle Enterprise Single Sign-On Logon Manager
Agent	ESSO-LM Client-Side Agent
Console	ESSO-LM Administrative Console

Accessing ESSO-LM Documentation

We continually strive to keep ESSO-LM documentation accurate and up to date. For the latest version of this and other ESSO-LM documents, visit http://download.oracle.com/docs/cd/E21040_01/index.htm.

Configuring the Agent

Global Agent Settings vs. Administrative Overrides

The behavior of the ESSO-LM Agent, including its interaction with the directory, is governed by settings configured and deployed to the end-user machine by the ESSO-LM administrator using the ESSO-LM 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 ESSO-LM 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).

  Caution: 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 guide describes the recommended optimal configuration and complements the information found in the other *ESSO-LM Best Practices* guides.

A typical view of the ESSO-LM Administrative Console is shown in Figure 1.

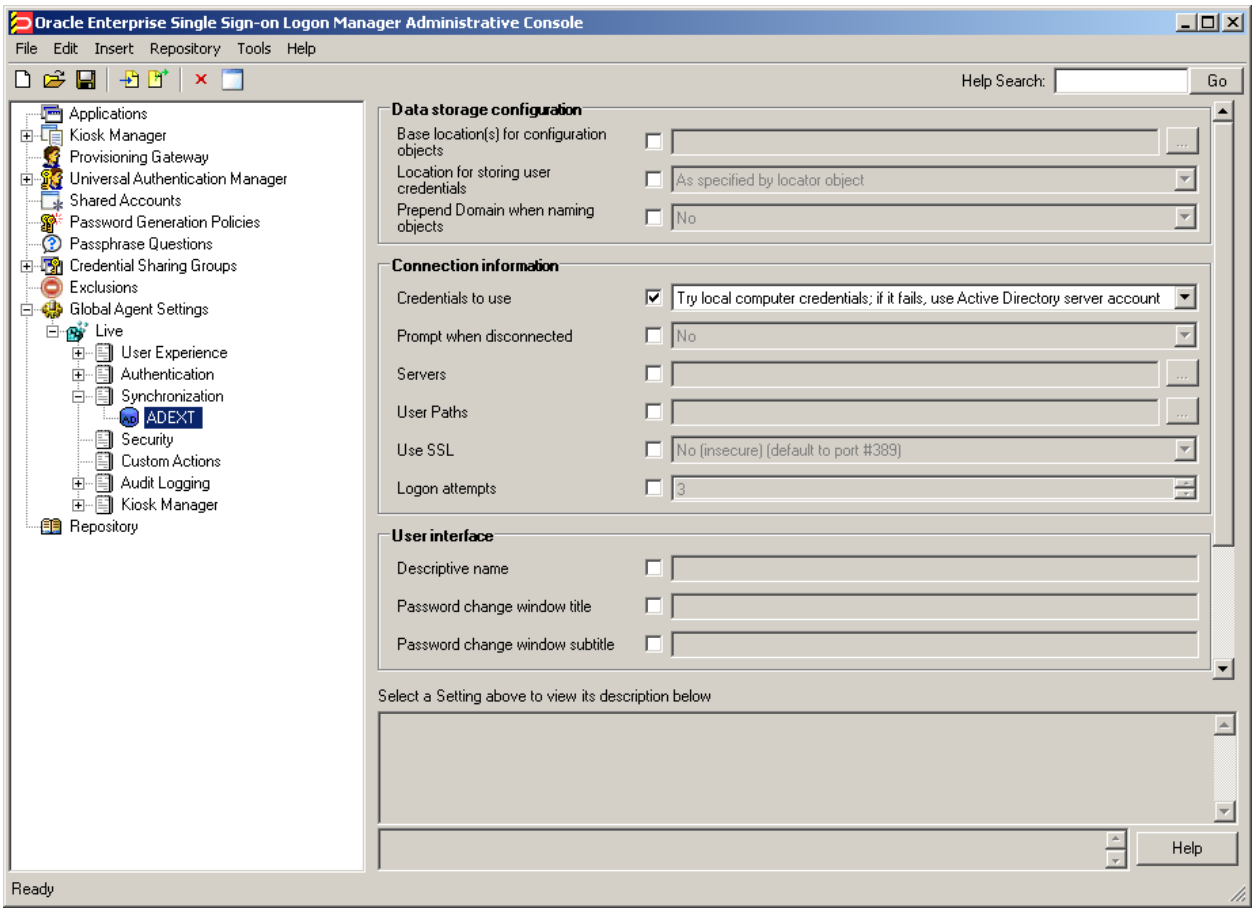


Figure 1 The ESSO-LM Administrative Console

If you need additional information on the settings described in this guide, see the online help included with the Console.

Tip: In a development or staging environment, disable the option **Check for publisher's certificate revocation** in Internet Explorer to eliminate a delay when the Console starts and your machine is not connected to the Internet. (The delay is caused by Internet Explorer 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 *ESSO-LM Best Practices* 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 ESSO-LM Administrative Console is *not* checked. The value is visible in the inactive field next to the check box.

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 ESSO-LM MSI package.

Allow Users to Exclude Logons 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.

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 ESSO-LM 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 Directory. (The override will be in effect after first successful synchronization.)

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 FTU wizard, as described in the next section
- If you want users to authenticate only via the selected primary authenticator.

For information on configuring specific authenticators, see the ESSO-LM Administrative Console help.

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

To set: Select the check box, then select the desired logon method from the drop-down list.

Do Not Show the First-Time Use Wizard

When ESSO-LM starts for the first time, the First-Time Use (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 ESSO-LM using the selected primary logon method
- Provide credentials for default applications.

As a best practice, avoid burdening end-users with setting up ESSO-LM 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 ESSO-LM's first launch is their Windows password.

Located in: Global Agent Settings → Live → User Experience → Setup Wizard

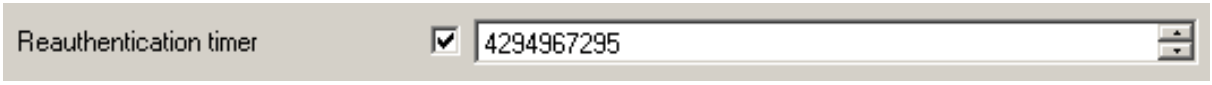
To disable: Select the check box, then select **No** from the drop-down list.

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



To disable: Select the check box, then enter **4,294,967,295** in the field; this value disables the timer.

Use the Default Encryption Algorithm

Do not change the default encryption algorithm (Triple-DES MS CAPI) that ESSO-LM uses to encrypt application credentials to retain compatibility with all supported operating systems. Not all algorithms supported by ESSO-LM 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: We strongly advise 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.

Recommended Administrative Overrides

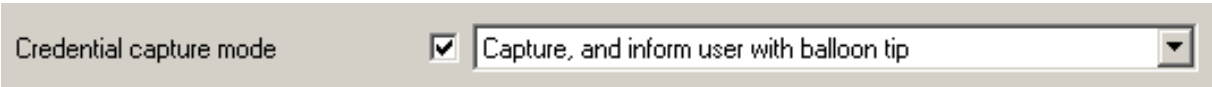
This section lists our recommended best-practice administrative overrides. Configure the overrides as described below and push them to the central repository. The overrides will be applied to end-user machines during the next synchronization event.

Configure Silent Credential Capture

ESSO-LM 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 ESSO-LM 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 ESSO-LM 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.

Make the ESSO-LM 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.

Use Optimized Synchronization

Optimized synchronization instructs the ESSO-LM 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.

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.

Note: This override **must** be applied in tandem with the restriction described in Restrict Disconnected Operation.

Located in: Global Agent Settings → Live → Synchronization

To allow: Select the check box, then select **Yes** from the drop-down list.

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, ESSO-LM may 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 ESSO-LM 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 ESSO-LM's 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 →Response → Web Applications

To set: Select the check box, then enter the desired value in the field.

Limit Users to Predefined Applications

ESSO-LM 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 ESSO-LM. Instruct ESSO-LM 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

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

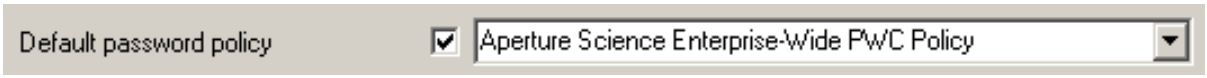
To set: Select the check box, then select **Unlimited** from the drop-down list.

Note: The individual options shown above take precedence over the **All applications** option.

Create and Set the Company Password Change Policy

By default, ESSO-LM 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 the Console help.

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.

Force Reauthentication when Revealing Masked Fields

To prevent unauthorized access to stored application passwords, configure ESSO-LM 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.

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, ESSO-LM 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 the Console help.

Select Event Types to Log

If you are using an audit logging method other than the ESSO 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.

Caution: 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>

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.