Oracle® Enterprise Single Sign-on Logon Manager

Best Practices: Deploying ESSO-LM with Microsoft Active Directory

Release 11.1.1.5.0

E21001-01

March 2011

ORACLE

Oracle Enterprise Single Sign-on Logon Manager Best Practices: Deploying ESSO-LM with Microsoft Active Directory

Release 11.1.1.5.0

E21001-01

Table of Contents

Introduction

About This Guide

This guide describes best practices and recommended procedures for deploying Oracle Enterprise Single Sign-On Manager (ESSO-LM) with Microsoft Active Directory. Readers of this guide should be experienced system administrators and have a solid understanding of Active Directory and related concepts, such as directory schema, structure, and security.

Oracle highly recommends that you read this guide before planning the deployment of ESSO-LM as it will familiarize you with the recommended preparation and deployment steps, as well as advise you how to avoid short- and long-term problems. By following the recommendations in this and other *ESSO-LM Best Practices* guides, you will implement an optimal ESSO-LM configuration.

> **Note:** Best practices described in this guide apply exclusively to plain ESSO-LM deployments on Active Directory. They do not apply to LDAP, Citrix, Terminal Services, kiosk, and Oracle Enterprise Single Sign-On Kiosk Manager (ESSO-KM) environments.

How This Guide Is Organized

For your convenience, this guide is divided into the following parts:

Part 1: Deployment Best Practices – Introduces you to ESSO-LM and describes best practices for planning and performing deployment on Active Directory. Topics include designing the tree for optimal performance vs. accurate template delivery, and best practices for configuring ESSO-LM for synchronization with Active Directory.

Part 2: Deployment Procedures – Contains the required deployment and configuration procedures, such as extending the schema and configuring ESSO-LM for Active Directory synchronization.

Part 3: Appendices – Contains reference material supplementing the earlier sections of the guide, as well as troubleshooting instructions for the most common deployment issues.

Terms and Abbreviations

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

Term or Abbreviation	Description
AD	Active Directory
DC	Domain Controller
OU	Organizational Unit
ESSO-LM	Oracle Enterprise Single Sign-On Logon Manager
ESSO-KM	Oracle Enterprise Single Sign-On Kiosk Manager
Agent	ESSO-LM client-side software
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.

Part 1: Deployment Best Practices

This part describes best practices for deploying ESSO-LM with Microsoft Active Directory. It contains the following sections:

Overview of Oracle ESSO-LM

Oracle Enterprise Single Sign-On Logon Manager (ESSO-LM) is a secure and easily deployable single sign-on solution that acts as a middle layer between the user and the target applications. Users need to authenticate only once; ESSO-LM automatically detects and handles all subsequent requests for user credentials.

ESSO-LM at a Glance

ESSO-LM uses client-side intelligence to respond to requests for user credentials from Windows, Web, and mainframe applications using a wide variety of industry-standard authentication methods and services. Credentials can either be stored locally or in a central repository such as Active Directory, ADAM, AD LDS, LDAP, a file system, or an SQL database. Add-on modules extend the core ESSO-LM functionality with features such as self-service password reset, remote credential provisioning, and the creation of fully-contained, pre-configured packages deployable automatically or by end-users.

ESSO-LM provides out-of-the-box support for authentication methods such as passwords, biometrics, and smart cards, and services such as Windows password, PKI, and LDAP. ESSO-LM does not require any modifications to authentication services, or a custom Windows GINA, to provide the benefits of single sign-on. In addition to technologies supported out of the box, ESSO-LM can be customized through standard APIs to support less-common technologies. Figure 1 gives a brief overview of the ESSO-LM architecture.

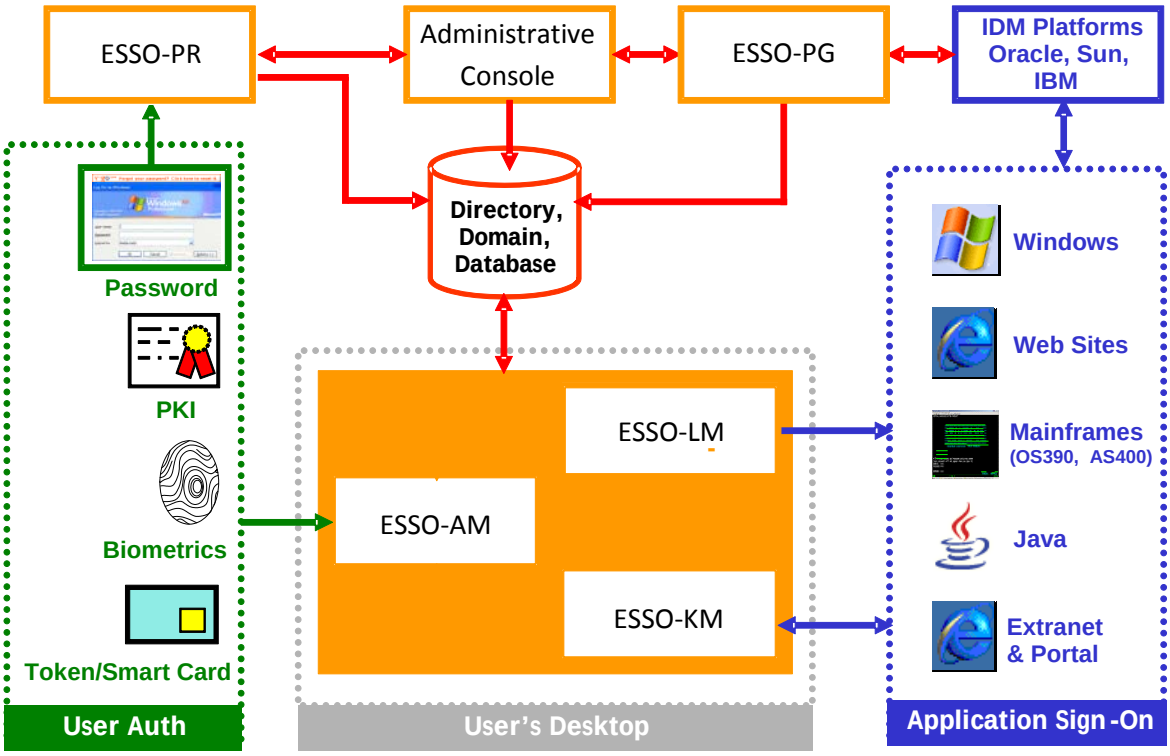


Figure 1 ESSO-LM architecture at a glance

ESSO-LM and Active Directory Environments

You have the choice to deploy ESSO-LM in a directory environment, such as Active Directory, which enables the delivery of single sign-on capability to any machine on the network through central storage of application credentials, templates, and policies. Users synchronize with the directory to download these items and update their credential stores with new or changed usernames and passwords.

Adding ESSO-LM to your existing directory environment provides the following benefits:

- ESSO-LM leverages the existing user accounts, groups, and native directory permissions (ACLs) without the need to manage these items separately or synchronize them with another directory or database.
- ESSO-LM data is automatically protected by your existing backup, failover, and disaster recovery plans.
- No dedicated servers or server-side processes are required; ESSO-LM's scalability and performance depend solely on the capacity and robustness of your existing directory infrastructure.
- Administrators are not burdened with additional administrative tasks or the need to learn new tools or concepts. Delegated administration of ESSO-LM is achieved through the native capabilities of the directory.

A directory also enables the organization of ESSO-LM templates and policies into a highly visual hierarchy. While you can use a flat model if your environment calls for it, a properly set-up hierarchy can help maintain top directory, Agent, and network performance, as well as simplify ESSO-LM administration by permitting more efficient access control.

How ESSO-LM Extends Your Active Directory Schema

Before ESSO-LM can store data in Active Directory, you must instruct ESSO-LM to extend your Active Directory schema. The schema extension consists of adding four object classes and setting the appropriate permissions so that objects of those types can be created, read, modified, and deleted. Existing classes and attributes are **not** modified in any way. If you decide to allow ESSO-LM to store application credentials under user objects (a recommended best practice), ESSO-LM will also apply the permissions required by this feature.

> **Note:** Schema extension is a post-installation procedure. For instructions, see Preparing Active Directory for ESSO-LM. Oracle highly recommends that you perform a schema health check using tools such as Microsoft MOM before performing the schema extension.

For detailed information on the schema extensions made by ESSO-LM, see the following appendices:

- Appendix A: Minimum Administrative Rights for ESSO-LM AD Objects
- Appendix B: ESSO-LM AD Classes and Attributes

How ESSO-LM Synchronizes with Active Directory

The ESSO-LM Agent uses the Active Directory synchronizer plug-in to communicate with Active Directory. When properly configured, synchronization occurs whenever one of the following events takes place:

- The ESSO-LM Agent starts.
- Application credentials are added, modified, or deleted by the end-user.
- The machine running the Agent acquires an IP address or its existing IP address changes. (if ESSO-LM is configured to respond to these events).
- The auto-synchronize interval elapses (if configured).
- The user initiates synchronization via the ESSO-LM Logon Manager's "Refresh" function.

During synchronization, the ESSO-LM Agent traverses the ESSO-LM tree and loads the contents of the sub-containers to which the current user has been granted access; it also synchronizes any credentials that have been added, modified, or deleted since the last synchronization.

How ESSO-LM Handles and Stores Application Credentials

ESSO-LM encrypts application credentials using a unique key generated when the user completes the First-Time Use (FTU) wizard. The credentials remain encrypted at all times, including in the Agent's local cache, the directory, and while in transit over the network. ESSO-LM only decrypts credentials (to memory, never to disk) when a configured application requests logon, and wipes the target memory location as soon as the logon request completes. The amount of data ESSO-LM stores per enabled application and per user is trivial (measurable in bytes and small kilobytes).

> **Note:** ESSO-LM supports SSL encryption for directory connections. While normally not required, SSL support is necessary in certain scenarios. See Configure SSL Support for details.

Further Reading

An in-depth discussion of the ESSO-LM software architecture is beyond the scope of this guide. To obtain Oracle white papers containing additional information, contact your Oracle representative.

Designing the ESSO-LM Directory Sub-Tree

ESSO-LM gives you the freedom to set up the directory structure to best fit the needs of your organization. Specifically, you have the choice to store your data in a flat model, or create a hierarchy. While a flat model works fine for small deployments, growing and large deployments should utilize a hierarchy from the very beginning. The exact structure of your sub-tree will depend on the following factors:

- Number of users
- Number of applications you want ESSO-LM to support
- Robustness of the existing infrastructure
- Structure of your organization

Always follow Microsoft's best practices for Active Directory design and implementation described in the following article: http://technet.microsoft.com/en-us/library/bb727085.aspx

Guidelines for Structuring the Sub-Tree

Oracle recommends that you set up your sub-tree as a hierarchy by following the guidelines below:

- Use OUs to group templates and policies by category, such as department or division, according to the structure of your organization.
- Control access at the OU level.
- Disable inheritance and grant no user rights at the root of the ESSO-LM sub-tree, unless your environment dictates otherwise.

When set up this way, a hierarchy provides the following benefits:

- **Highly visual and self-documenting tree structure.** When you view your sub-tree in a directory browser, the sub-tree structure is self-descriptive and easy to follow.
- **No unwanted inheritance of rights.** Users will not natively inherit rights to sub-OUs you don't want them to access. This eliminates the need to explicitly deny unwanted access rights that are being passed down the tree.
- **Robust network, Agent, and directory performance.** Typically, users who download large numbers of templates and policies generate more network traffic and a higher load on the directory than users who only download items relevant to their jobs. Grouping conserves your environment's resources and improves Agent response time.
- **Distributed administrative tasks.** Your templates are organized into easily controllable sets, and access rights determine who can manage which templates. You also have the ability to implement rights-based version control of your templates.
- **Low administrative overhead.** Controlling access at the template level requires setting permissions for each individual template via the ESSO-LM Administrative Console; controlling access at the OU level is achieved via delegated administration using Microsoft and third-party management tools.

Figure 2 depicts a sample ESSO-LM sub-tree whose design reflects the above best practices.

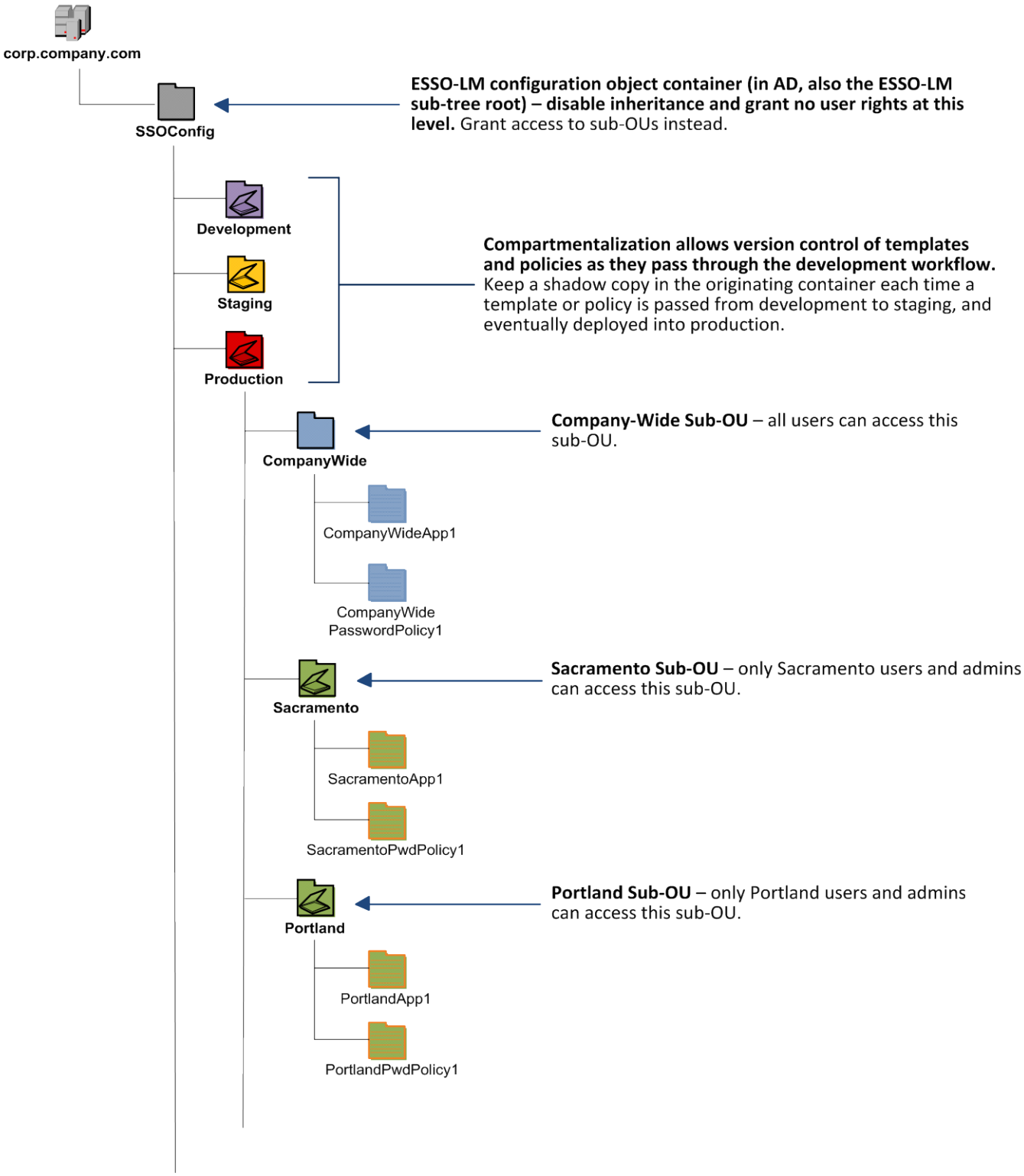


Figure 2 Recommended ESSO-LM sub-tree design

In our sample scenario, users from the Portland division do not need access to applications used by the Sacramento division, and vice versa; therefore, each division's templates and policies live in dedicated sub-OUs under the root and one division cannot access another division's sub-OU. In the end, your environment will dictate the specifics of your implementation.

Note: To permit ESSO-LM to store templates and policies in individual OUs, you must enable the use of configuration objects.

If you are starting out with a flat model, but expect the number of users and provisioned applications to grow, create a sub-container under the root and use it to store your templates and policies as a flat file until you are ready to transition to a hierarchy. Monitor the performance of your environment as you add more users and provision more applications, and transition to a hierarchy sooner rather than later to minimize the required effort.

Version Control and Pre-Flight Testing of Templates and Policies

Oracle recommends that you create dedicated sub-OUs for each stage of your workflow: development, staging, and production, as shown in Figure 2 on page 12. This way you will be able to:

- Track changes made to templates and policies as they pass through the workflow and enter production by keeping shadow copies each time templates and policies move from one workflow stage to the next.
- Roll back to a previous version of a template or policy if need arises.
- Control who can work on which templates and policies at each workflow stage. In particular, you should strictly enforce rules governing who can put a template or a policy into production.

Always test every application template and administrative override in a contained environment before you deploy it to end-users. Testing helps you stage your changes and resolve any potential issues that would be much more costly to resolve were they to occur in production. Testing is particularly critical in large deployments: if you push out a misconfigured template or an incorrect administrative override network-wide, access to mission-critical applications may be lost enterprise-wide.

When setting up a contained test environment, create a dedicated test container to which only members of your development group will have access. Then, point the test ESSO-LM Agent(s) at this container and place your templates and administrative overrides in it. Once you confirm that the templates and policies are functioning as intended, move them to the target production container.

If you decide not to keep shadow copies of your templates after you test them, move them from the test container to target production containers as follows:

1. Pull down the template from the directory.
2. Create a local backup of the template.
3. Push the duplicate into the new location within the directory.
4. Delete the template from its original location.

Precautions for Configuring Object Access Control Lists (ACLs) Using the Console

When you modify an object's Access Control List (ACL) using the Console, the connection string (repository host name or IP) used to connect to the repository is treated by the Console as a unique repository identifier and recorded in the object. The Console is thus unable to distinguish between two unique repositories and two methods to connect to the same repository.

Because of this, if you use different connection strings for the same repository, e.g. an IP address and host name, the changes made to an object from one session to the next will be lost. To work around this issue in an Active Directory environment, use the repository's domain instead of a particular IP address or host name. This will ensure consistency of the connection string by allowing the Console to automatically connect to the nearest DC and changes made to object ACLs will then be retained from one session to the next.

Precautions for Upgrading the Agent and Console

To maintain template and settings compatibility throughout your environment, you should always use a version of the Console matching the oldest version of the Agent still deployed in production. Due to template schema changes between releases, older Agents may exhibit unexpected behavior when supplied with a template created or modified by a newer version of the Console. For this reason, if you are upgrading to a newer release of ESSO-LM, Oracle highly recommends that you do not upgrade your Console until all deployed Agent installations have been upgraded.

Note: Even if you do not make any changes to a template, it is still rewritten using the currently installed Console's data schema when you push the template back to the repository.

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.

Warning: Settings such as domain names and user object paths should always be thoroughly tested before deployment and not deployed as administrative overrides unless absolutely necessary. A simple mistake, such as a mistyped domain name, can render end-user workstations unable to synchronize with the directory, in which case you will not be able to propagate a correction through the Console – changes will have to be made to user machines using other tools.

Figure 3 depicts a typical view of the ESSO-LM Administrative Console set up for synchronization with Active Directory.

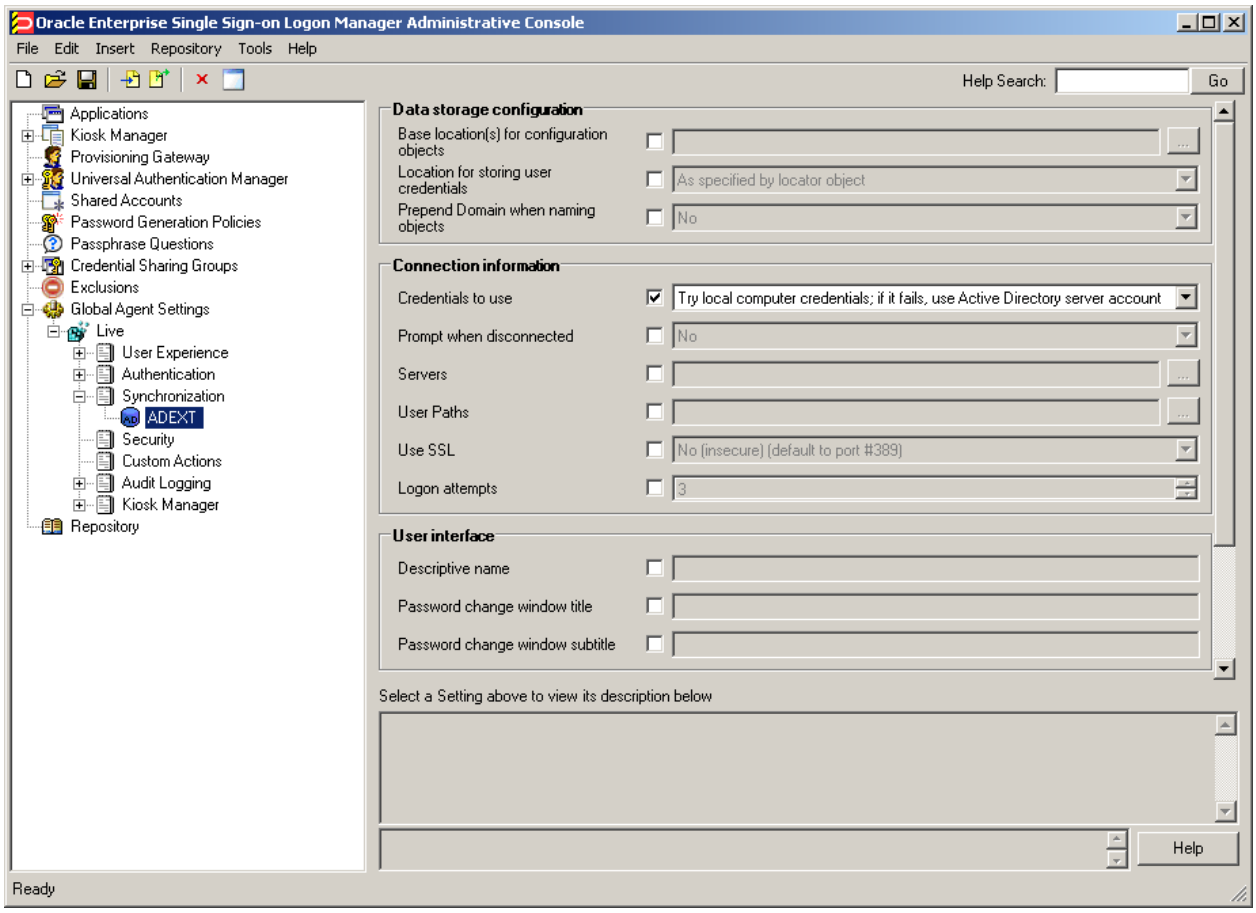


Figure 3 The ESSO-LM Administrative Console

The next section describes best practices for configuring ESSO-LM for synchronization with Active Directory. If you need additional information on settings described in this guide, see the online help included with the Console.

Note: Before you begin, make sure that the ESSO-LM Agent and the Active Directory synchronizer plug-in are installed on your machine; otherwise, AD settings will not be displayed in the Console. For installation instructions, see the *Installation and Setup* guide for your version of ESSO-LM.

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.

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. (For instructions on creating the package, see the guide *Best Practices: Configuring ESSO-LM for Mass Deployment*.)

Data Storage Settings

Oracle recommends configuring ESSO-LM's data storage settings as described below.

Use Configuration Objects

On Active Directory deployments, ESSO-LM supports the use of directory objects for storing user and configuration data, allowing hierarchical storage, as well as role/group-based access control for individual containers, templates, and policies as described in Designing the ESSO-LM Directory Sub-Tree. If you disable this feature, ESSO-LM will store all template and configuration data as a single flat file under the tree root.

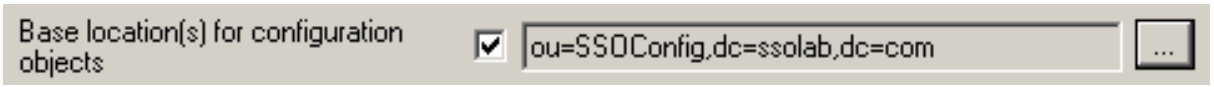
Located in: Global Agent Settings → Live → Synchronization

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

Specify the Path to the ESSO-LM Configuration Objects

You must specify the location of the ESSO-LM root container (which stores ESSO-LM configuration objects) for ESSO-LM to store data in Active Directory.

Located in: Global Agent Settings → Live → Synchronization → ADEXT



To set: Select the check box, click the (**…**) button, and enter the desired value.
When you are finished, click **OK**.

Store User Credentials Under Respective User Objects

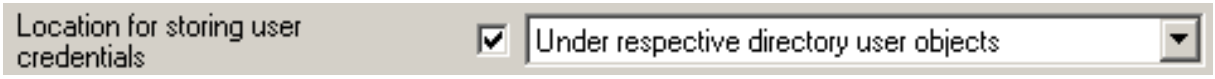
A major benefit of using ESSO-LM with Active Directory is the ability to store user credentials under the respective user objects. Doing so simplifies administration as follows:

- Locating and viewing the credentials of individual users is quick and intuitive.
- Deleting a user from the directory automatically removes the user's application credential cache from under the respective user object.

Note: This option will not work until you perform the necessary schema modification and permission assignment. For instructions, see Preparing Active Directory for ESSO-LM.

Note: When user credentials are stored under respective user objects and use of credential objects is enabled, you do not need to use the Locator object. (The Locator is a pointer object that tells ESSO-LM where in the directory to look for templates, credentials, and other objects when using a flat directory model; for more information, see Appendix B: ESSO-LM AD Classes and Attributes.)

Located in: Global Agent Settings → Live → Synchronization → ADEXT



To enable: Select the check box, then select **Under respective directory user objects** from the drop-down list.

Repository Connection Settings

Oracle recommends configuring ESSO-LM's repository connection settings as described below.

Let ESSO-LM Find the Nearest Domain Controller

Oracle recommends that you let ESSO-LM locate and synchronize with the closest domain controller on the network, unless your environment calls for providing a specific value in this field. For example, if end-user machines are not on the same domain as the directory, you will need to provide the correct domain name. If you hardcode a complete URL in this field, you will lose fault tolerance (fallback) in the event the DC in question goes offline.

Located in: Global Agent Settings → Live → Synchronization → ADEXT

To let ESSO-LM find the nearest DC: deselect the check box (default setting).

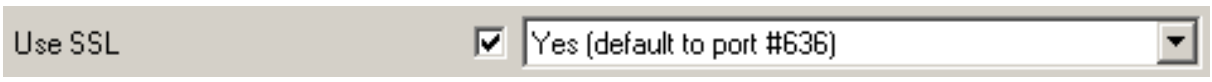
To set: Select the check box, click the (**…**) button, enter the desired values (one per line) and click **OK**.

Configure SSL Support

By default, the ESSO-LM AD synchronizer ships with SSL support disabled. To save time during deployment, it is normally safe to leave SSL support disabled in ESSO-LM if your network is not already set up for it. If, on the other hand, your network has been configured for SSL, or you are planning to add SSL support to your network before deploying ESSO-LM, enable SSL support in ESSO-LM as shown below.

Note: When ESSO-KM is in use, ESSO-LM performs direct clear text LDAP authentication to the directory. In such a scenario, Oracle highly recommends that you enable SSL to encrypt the authentication information. Note that you must configure your domain controllers to use SSL before enabling SSL support in ESSO-LM. For instructions, see the following MSDN article: http://msdn.microsoft.com/en-us/library/aa364671(VS.85).aspx

Located in: Global Agent Settings → Live → Synchronization → ADEXT



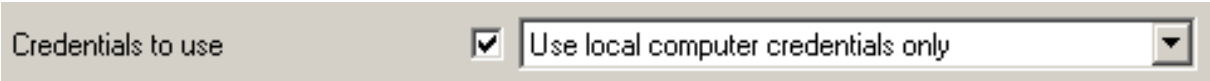
To enable: Select the check box, then select **Yes (default to port #636)** from the drop-down list.

Select the Credentials to Use when Authenticating to the Directory

Use the **Credentials to use** option to select the credentials that ESSO-LM should use when authenticating to the directory. Oracle recommends that you set this to **Use local computer credentials only** so that the user will not be prompted to reauthenticate if ESSO-LM is unable to authenticate to the directory.

> **Note:** Do **not** leave this at the default setting, **Try local computer credentials; if it fails, use Active Directory server account**. Doing so will cause an authentication failure (and the re-authentication prompt to appear, unless disabled) if the directory and the end-user machine are not part of the same domain.

Located in: Global Agent Settings → Live → Synchronization → ADEXT



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

Decide Whether to Prompt the User when Disconnected from the Directory

Use the **Prompt when disconnected** option to decide whether ESSO-LM should prompt the user to re-authenticate to the directory upon authentication failure or disconnection. Oracle recommends that you leave this setting at its default value of **No** to avoid unnecessary user confusion and resulting helpdesk calls.

Located in: Global Agent Settings → Live → Synchronization → ADEXT

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

This option is directly related to the **Credentials to use** option described earlier and has no effect if **Allow disconnected operation** is set to **No**.

Let ESSO-LM Search for User Accounts

Oracle recommends that you let ESSO-LM automatically search for user accounts in Active Directory, unless your environment calls for providing a specific value in this field. If you hardcode a path incorrectly or the path changes, you will need to update each end-user machine using tools other than the Console.

Warning: In production environments, this field must always be left blank to ensure fault tolerance.

Tip: If you have only one domain, or a primary domain to which most of your users belong, specifying the domain name will save end-users the trouble of entering the domain name when authenticating to ESSO-LM with their Windows password.

Located in: Global Agent Settings → Live → Synchronization → ADEXT

To let ESSO-LM search for user accounts: deselect the check box (default setting).

To set: Select the check box, click the (**…**) button, enter the desired values (one per line), and click **OK**.

Add the Active Directory Synchronizer to the Synchronizer Order List

Ensure that the Active Directory (ADEXT) synchronizer plug-in is present and enabled in the **Synchronizer order** list if at least one of the following is true for your environment:

- ESSO-LM is synchronizing with more than one repository.
- ESSO-LM is using roaming synchronization.
- ESSO-KM is installed in your environment.

Note: Instructions for configuring ESSO-LM for multi-repository and roaming synchronization, as well as installing and configuring ESSO-LM, are beyond the scope of this guide. For more information, see the documentation for your version of ESSO-LM and/or ESSO-KM.

Located in: Global Agent Settings → Live → Synchronization

To set: Select the check box, then click the (**…**) button. In the list that appears, select the check box next to **ADEXT** and click **OK**. Use the up/down arrows to set synchronization order as necessary.

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. 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

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

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 large numbers of credentials per user.
- Disable this option to improve synchronization performance on deployments with fewer than five credentials per user and large number of templates downloaded per user.

Located in: Global Agent Settings → Live → Synchronization

Use the default value (**Yes**) unless your environment requires otherwise.

Restrict Disconnected Operation

During deployment, configure the ESSO-LM Agent not to run if a connection to the directory cannot be established. This will prevent users from completing the First-Time Use (FTU) wizard when the Agent is not connected to the directory and no local cache is present. By not allowing the Agent to run when the directory is not available, you avoid a common situation in which a second set of encryption keys is created when a user completes the FTU wizard while disconnected from the directory.

Note: See the guide *ESSO-LM Best Practices: Configuring the ESSO-LM Agent* for more information on this required best practice.

Located in: Global Agent Settings → Live → Synchronization

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

Recommended Administrative Overrides

Directory synchronization settings, such as domain names and object paths, should not be deployed as administrative overrides. (See Global Agent Settings vs. Administrative Overrides for an explanation.) The recommended best-practice overrides are described in the guide *ESSO-LM Best Practices: Configuring the ESSO-LM Agent*.

Part 2: Deployment Procedures

This part describes the most important procedures for deploying ESSO-LM with Microsoft Active Directory. It contains the following sections:

Overview of the Deployment Process

This section provides a brief high-level overview of the ESSO-LM deployment process on MS Active Directory. Make sure you have read all of the preceding sections of this document before proceeding with deployment. Deploying ESSO-LM with MS Active Directory requires you to:

1. Obtain the following documents:
    - The latest version of this document
    - *ESSO-LM Best Practices: Configuring the ESSO-LM Agent*
    - *ESSO-LM Best Practices: Packaging ESSO-LM for Mass Deployment*
    - *Installation and Setup* guide for your version of ESSO-LM
2. Install the ESSO-LM Agent and the ESSO-LM Administrative Console on a machine within your domain, as described in the installation guide for your version of ESSO-LM. Make sure you select the Active Directory Synchronizer plug-in when installing the Agent.
3. Complete the steps in Preparing Active Directory for ESSO-LM:
    a. Extend the Active Directory schema with ESSO-LM classes and attributes.
    b. Enable storage of user credentials under user objects.
    c. Create the desired tree structure and grant the required permissions.
4. Configure ESSO-LM as follows:
    a. Complete the steps in Configuring the Active Directory Synchronizer.
    b. Configure the options described in Recommended Global Agent Settings in this guide.
    c. Test your configuration as described in Testing the ESSO-LM Configuration.
    d. Configure the options described in the guide *ESSO-LM Best Practices: Configuring the ESSO-LM Agent*.

    Note: For detailed descriptions of the settings in question, see the Console's online help. The online help is available via the Console's **Help** menu.

5. On a test machine, do the following:
    - Create a pilot set of core templates and policies.
    - Finalize the end-user experience by testing each core template, global Agent setting, and administrative override that will be deployed into production.
6. Create a custom MSI package and deploy it to end-user machines by completing the steps in the guide *Best Practices: Packaging ESSO-LM for Mass Deployment*.
7. Create, test, and deploy the remaining application templates. See the *ESSO-LM Best Practices* guides *Template Configuration and Diagnostics* for the target application type (Windows, Web, or mainframe) for in-depth information on provisioning different types of applications.

Preparing Active Directory for ESSO-LM

This section describes the basic procedures for preparing Active Directory for use with ESSO-LM. The preparation consists of extending your Active Directory schema with ESSO-LM classes and attributes, allowing ESSO-LM to store credentials under respective user objects, and creating the desired tree structure. Before starting this procedure, make sure you have done the following:

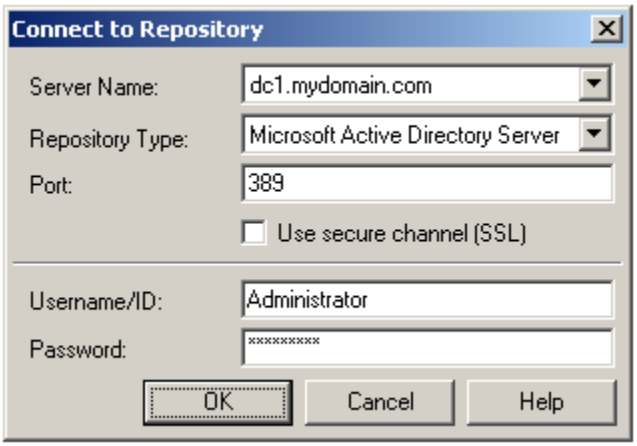
1. Performed a health check on your Active Directory schema. Instructions are provided in the following article: http://www.microsoft.com/technet/opsmgr/2005/library/dirmgmtpack/dirmgmtpackmom_3.mspx
2. Installed the ESSO-LM Administrative Console, as described in the *ESSO-LM Installation and* Setup guide for your version of ESSO-LM.

Step 1: Extending the Schema

1. Start the ESSO-LM Administrative Console. By default, the shortcut to the console is located in **Start → Programs → Oracle → ESSO-LM → ESSO-LM Console**.

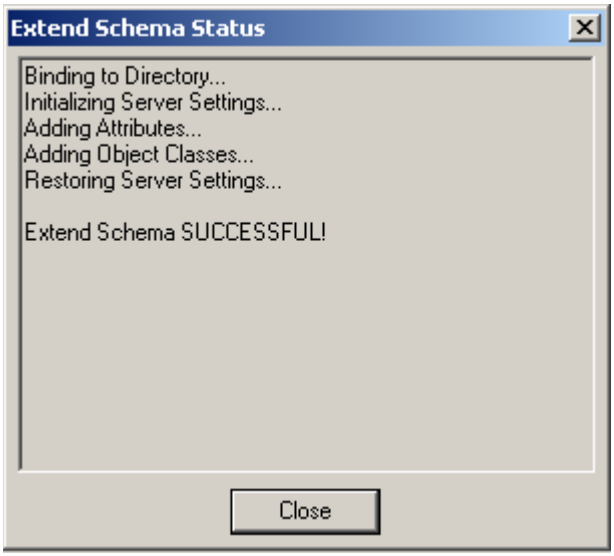
> **Note:** In a development or staging environment, disable the option **Check for publisher's certificate revocation** in Internet Explorer to eliminate a delay when the Console starts and your machine is not connected to the Internet. (The delay is caused by Internet Explorer attempting to look up the server's certificate and timing out when a certificate authority cannot be reached.) Do not disable this option on production machines.

2. In the Console, select **Extend Schema** from the **Repository** menu. The Console displays the "Connect to Repository" dialog.



3. In the **Server Name** field, enter a fully qualified IP address, hostname, or NetBIOS name of your schema master domain controller.
4. In the **Repository Type** drop-down list, select **Microsoft Active Directory Server**.
5. Enter the port number on which your directory is listening for connections. The default ports are 636 for SSL connections and 389 for non-SSL connections.

6. (Optional) If you configured your domain controllers to use SSL, leave the **Use secure channel (SSL)** option enabled; otherwise, disable it. (See Configure SSL Support for more information.)
7. In the **Username/ID** and **Password** fields, enter the credentials of the account you want ESSO-LM to use to connect to Active Directory. Depending on your environment, you may need to include the corresponding domain name as part of the user name, e.g., `ITSLIFE\Jim`.
8. Click **OK** and wait for the Console to perform the schema extension. The Console displays a status dialog showing the progress. When the schema has been successfully extended, a confirmation message appears in the status dialog:



   If the schema extension fails, see Active Directory Schema Extension Failures in Appendix C for troubleshooting steps.
9. Click **Close**.

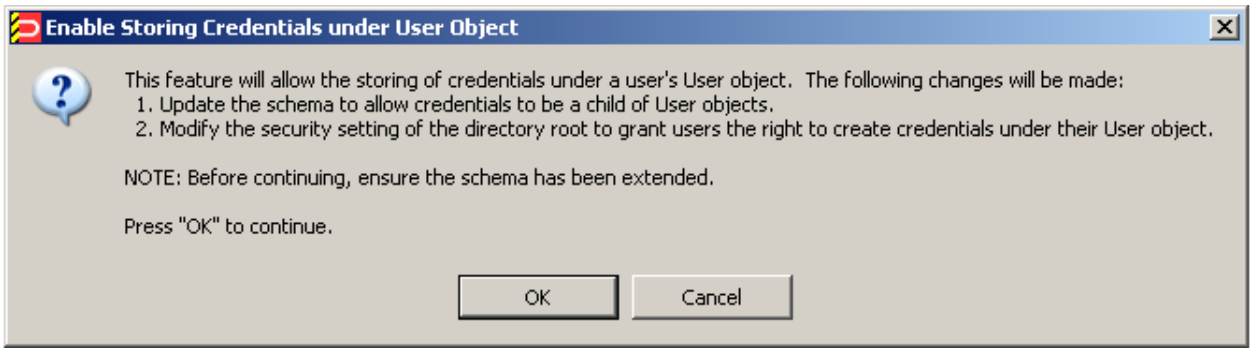
Step 2: Enabling the Storage of User Credentials Under User Objects

When you enable the storage of user credentials under respective user objects, ESSO-LM makes the following changes in the directory:

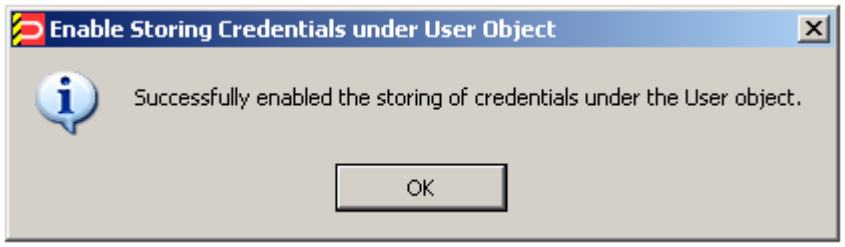
- Adds the `user` class as a possible superior to the `vGOUserData` class.
- Grants all users the right to create `vGOUserData` objects. These rights are granted at the directory root and are recursively inherited down to the user objects.

To enable the storage of user credentials under respective user objects:

1. In the Console, select **Enable Storing Credentials Under User Object (AD Only)** from the **Repository** menu. The Console displays a confirmation dialog informing you of the changes about to be made to your Active Directory schema.

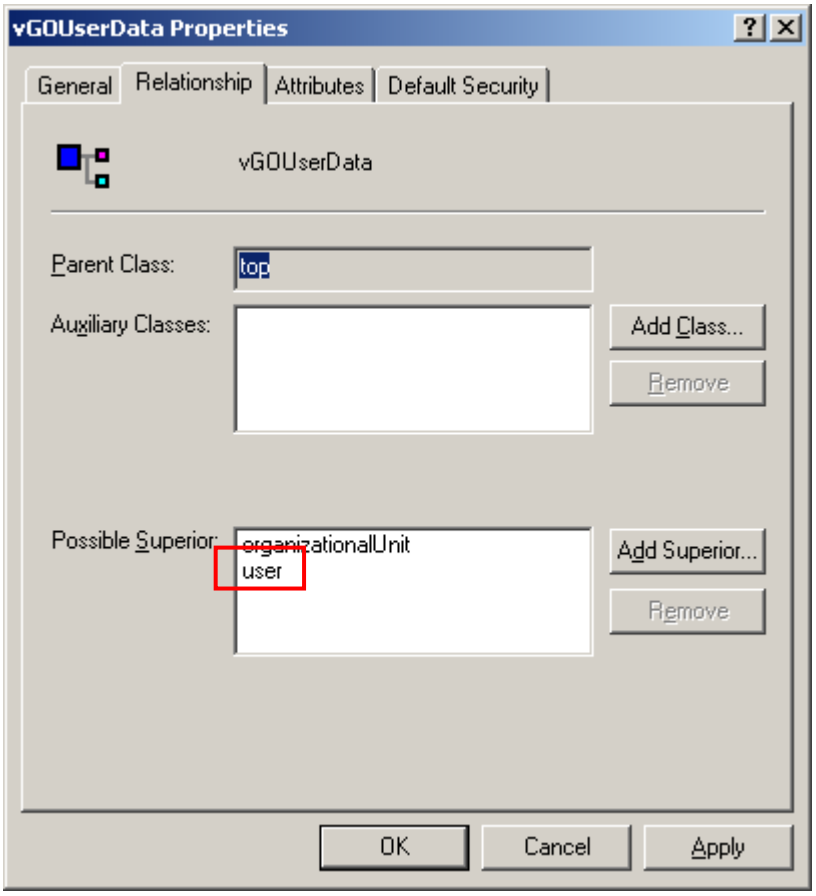


2. Click **OK** and wait for the Console to make the changes. When the changes have been made, the Console displays a confirmation dialog:



3. Verify that the changes have been made successfully:
   a. Open the “Active Directory Schema” snap-in in the Microsoft Management Console. If the snap-in is not present in the console, install it by following the instructions at: http://technet2.microsoft.com/windowsserver/en/library/8c76ff67-9e9d-4fc7-bfac-ffedee8a04d41033.mspx?mfr=true
   b. Expand the **Classes** node and navigate to the **`vGOUserData`** class.
   c. Right-click the **`vGOUserData`** class and select **Properties** from the context menu.
   d. In the “vGOUserData Properties” dialog, select the **Relationship** tab.

e. Check whether the `user` class appears in the **Possible Superior** field:



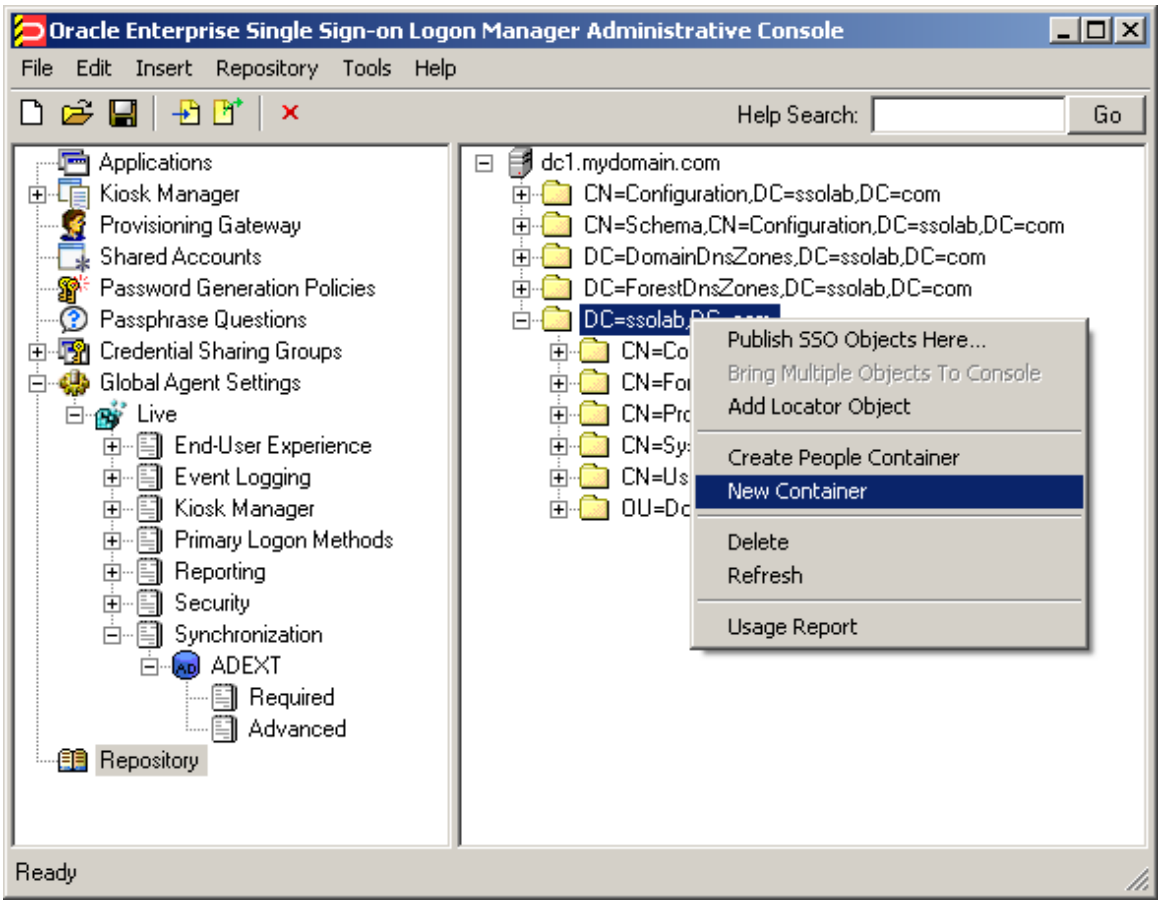
If the user class does not appear as a possible superior, see All Users Unable to Store Credentials under User Objects in Appendix C for possible causes and remedial steps.

Note: Members of protected groups (i.e., users whose ACLs are governed by the `AdminSDHolder` object) will not be able to store credentials under their user objects until the `AdminSDHolder` ACL is updated with permissions required by this feature. See Select Users Unable to Store Credentials under User Objects in Appendix C for instructions on how to remedy this issue.

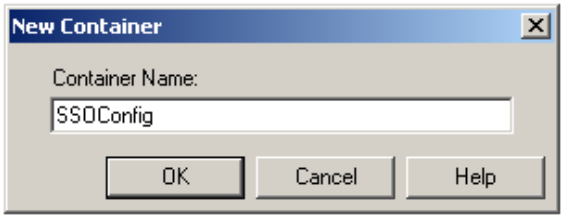
Step 3: Creating the ESSO-LM Configuration Object Container and Sub-Tree Structure

Note: While it is possible to use an existing container for storing ESSO-LM objects, doing so may impair directory performance. Oracle highly recommends that you create a dedicated configuration object container.

1. In the ESSO-LM Administrative Console, select the **Repository** node in the tree in the left pane.
2. Click the **Click here to connect** link in the right-hand pane. The Console displays the "Connect to Repository" dialog.
3. Fill in the fields as explained in steps 3–7 on pages 26-27 and click **OK** to connect.
4. In the tree, right-click the desired parent container and select **New Container** from the context menu, as shown below:



The Console displays the "New Container" dialog:



5. In the “New Container” dialog, enter the desired name and click **OK**.

> **Note:** Unless your environment calls for a specific name for this container, Oracle recommends that you use the default name, `SSOConfig`.

6. Repeat steps 4 and 5 to create any additional containers you may need.

Configuring the Active Directory Synchronizer

After you have prepared Active Directory for ESSO-LM, you must configure the Active Directory synchronizer for your environment. Configure these settings on your “template” client machine and include them in the MSI package you will use to deploy ESSO-LM to end-users. Before starting this procedure, make sure that the ESSO-LM Administrative Console and the ESSO-LM Agent (including the Active Directory synchronizer plug-in) are installed.

> **Note:** Do not include application templates in the MSI package as they will not function in a directory-synchronized environment. The ability to include templates directly in the MSI package is for specialized use only. Instead, push them to the directory for automatic retrieval by the ESSO-LM Agent.

1. Launch the ESSO-LM Administrative Console.
2. In the left-hand pane, right click the **Global Agent Settings** node, then select **Import → From Live HKLM** from the context menu. The Console imports the current Agent settings from the Windows registry.
3. Configure the Agent as described in Recommended Global Agent Settings and Recommended Administrative Overrides.

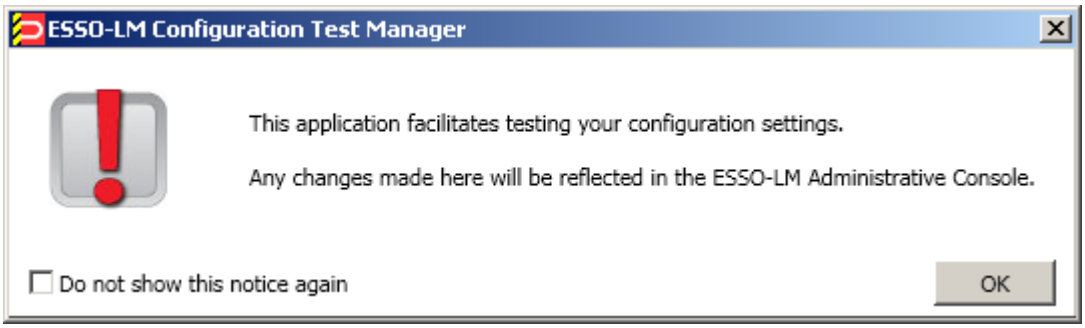
> **Note:** When the check box next to a setting is unchecked, the default value for the setting (shown grayed-out to the right of the check box) is in effect.

4. Save your configuration to an XML file for future reference. From the **File** menu, select **Save**, enter the desired file name, and click **Save**. If you change your settings, you can load this XML file into the Console to revert back to your original choices.
5. From the **Tools** menu, select **Write Global Agent Settings to HKLM**. The Console writes your changes to the registry and restarts the Agent.
6. Continue to the next section to complete the configuration of ESSO-LM.

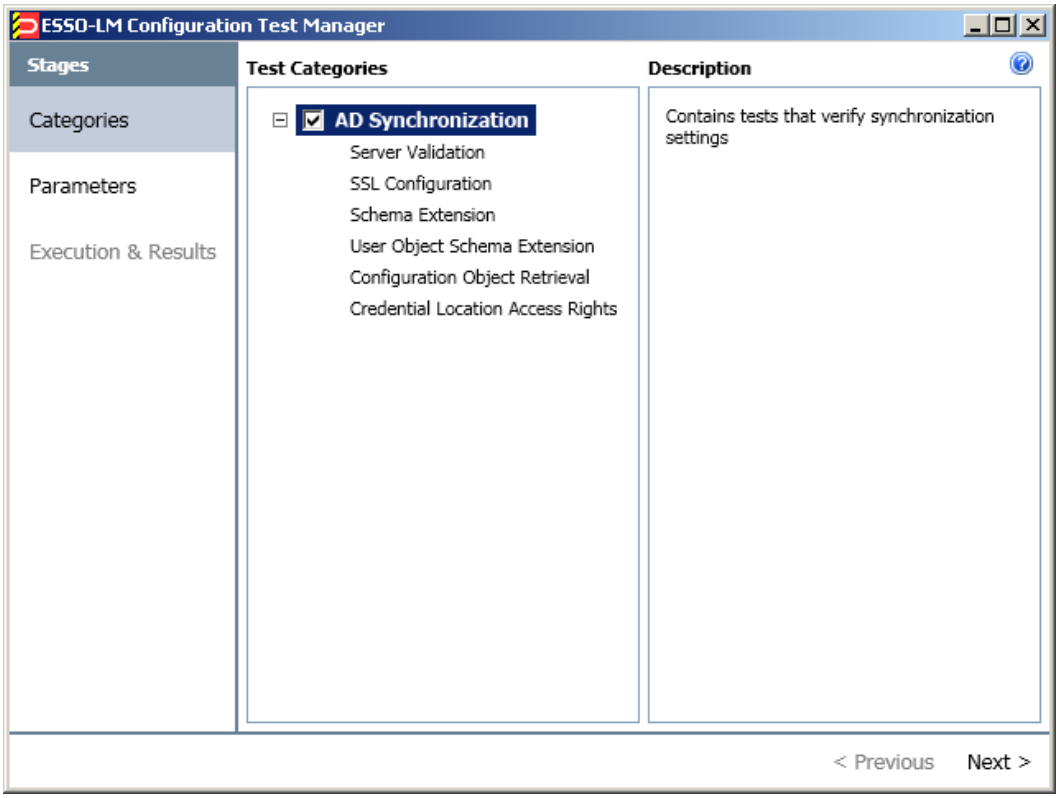
Testing the ESSO-LM Configuration

Once you have finished configuring your ESSO-LM configuration, complete the following steps to test it and correct any errors that might prevent ESSO-LM from functioning:

1. Launch the ESSO-LM Administrative Console.
2. In the left-hand pane, right click the **Global Agent Settings** node, then select **Import → From Live HKLM** from the context menu. The Console imports the current Agent settings from the Windows registry.
3. From the **Tools** menu, select **Test Global Agent Settings**.
4. Read the warning that appears and click **OK** to proceed:



5. The "ESSO-LM Configuration Test Manager" window appears. Follow the instructions in the window to test your configuration and correct any errors. For more information on each option, select the **Help** (question mark) button in the upper right corner of the window.



Next Steps

Read the guides *Best Practices: Configuring the ESSO-LM Agent* and *Best Practices: Packaging ESSO-LM for Mass Deployment* to complete the configuration of ESSO-LM and deploy it to end-user machines.

Part 3: Appendices

This part provides material supplementing the information included earlier in this guide.
It contains the following appendices:

- Appendix A: Minimum Administrative Rights for ESSO-LM AD Objects
- Appendix B: ESSO-LM AD Classes and Attributes
- Appendix C: Troubleshooting ESSO-LM on Active Directory

Appendix A: Minimum Administrative Rights for ESSO-LM AD Objects

This appendix lists the minimum administrative rights that must be granted to specific ESSO-LM objects for ESSO-LM to function.

Note: Information in this appendix is provided for your reference. By default, ESSO-LM automatically sets the appropriate rights when you extend your Active Directory schema. If necessary, these rights can be manually granted and modified directly in Active Directory using the Microsoft Management Console.

Minimum Administrative Rights Required by ESSO-LM Containers

You must grant the following administrative rights to each container in which you want ESSO-LM to store templates, policies, and other configuration items:

- List Contents
- Read All Properties
- Write All Properties
- Delete
- Read Permissions
- Modify Permissions
- Modify Owner
- Create `vGOConfig` Objects
- Delete `vGOConfig` Objects
- Create Organizational Unit Objects
- Delete Organizational Unit Objects

Minimum Administrative Rights Required for Credential Auditing

You must grant the following administrative rights to `vGOUserData` and `vGOSecret` objects to audit user credentials:

For `vGOUserData` objects:

- List Contents
- Read All Properties

For `vGOSecret` objects:

- List Contents
- Read All Properties

Minimum Administrative Rights Required for Credential Deletion

You must grant the following administrative rights to `vGOUserData` and `vGOSecret` objects in order to delete user credentials:

> **Note:** Users able to delete credentials are automatically able to audit them.

For `vGOUserData` objects:

- List Contents
- Read All Properties
- Delete
- Delete Subtree
- Delete All Child Objects

For `vGOSecret` objects:

- List Contents
- Read All Properties
- Delete
- Delete Subtree
- Delete All Child Objects

Appendix B: ESSO-LM AD Classes and Attributes

This appendix describes the directory classes, attributes, and access rights that ESSO-LM adds to your directory during schema extension.

vGOUserData

`vGOUserData` objects are containers that store application credentials. (Credentials are stored as objects of type `vGOSecret`.)

Attributes:

Attribute Name	Syntax	Flag
`vGOSecretData`	Case Ignore String	Singled Valued, Synchronize
`vGORoleDN`	Not Used	
Other optional attributes	ou, dn, cn, o	

Access rights: Users can read and write the above attributes under their own user objects. The administrator has full rights but will not be able to read the encrypted children (`vGOSecret`) of this object.

vGOSecret

`vGOSecret` objects store all user secrets, including an object that stores each user's application credentials and deleted objects. This is added to the `vGOUserData` object as an auxiliary class.

Attributes:

Attribute Name	Syntax	Flag
`vGOsecretData`	Case Ignore String	Singled Valued, Synchronize
`vGOSharedSecretDN`	Not Used	
Other optional attributes	ou, dn, cn, o	

Access rights: As inherited from the `vGOUserData` object, plus: all users can read this object; only the owner can write to this object; and only the owner or an administrator can delete this object.

vGOConfig

vGOConfig objects are containers that store ESSO-LM configuration objects such as application templates, password generation policies, and administrative overrides.

Attributes:

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	

Access rights: All users have read-only rights to the attributes within this object.
The administrator has full rights.

vGOLocatorClass

vGOLocatorClass is a pointer object class. Objects of this class point the ESSO-LM Agent to the location in which user credentials should be stored.

Attributes:

Attribute Name	Syntax	Flag
vGOLocatorAttribute	Case Ignore String	Single Valued
Other optional attributes	dn, cn, o	

Access rights: All users have read, compare, and search rights to these attributes for all objects of this class; the administrator has all rights.

Appendix C: Troubleshooting ESSO-LM on Active Directory

This appendix contains descriptions of issues that may arise during deployment of ESSO-LM, and instructions for remedying those issues.

Active Directory Schema Extension Failures

If the AD schema extension fails, follow the steps below to identify and remedy the possible cause:

1. Check the following, then retry extending the schema:
   - The machine from which you are performing the extension is on the same domain as the directory.
   - You are performing the extension against the schema master DC.
   - You are logged on as the schema administrator.
2. If schema extension still fails, install the ESSO-LM Administrative Console directly on your schema master DC and perform the schema extension locally. This solution rules out all possible network issues (such as DNS problems) and does not fail unless your AD schema contains errors.
3. If you are still unable to extend your schema, the schema might be damaged.
   Check the health of your schema using Microsoft's MOM tool and make sure your schema adheres to Microsoft's best practices described in the following MS TechNet article:
   http://technet.microsoft.com/en-us/library/bb727085.aspx

All Users Unable to Store Credentials Under User Objects

When you enable the storage of credentials under user objects, ESSO-LM grants all users rights to create objects of type `vGOUserData` and `vGOSecret`. These rights are granted at the directory root and are inherited all the way through to the respective user objects. When these rights are not granted or inherited properly, users are unable to store application credentials under their respective user objects. Possible points of failure include:

- The necessary rights have not been granted. You must instruct ESSO-LM to set the necessary rights by selecting **Enable storage of credentials under the user object (AD only)** from the **Repository** menu in the ESSO-LM Administrative Console.
- The rights were granted at the parent domain instead of the user-specific child domain and have not propagated to the child domain. In such case, you can use the Console running on the parent domain DC to grant the necessary rights automatically, or manually grant the rights at the root of each child domain and wait for them to propagate to the user objects.

Note: If the issue affects only certain groups of users, specifically members of Administrators, Power Users, and other protected groups, see Select Users Unable to Store Credentials under User Objects.

Select Users Unable to Store Credentials Under User Objects

The rights necessary to store credentials under user objects are granted at the tree root and inherited down to user objects. When only select users (specifically, members of protected user groups such as Administrators), are unable to store credentials under user objects, the most likely cause is blocked rights inheritance caused by the `AdminSDHolder` object. The object's ACL, which governs the ACLs of all protected groups, prohibits rights inheritance by default. More information about this issue is available in the following MS Knowledge Base article: http://support.microsoft.com/kb/817433.

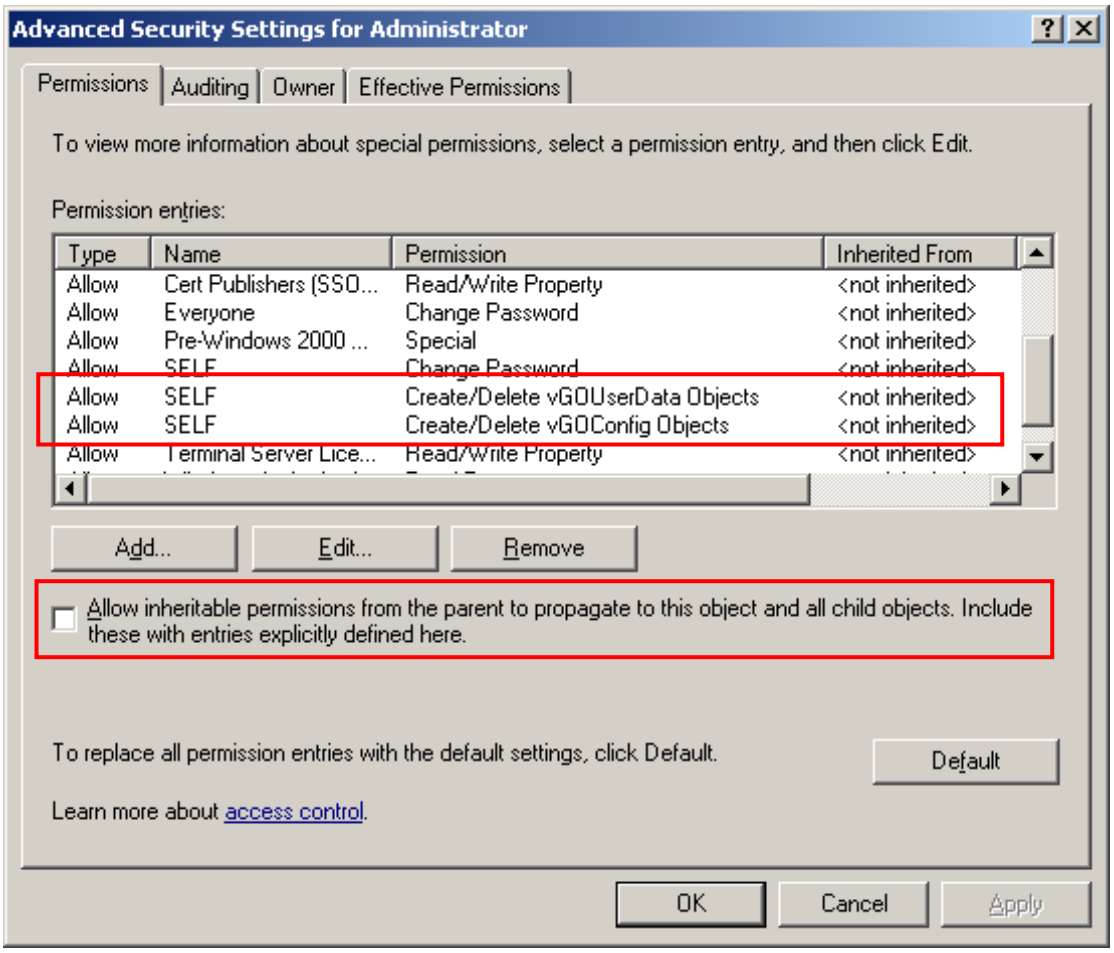
The following protected user groups are known to be affected by this problem:

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

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

1. Log in to the primary DC 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:
   a. The **Allow inheritable permissions…** check box is not selected.
   b. 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.

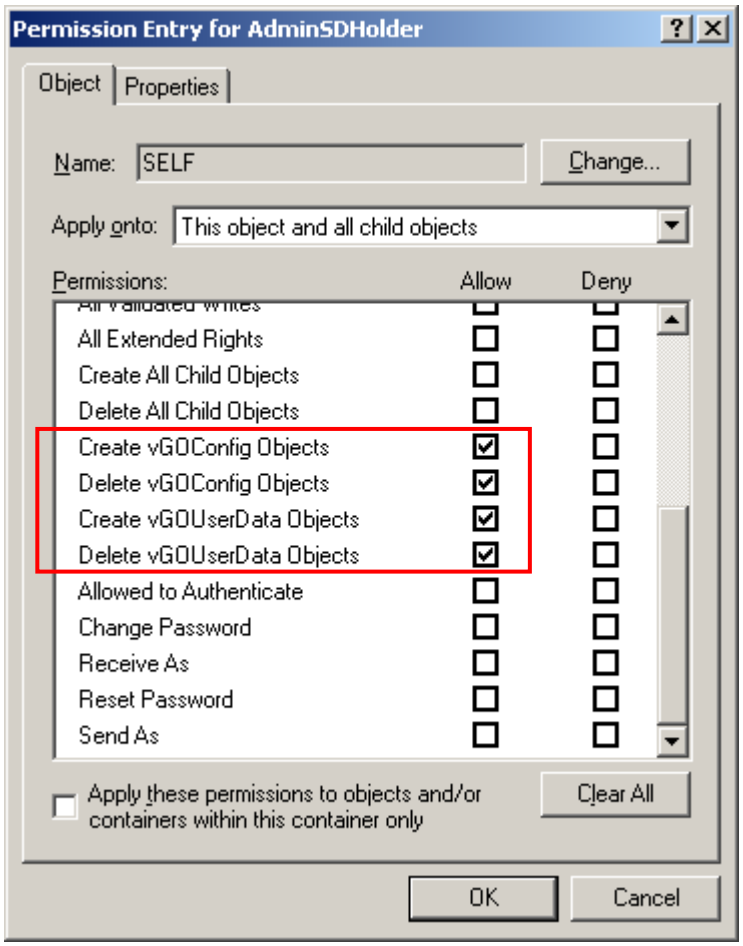
To rectify this issue, you must manually modify the ACL of the `AdminSDHolder` object to grant the right to create objects of type `vGOConfig` and `vGOUserData`. The steps are as follows:

1. Log in to the primary DC as a domain administrator.
2. In the Microsoft Management Console, open the **Active Directory Users and Computers** snap-in.
3. From the **View** menu, select **Advanced Features**.
4. Navigate to the `AdminSDHolder` container located in:
   `cn=AdminSDHolder,cn=System,dc=<domainName>,dc=<domainSuffix>`
5. Right-click the `AdminSDHolder` container and select **Properties**.
6. In the “Properties” dialog, select the **Security** tab and click **Advanced**.
7. In the “Advanced Security Settings” dialog, click **Add…** .

8. In the “Select User, Computer, or Group” dialog, enter **SELF** and click **OK**.
9. In the “Permission Entry” dialog, do the following:
   a. In 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 onto:** drop-down list instead. This variation occurs between different versions and patches of Active Directory and the underlying operating system.

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



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

> **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.