**Oracle® Enterprise Single Sign-on Logon Manager**

Best Practices: Deploying ESSO-LM with Microsoft ADAM/AD LDS

Release 11.1.1.5.0

**E21002-01**

March 2011

ORACLE

Oracle Enterprise Single Sign-on Logon Manager Best Practices: Deploying ESSO-LM with Microsoft ADAM/AD LDS

Release 11.1.1.5.0

E21002-01

# 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 Application Mode (ADAM/AD LDS) and Microsoft Active Directory Lightweight Directory Services (AD LDS). Readers of this guide should be experienced system administrators and have a solid understanding of Active Directory, ADAM/AD LDS, AD LDS, 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 ADAM/AD LDS and AD LDS. They do not apply to LDAP, Citrix, Terminal Services, kiosk, and
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 ADAM/AD LDS. Topics include designing the tree for optimal performance vs. accurate template delivery, and best practices for configuring ESSO-LM for synchronization with ADAM/AD LDS.

**Part 2: Deployment Procedures** – Contains the required deployment and configuration procedures, such as creating an ADAM/AD LDS instance, preparing the instance for ESSO-LM, and configuring ESSO-LM for synchronization with ADAM/AD LDS.

**Part 3: Appendices** – Contains reference material supplementing the earlier sections of the guide, as well as troubleshooting instructions for the most common ADAM/AD LDS connection issues.

## Terms and Abbreviations

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

| Term or Acronym | Description |
|---|---|
| AD | Active Directory |
| ADAM/AD LDS | Active Directory Application Mode |
| AD LDS | Active Directory Lightweight Directory Services |
| 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 SSO with Microsoft ADAM/AD LDS / AD LDS. It contains the following sections:

## Overview of ESSO-LM

Oracle Enterprise Single Sign-on Logon Manager 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, 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 that can be deployed 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.

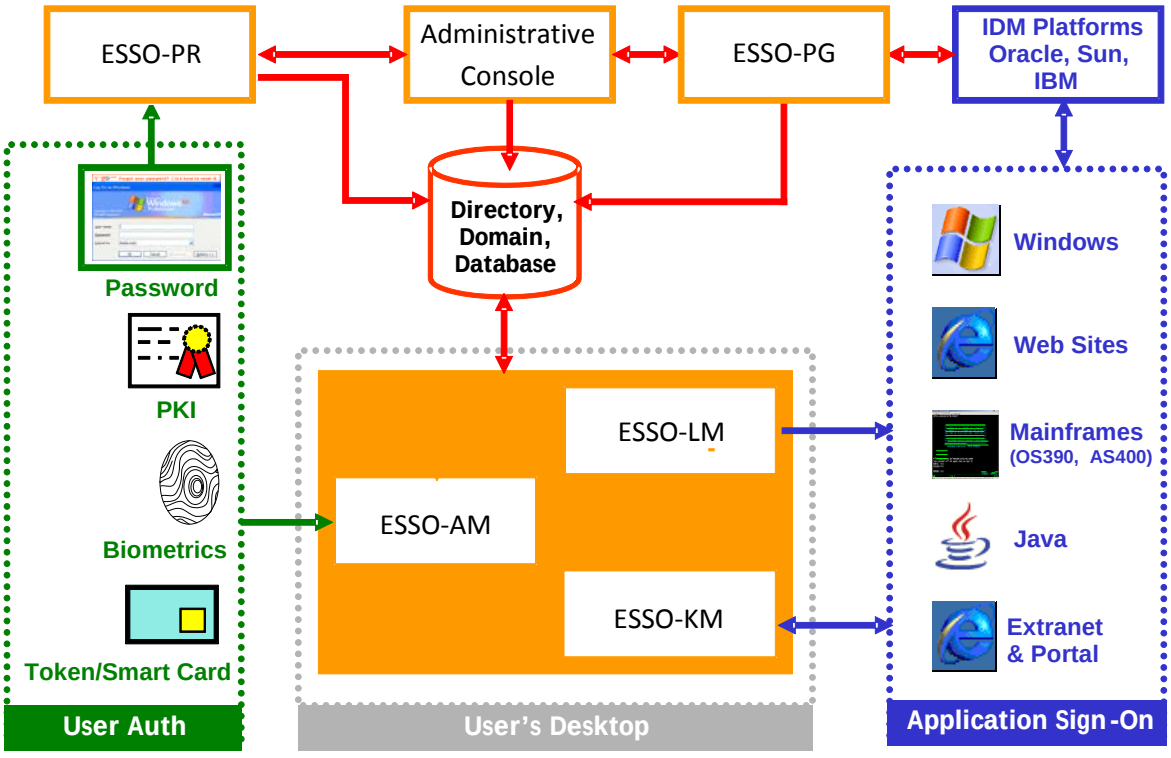



**Figure 1** ESSO-LM architecture at a glance

## ESSO-LM and ADAM/AD LDS Environments

You have the choice to deploy ESSO-LM in a directory environment, such as ADAM/AD LDS or AD LDS, 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 credentials.

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 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.

### Benefits of ADAM/AD LDS-Based Deployments

ADAM/AD LDS provides data storage and retrieval for directory-enabled applications, without the dependencies that are required by Active Directory. ADAM/AD LDS provides much of the same functionality as Active Directory, but it does not require the deployment of domains or domain controllers, and the directory schema for ADAM/AD LDS is completely independent of the enterprise schema you may be using in an Active Directory domain. You can run multiple instances of ADAM/AD LDS concurrently on a single server, with an independently managed schema for each ADAM/AD LDS instance. The following are the benefits of deploying ESSO-LM with ADAM/AD LDS:

- **Ideal for pilot and proof-of-concept deployments.** A fully functional ADAM/AD LDS instance that very closely mimics a full-scale Active Directory environment can be set up in minutes and is entirely self-contained (requiring only the Active Directory host on which it runs).
- **Simplified deployment**. ADAM/AD LDS is available free of charge from Microsoft. Deployment within existing Active Directory environments is easy and allows the reuse of existing user accounts and groups.
- **Efficient scaling and fault tolerance**. Since ADAM/AD LDS is based on Active Directory code, its scalability characteristics are similar to those of Active Directory. Just two servers, capable of supporting approximately 5,000 ESSO-LM users, are enough to ensure basic fault tolerance. If your organization consists of more than 5,000 members, consult a Microsoft expert for more information on scalability and fault tolerance.

Additionally, deploying ESSO-LM with ADAM/AD LDS in an existing Active Directory environment provides the following benefits:

- **Retraining is minimized.** Administrative procedures for ADAM/AD LDS are very similar to those for Active Directory. Administrators skilled with Active Directory will be able to deploy and maintain ADAM/AD LDS instances with little additional effort; management tools for both platforms mirror management tools for Active Directory.
- **Existing Active Directory accounts and policies can be leveraged.** Active Directory user accounts, groups, and policies are instantly available in ADAM/AD LDS. You do not need to import, re-create or synchronize your existing configuration and user account data.

### Active Directory vs. ADAM/AD LDS

The table below highlights the key differences between Active Directory and ADAM/AD LDS:

| Feature | Active Directory | ADAM/AD LDS |
|---|---|---|
| **Server Discovery and Failover** | **Fully automatic**. Client broadcasts request and listens for reply from the nearest server. Failover is simplified as fallback from server to server is automatic. | **Automatic when using a load balancer; otherwise requires an explicit server list.** For the benefits provided by a load balancer, see Load-Balancing an ESSO-LM Deployment. If not using a load balancer, client must be explicitly provided with a list of servers to connect to, ordered by geographic proximity. |
| **Schema Extension** | **Global**. You must perform a schema extension to add the required ESSO-LM object classes to your Active Directory schema. Existing classes and attributes are **not** modified in any way. Administrators must understand the impact (usually negligible) of the extension on the directory as a whole. Detailed information on the schema extension is available in Appendix C: ESSO-LM Directory Classes and Attributes. | **Local**. When deploying ESSO-LM on ADAM/AD LDS, you must perform a schema extension against the target ADAM/AD LDS instance only. The extension consists of the same four object classes as the Active Directory schema extension. |
| **Credential Storage Under User Objects** | **Yes**. You have the option to store ESSO-LM application credentials under respective user objects. | **No**. All user credentials are stored under a dedicated OU within the ADAM/AD LDS instance. This OU contains an object for each ESSO-LM user. |
| **Usage Reporting** | **Yes**. When ESSO-LM is deployed on Active Directory, you can obtain point-in-time information on user credentials stored in the directory. | **No**. ADAM/AD LDS environments do not support point-in-time information reporting for ESSO-LM. (Available on ADAM/AD LDS when ESSO-PG is installed.) |

For more in-depth information about ADAM/AD LDS and its applications, please see:

- ADAM FAQ: http://www.microsoft.com/windowsserver2003/ADAM/ADAMfaq.mspx
- AD LDS FAQ: http://technet.microsoft.com/en-us/library/cc755080%28WS.10%29.aspx

### How ESSO-LM Extends the ADAM/AD LDS Schema

Before ESSO-LM can store data in ADAM/AD LDS, you must instruct ESSO-LM to extend the schema of the selected ADAM/AD LDS instance (the Active Directory host's schema is not affected). 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.

> **Note:** Schema extension is a post-installation procedure. For instructions, see Preparing the ADAM/AD LDS Instance for ESSO-LM. Oracle highly recommends that you perform a schema health check (as described by Microsoft best practices) 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/ADAM/AD LDS Objects
- Appendix C: ESSO-LM Directory Classes and Attributes

### How ESSO-LM Synchronizes with ADAM/AD LDS

The ESSO-LM Agent uses the ADAM/AD LDS synchronizer plug-in to communicate with ADAM/AD LDS. 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 Agent's "Refresh" function

During synchronization, the ESSO-LM Agent traverses the ESSO-LM sub-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).

## Benefits of Load-Balancing an ESSO-LM Deployment

When a directory server fails, ESSO-LM will attempt to contact the next one on its server list. If no servers on the list can be reached, synchronization becomes unavailable until the problem is remedied. If your environment calls for more than one physical ADAM/AD LDS server, Oracle highly recommends using a load balancer that will evenly and automatically distribute the requests coming from the network among the ADAM/AD LDS servers behind it. If a server goes offline, the rest can temporarily absorb the workload of the failed machine, providing failover transparency to the end-user and adequate time to bring the faulty server back online.

**Note:** ADAM/AD LDS supports Network Load Balancing (NLB) only when running on the Windows Server 2003 and later operating system families.

## 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 ADAM/AD LDS Directory Sub-Tree for ESSO-LM

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 that ESSO-LM will support
- Robustness of the existing infrastructure
- Structure of your organization.

### Guidelines for Structuring the ADAM/AD LDS Sub-Tree for ESSO-LM

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 ESSO-LM root container, 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 that you do not 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.

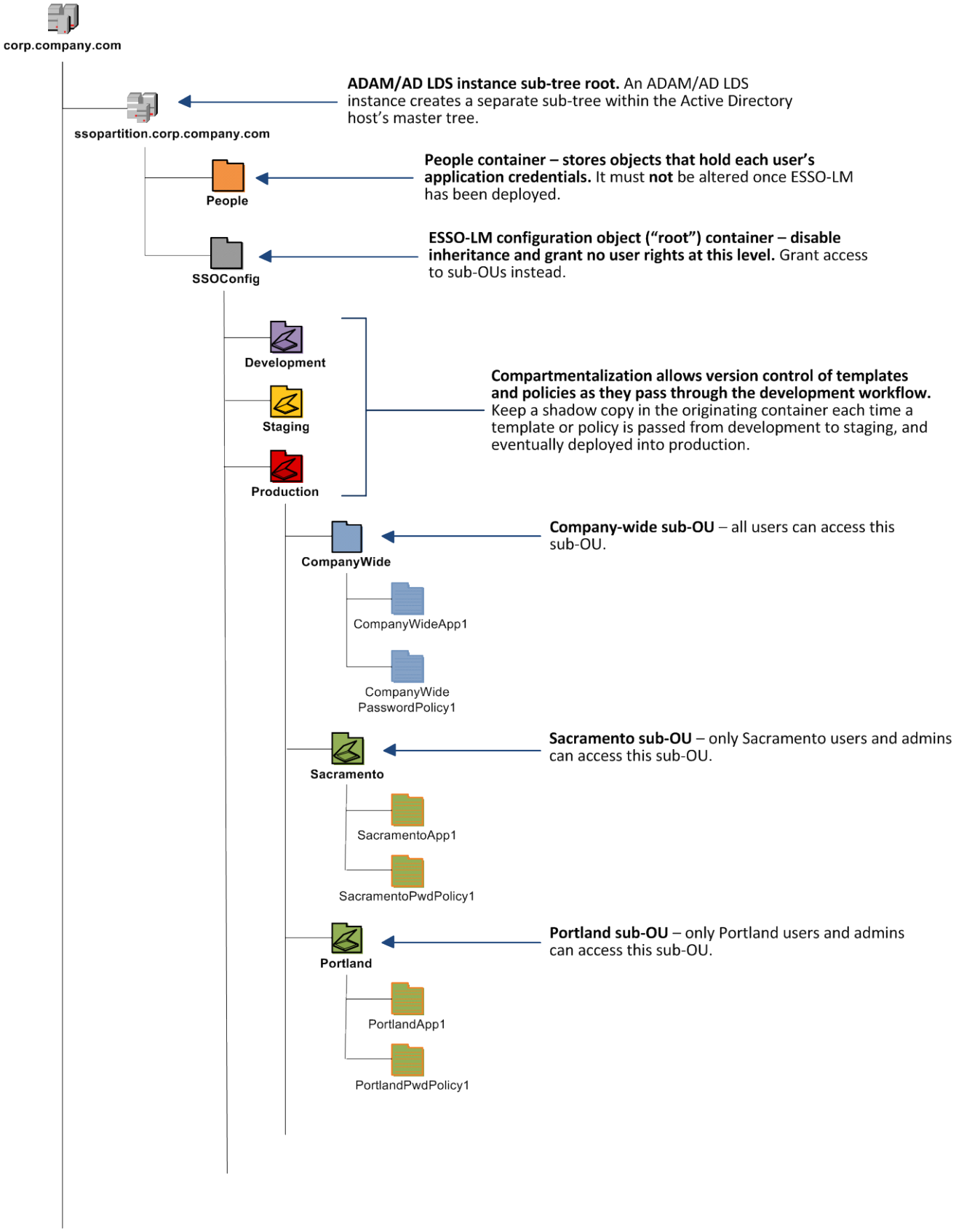



**Figure 2** Recommended ESSO-LM sub-tree design

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.

Unlike Active Directory, ADAM/AD LDS does not permit ESSO-LM to store application credentials under user objects. Instead, when deployed on ADAM/AD LDS, ESSO-LM stores application credentials in flat format inside a special OU called `People`. You must create this OU as described in Creating the People OU.

**Note:** A container object is automatically created inside the `People` OU at first use for each ESSO-LM user in order to keep user data private and separate.

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. When transitioning to a hierarchy, use the existing container as your new ESSO-LM root container and create sub-OUs underneath it.

## 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 14. 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. Retrieve 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 ADAM/AD LDS environment, always use the same connection string (IP address *or* host name) when modifying object ACLs through the Console.

## 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 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 on page 18 depicts a typical view of the ESSO-LM Administrative Console set up for synchronization with ADAM/AD LDS.

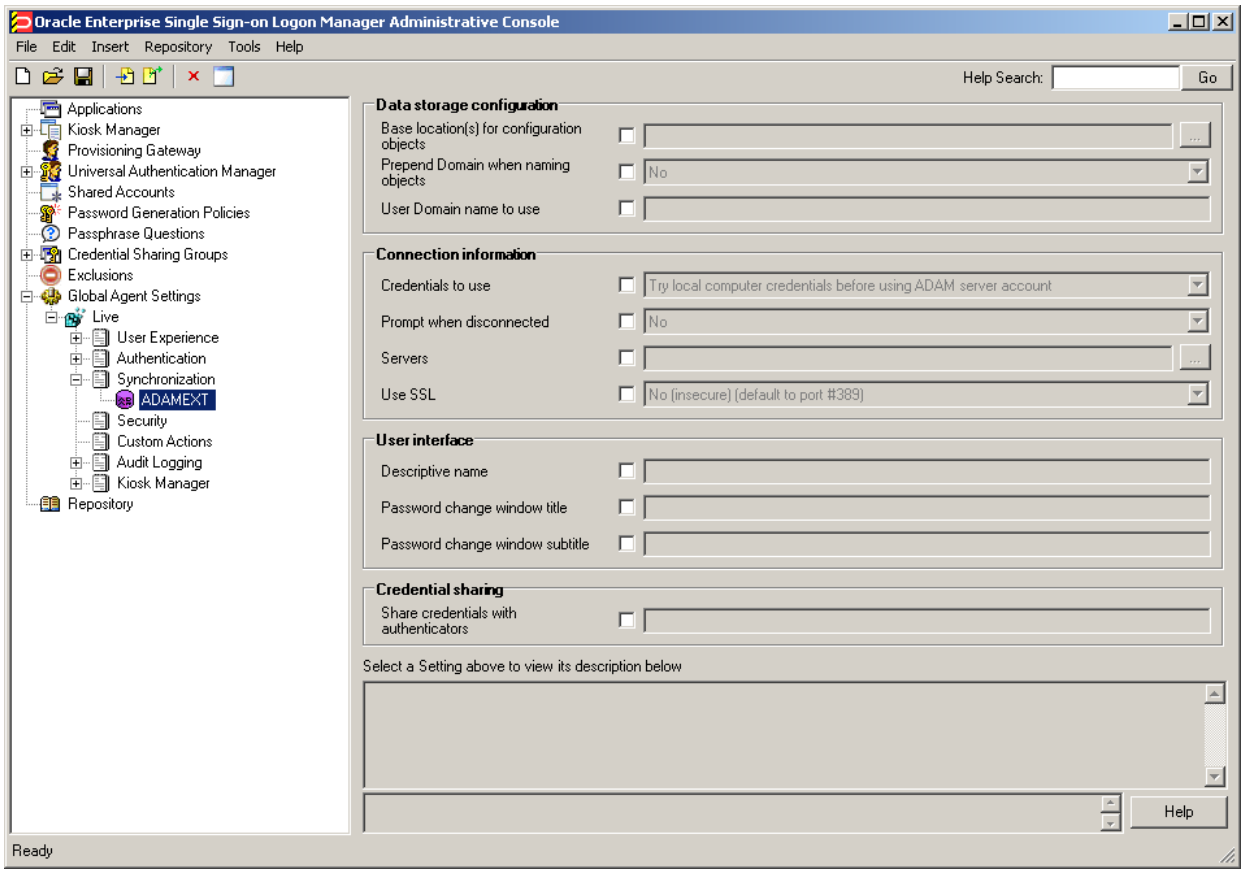



**Figure 3** The ESSO-LM Administrative Console

The next section describes best practices for configuring ESSO-LM for synchronization with ADAM/AD LDS. 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 ADAM/AD LDS synchronizer plug-in are installed on your machine; otherwise, ADAM/AD LDS-related settings will not be displayed in the Console. For installation instructions, see the installation 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.

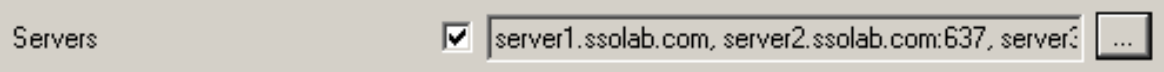
## Recommended Global Agent Settings

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: Packaging ESSO-LM for Mass Deployment*.)

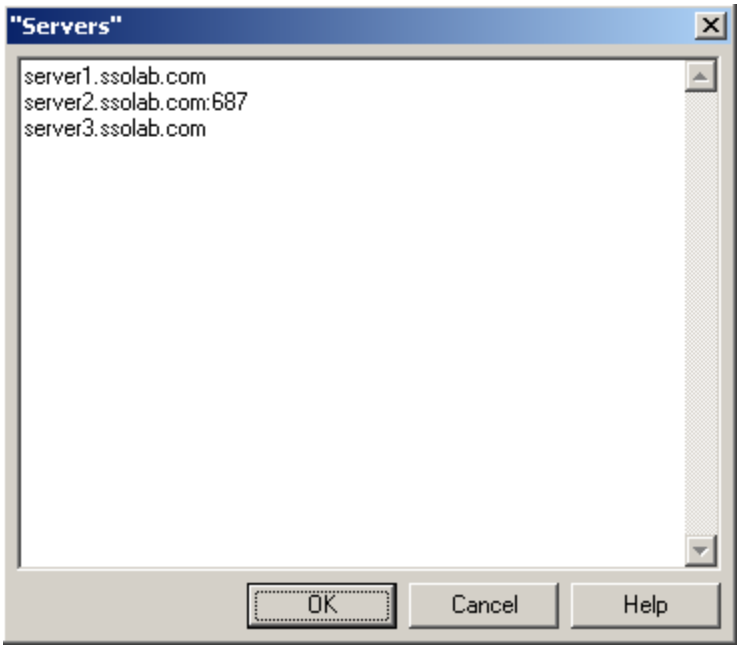
### Configure a Server List with Desired Failover Order

In ADAM/AD LDS environments, server URLs must be explicitly provided to ESSO-LM. Oracle highly recommends using at least two physical ADAM/AD LDS servers and placing them behind a load balancer for automatic, transparent failover. If you choose not to use a load balancer, arrange the server URLs in order of geographic proximity to the end-user so that the performance hit due to physical distance between the end-user and the next available server is minimized. For more information on load balancing, see Load-Balancing an ESSO-LM Deployment.

**Located in:** Global Agent Settings → Live → Synchronization → ADAMSyncExt




**To set:** Select the check box, click the (**…**) button, and enter the desired values (one per line) as shown below. When you are finished, click **OK**.



## Use Configuration Objects

On ADAM/AD LDS 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 ADAM/AD LDS Directory Sub-Tree for ESSO-LM. 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 ADAM/AD LDS.

**Located in:** Global Agent Settings → Live → Synchronization → ADAMSyncExt


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

## Configure SSL Support

By default, the ESSO-LM ADAM/AD-LDS 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.

**Located in:** Global Agent Settings → Live → Synchronization → ADAMSyncExt

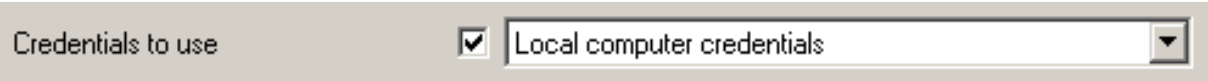

**To enable:** Select the check box, then select **Yes (default to port #636)** from the drop-down list.

## Select the Credentials to Use when Authenticating to the Repository

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

**Note:** Do **not** leave this at the default setting, **Try local computer credentials before using ADAM/AD LDS server account**. Doing so will cause an authentication failure (and the re-authentication prompt to appear, unless disabled) if the repository and the end-user machine are not part of the same domain.

**Located in:** Global Agent Settings → Live → Synchronization → ADAMSyncExt




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

## Choose Whether to Prompt the User when Disconnected from the Repository

Use the **Prompt when disconnected** option to decide whether ESSO-LM should prompt the user to re-authenticate to the repository upon authentication failure or disconnection. Oracle recommends that you set this to **No**; doing so will avoid unnecessary confusion and helpdesk calls.

**Located in:** Global Agent Settings → Live → Synchronization → ADAMSyncExt


**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 above and has no effect if **Allow disconnected operation** is set to **No**.

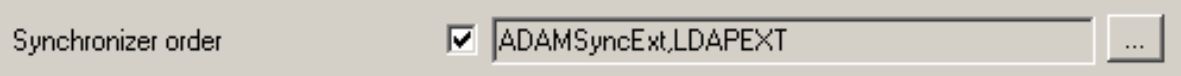
## Add the ADAM/AD LDS Synchronizer to the Synchronizer Order List

Ensure that the ADAM/AD LDS (`ADAMSyncExt`) 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-KM, 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 → Synchronization




**To set:** Select the check box, then click the (**…**) button. In the list that appears, select the checkbox next to **ADAMSyncExt** 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


Use the default value (**Yes**) 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 large numbers of credentials per user.
- Disable this option to improve synchronization performance on deployments with fewer than five credentials per user and a 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 ADAM/AD LDS. 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 ADAM/AD LDS. Make sure you have read all of the preceding sections of this document before proceeding with deployment. Deploying ESSO-LM with MS ADAM/AD LDS 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. If you have not already done so, install ADAM/AD LDS on the target server. The ADAM/AD LDS installer and installation instructions are available on the Microsoft Web site.
3. Create groups for ESSO-LM administrators and ESSO-LM users. Basic instructions are provided in Appendix B: Creating Groups for ESSO-LM Administrators and ESSO-LM Users.
4. Create a new ADAM/AD LDS instance that will be used by ESSO-LM, as described in Creating an ADAM/AD LDS Instance.
5. 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 ADAM/AD LDS Synchronizer when installing the Agent.
6. Complete the steps in Preparing the ADAM/AD LDS Instance for ESSO-LM:
   a. Extend the ADAM/AD LDS instance schema with ESSO-LM classes and attributes.
   b. Create the `People` OU, which will store each user's application credentials.
   c. Create the ESSO-LM configuration object container and desired tree structure.
   d. Grant the required permissions.
7. Configure ESSO-LM as follows:
   a. Complete the steps in Configuring the ADAM/AD LDS 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.

8. 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.
9. 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*.
10. 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.

## Creating an ADAM/AD LDS Instance

This section describes how to create an ADAM/AD LDS instance on which you will deploy ESSO-LM. If you have not already done so, install ADAM/AD LDS on the target server. The ADAM/AD LDS installer and installation instructions are available on the Microsoft web site. Before you begin, note the following:

- Oracle recommends deploying on Windows Server 2003 and later versions of the Windows Server operating system family. (ADAM/AD LDS does not support Windows 2000). Deployment on Windows XP, Windows Vista, or Windows 7 is discouraged.
- To simplify deployment, Oracle highly recommends creating an ADAM/AD LDS instance that runs on the default port (389 for non-SSL connections; SSL connections to ADAM/AD LDS are not supported). If you use a custom port, it must be open between all clients and the target servers.

  **Note:** Regardless of the type of connection to the repository, user credential data remains encrypted at all times.

- If you are installing ADAM/AD LDS on a domain controller or another server on which a directory is already running, you will not be able to use the default ports; therefore, Oracle highly recommends deploying ESSO-LM on a member server instead of a domain controller.

To create the target ADAM/AD LDS instance:

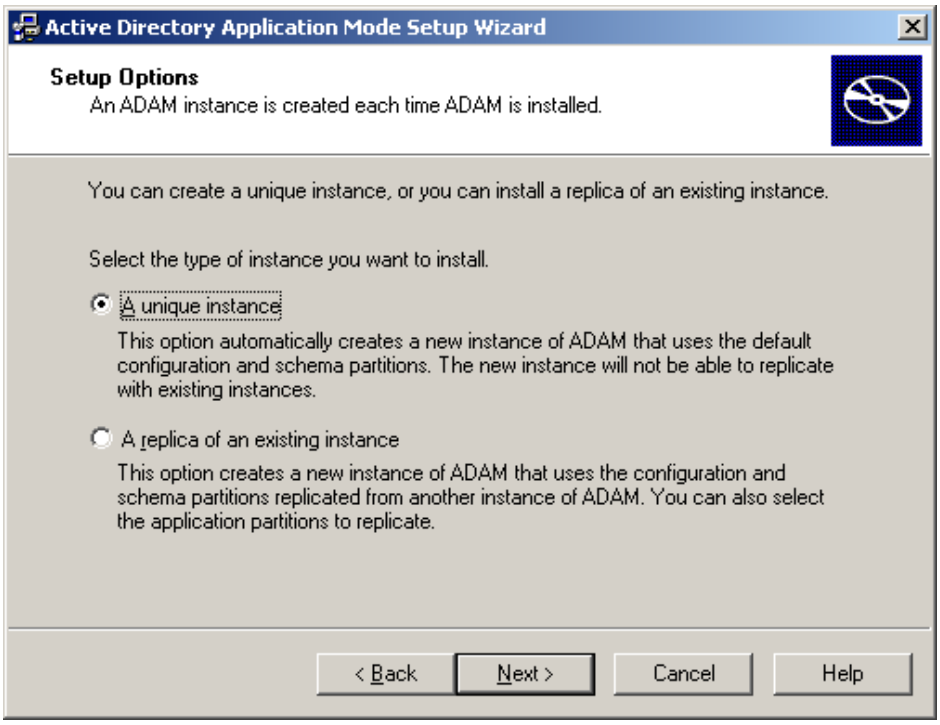
**Note:** The ADAM/AD LDS setup wizard screens depicted in this guide may differ visually across the supported versions of the Windows Server operating system family; however, the procedure is identical for all supported versions.

1. Launch the ADAM/AD LDS Setup Wizard.
   - **On Windows Server 2003**:
     Click **Start → Programs → ADAM → Create an ADAM instance**.
   - **On Windows Server 2008**:
     Click **Start → Programs → Administrative Tools → Active Directory Lightweight Directory Services Setup Wizard**.
   - **On Windows Server 2008 R2:**

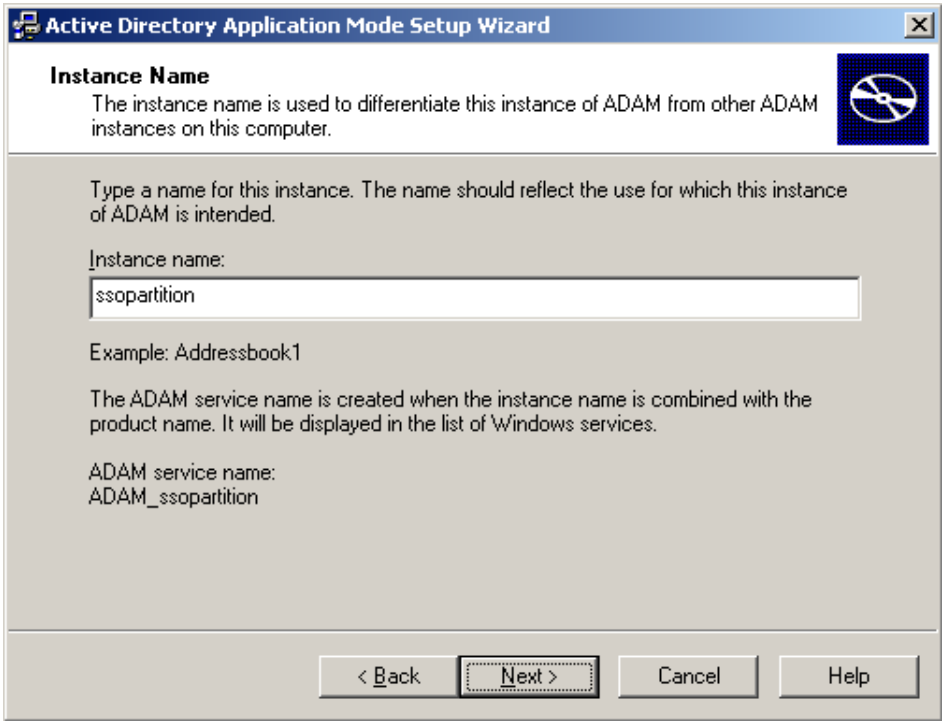
     **Note**: Make sure you have added the "Active Directory Lightweight Directory Services" role to your server before starting this procedure.

     i. In Server Manager, expand the **Roles** node and select the **Active Directory Lightweight Directory Services** role.
     ii. In the right-hand pane, expand the **Advanced Tools → AD LDS Tools** section and click **AD LDS Setup Wizard**.
2. In the "Welcome" screen, click **Next**.

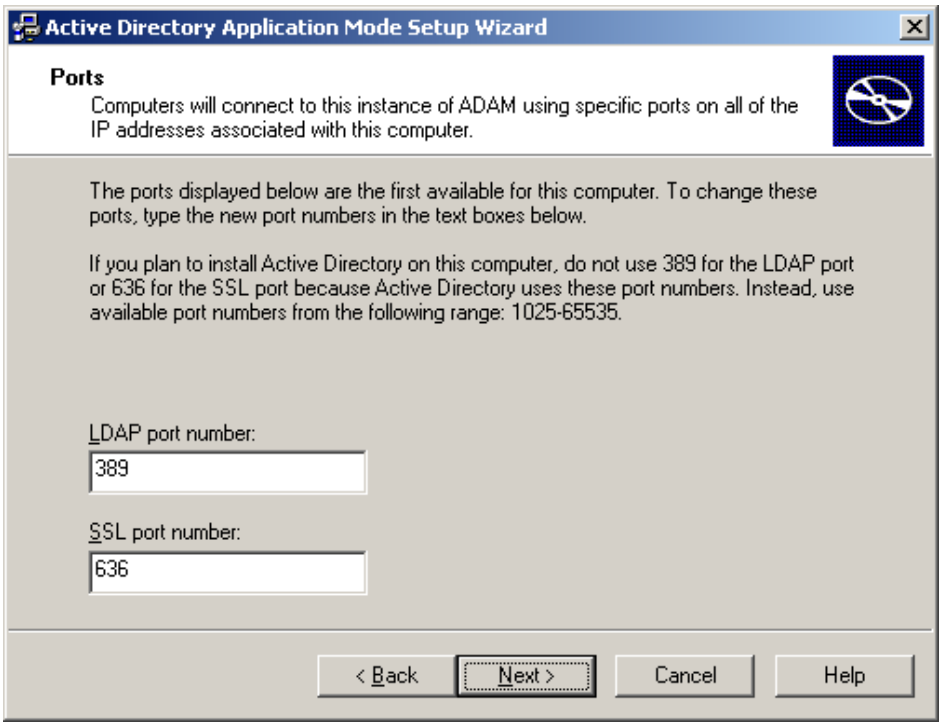
3. In the “Setup Options” screen, select **A unique instance** and click **Next**.



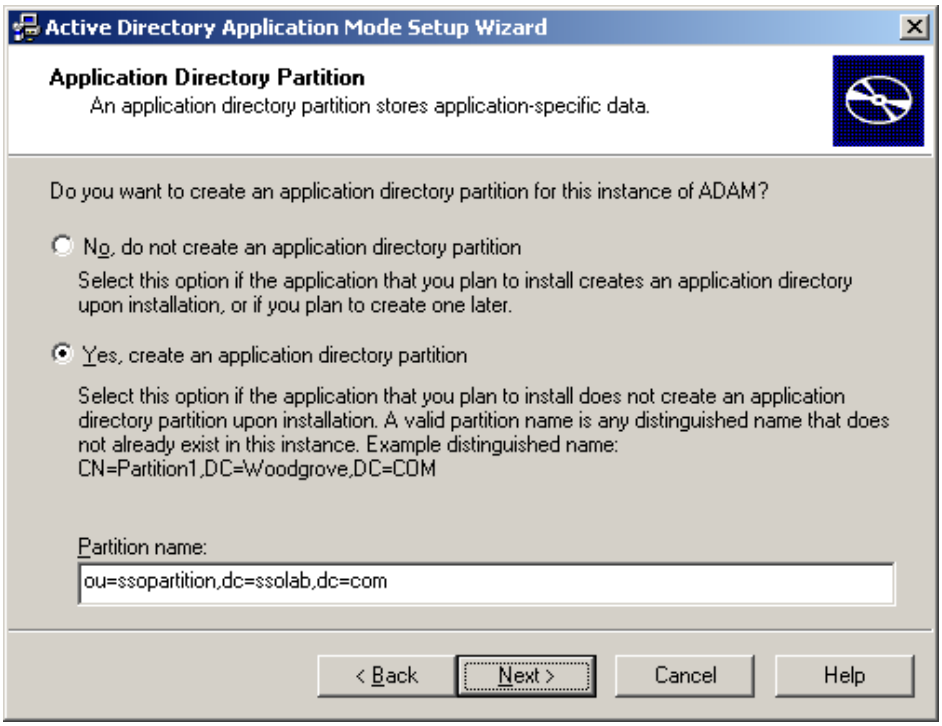

4. Name your ADAM/AD LDS instance and click **Next**. The recommended name is `ssopartition`.



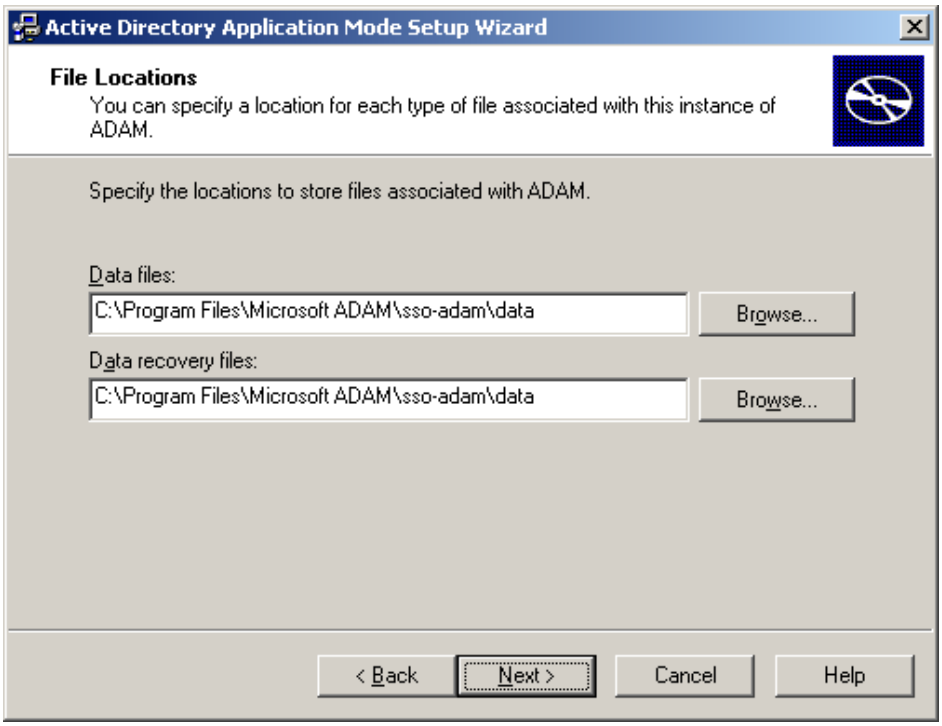
5. Enter the desired port numbers for this ADAM/AD LDS instance. If you are not using the default ports (389/636), note the custom port numbers you enter here – you will need them later to configure ESSO-LM.



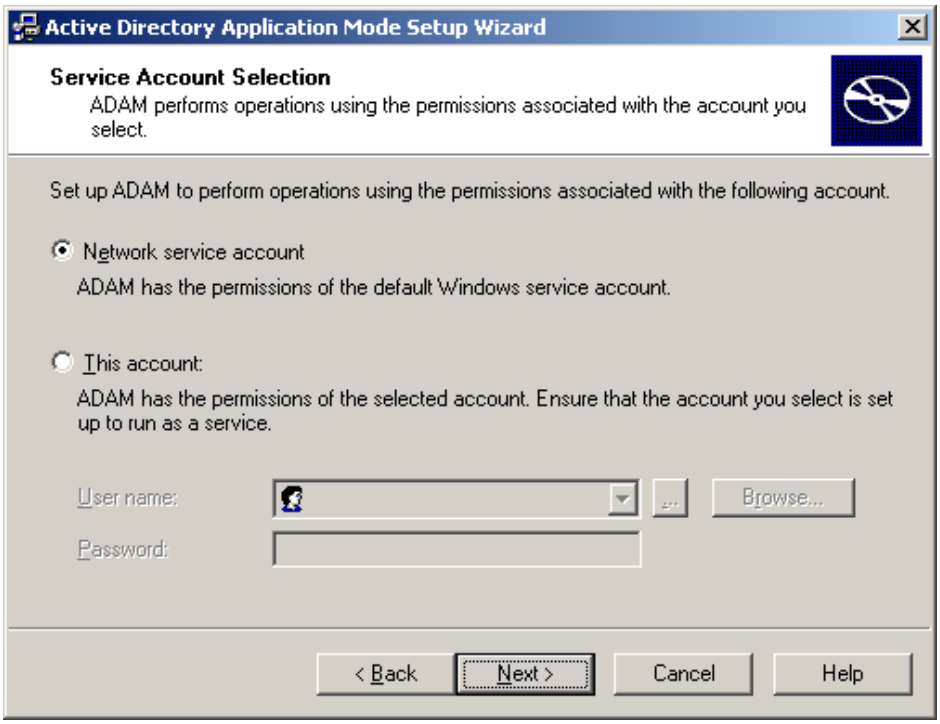

6. Select **Yes, create an application directory partition** and give the partition a fully-qualified DN. This is the root of your ADAM/AD LDS instance's sub-tree. The DN *must* start with `ou=` and not `cn=` as the dialog box suggests; otherwise, the ESSO-LM deployment will fail.



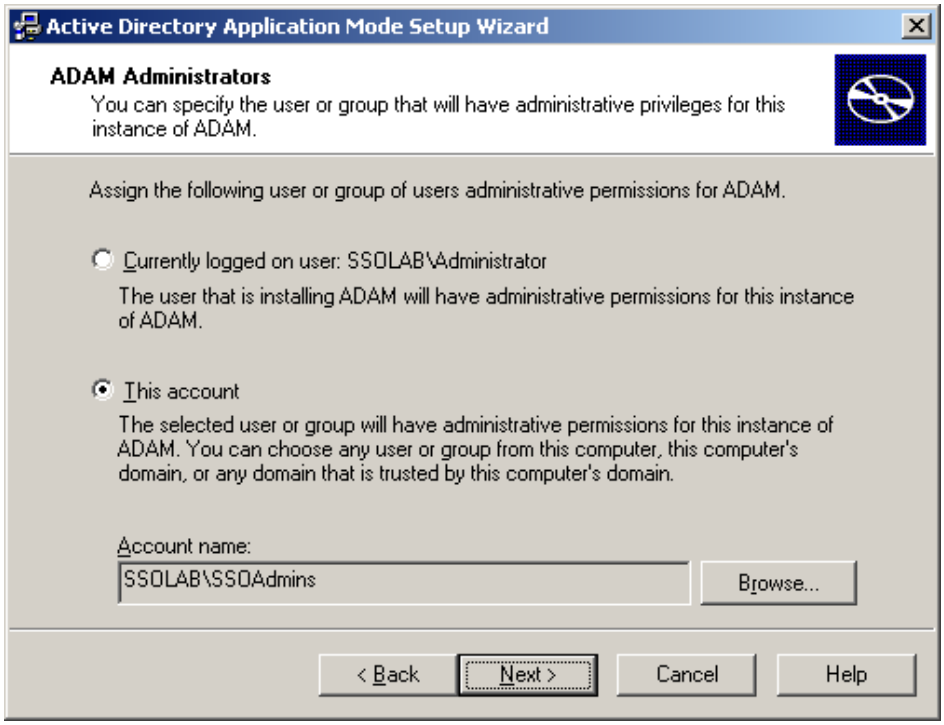
7. Specify the locations in which you want ADAM/AD LDS to store its files. In most cases, it is safe to accept the default values.



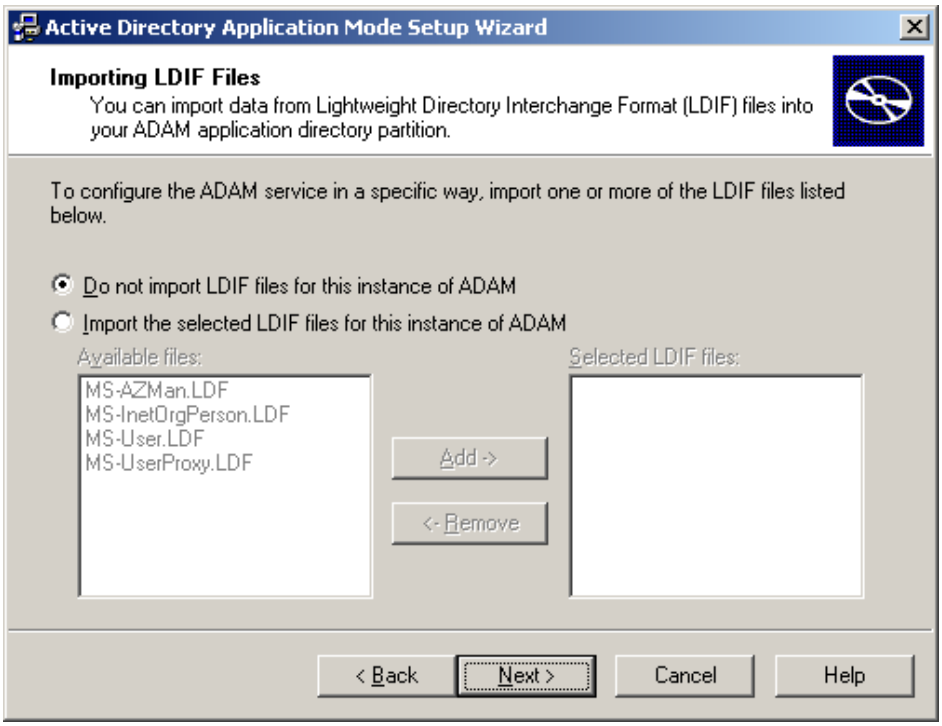

8. Specify the privileges that this instance of ADAM/AD LDS will use to run.



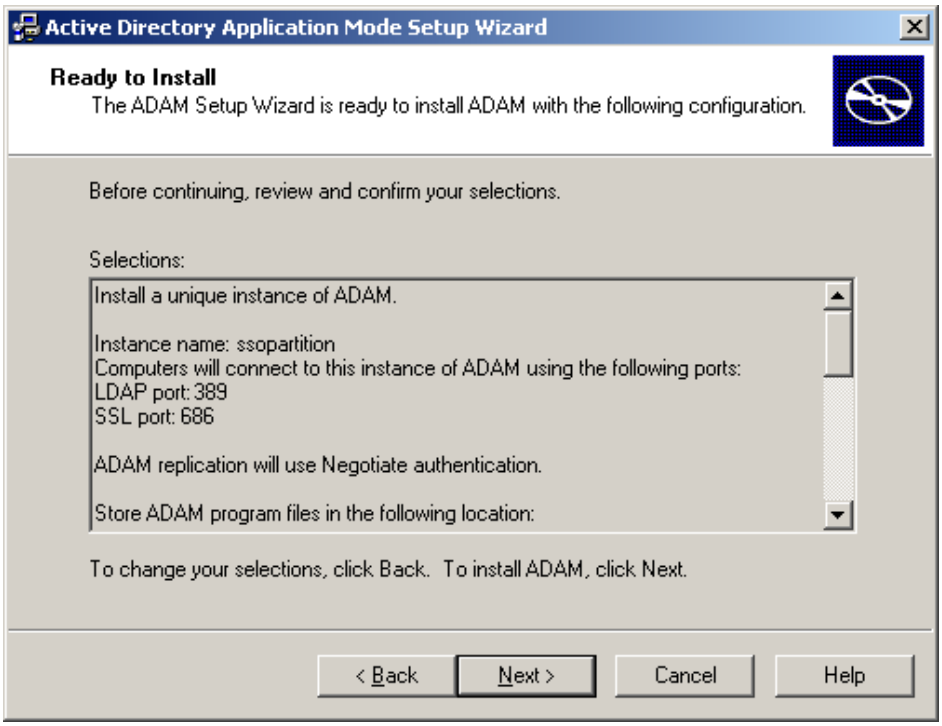
9. Select **This Account**, then click **Browse** to specify a user or group you want to have administrative privileges for this instance of ADAM/AD LDS. To prevent lockout from your entire ESSO-LM deployment, Oracle highly recommends creating a dedicated group that contains two or more users with administrative privileges over the target ADAM/AD LDS instance. For more information, see Appendix B: Creating Required User Groups.




10. Select **Do not import LDIF files for this instance of ADAM/AD LDS** and click **Next**.



11. In the summary screen, review your configuration choices. If you need to make changes, click **Back**; otherwise, click **Next** and wait for ADAM/AD LDS to create the instance.




12. When the process is complete, click **Finish** to quit the wizard.

## Preparing the ADAM/AD LDS Instance for ESSO-LM

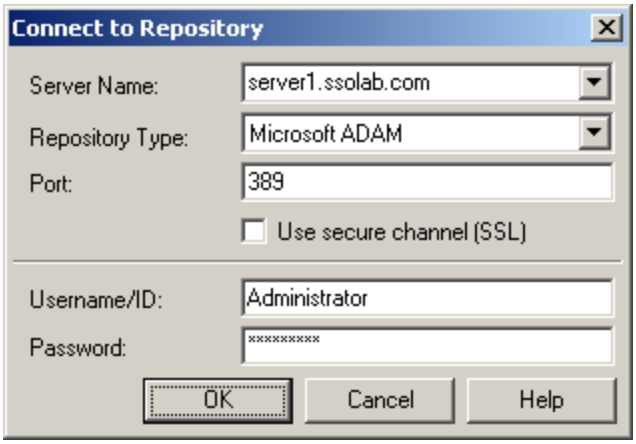
This section describes the basic procedures for preparing ADAM/AD LDS for use with ESSO-LM. The preparation consists of extending your ADAM/AD LDS schema with ESSO-LM classes and attributes, allowing ESSO-LM to store credentials under respective user objects, and creating the desired tree structure. Before starting this procedure, make sure that you have installed the ESSO-LM Administrative Console, as described in the ESSO-LM installation 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 Console**.

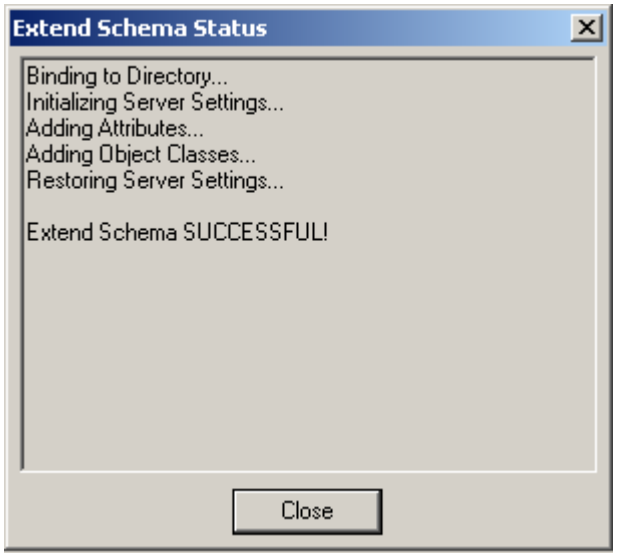
> **Note:** In a development or staging environment, disable the option **Check for publisher's certificate revocation** in Internet Explorer to eliminate a delay when the Console starts and your machine is not connected to the Internet. (The delay is caused by Internet Explorer attempting to look up 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 ADAM**.
5. Enter the port number on which your directory is listening for connections.
   The default port is 636 for SSL connections and 389 for non-SSL connections.
6. (Optional) If you configured your network environment to use SSL, select the **Use secure channel (SSL)** option enabled; otherwise, deselect 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 ADAM/AD LDS. Depending on your environment, you may need to include the corresponding domain name as part of the user name, for example `DOMAIN\user`.
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:




9. Click **Close**.

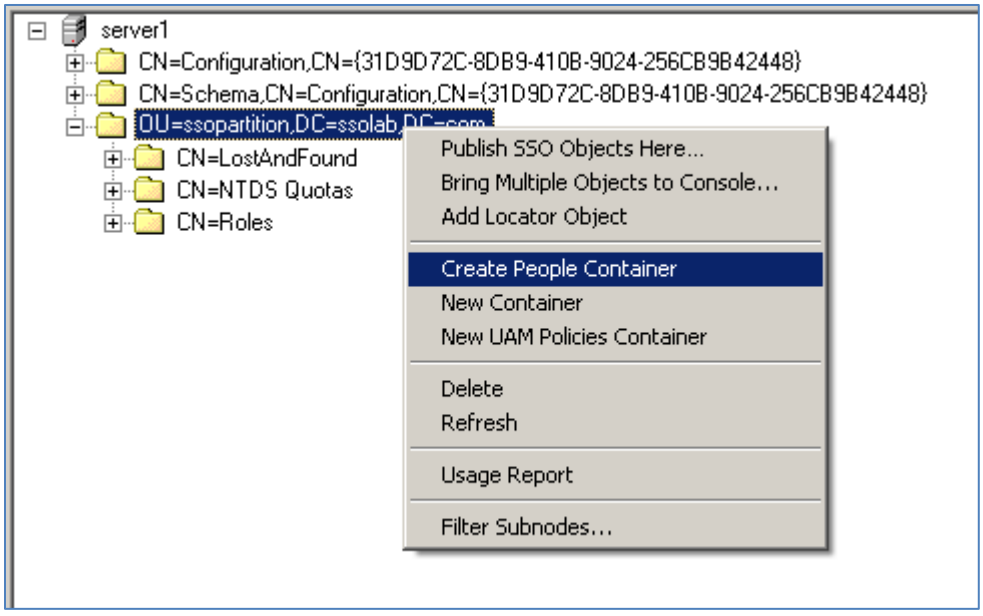
If the schema extension fails, check to make sure you have specified the ADAM/AD LDS instance DN correctly, as described in step 6 on page 28. If the DN is incorrect, delete and re-create the ADAM/AD LDS instance, then repeat this procedure.

## Step 2: Creating the People OU

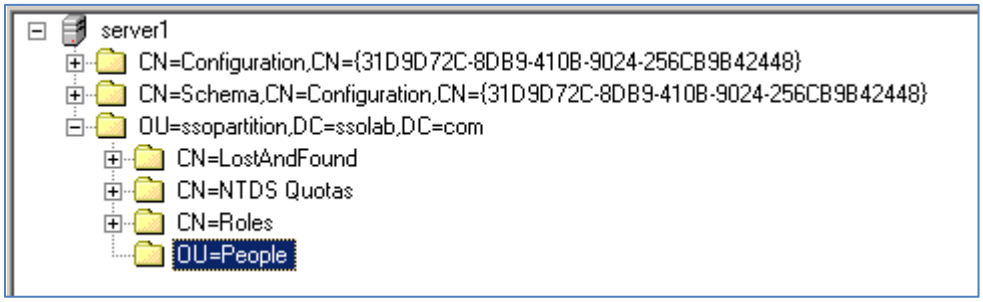
After extending the ADAM/AD LDS instance schema, you must create the People OU at the root of the instance's sub-tree. ESSO-LM will use this OU to store user application credentials.

To create the People OU:

1. In the ESSO-LM 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 steps 3–7 on page 31 and click **OK** to connect.
3. In the tree, right-click the root of the target ADAM/AD LDS instance, and select **Create People Container** from the context menu.




4. Verify that the People OU now exists at the root of the ADAM/AD LDS instance's sub-tree.

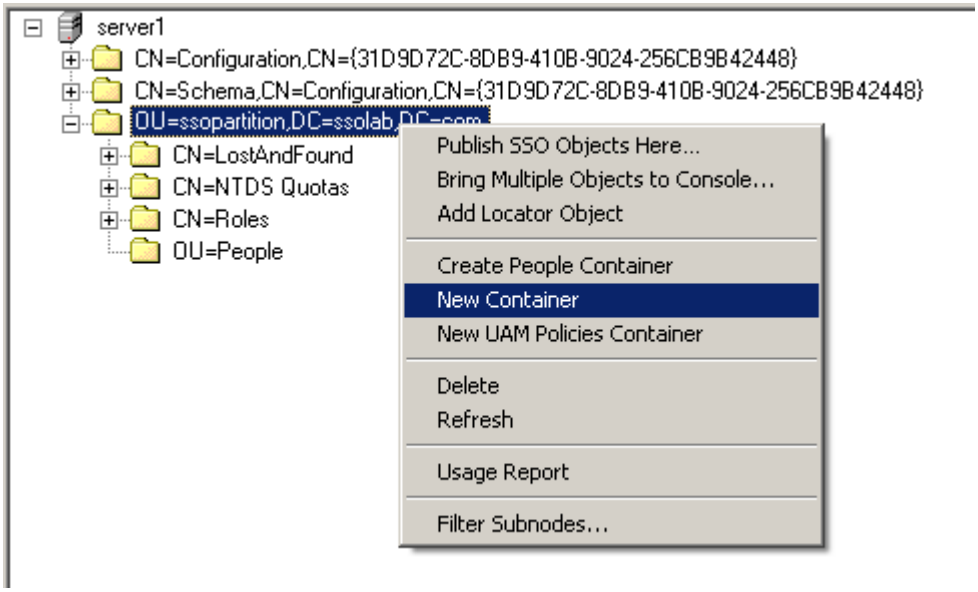



If the People OU does not appear after you complete the above steps, or if you receive errors indicating naming violations or other problems in the directory, consult the ADAM/AD LDS documentation for possible causes and remedies.

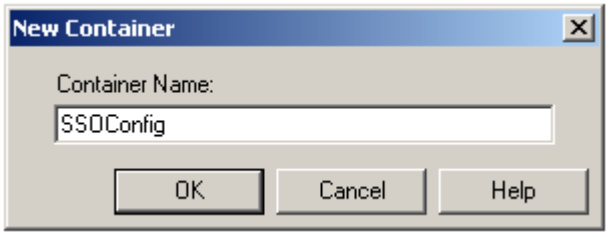
## Step 3: Creating the ESSO-LM Configuration Object Container and Sub-Tree Structure

**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.
2. Click the **Click here to connect** link in the right-hand pane. The Console displays the "Connect to Directory" dialog.
3. Fill in the fields as explained in steps 3–7 on page 32 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.

## Step 4: Granting Required Permissions to ESSO-LM Users

You must grant ESSO-LM users the following permissions in order to enable them to use ESSO-LM:

- **Read access to the ESSO-LM application partition.** This permits users to read configuration objects and credentials during synchronization.
- **Write access to the `People` OU.** This permits users to create credential objects during synchronization.

> **Note:** This procedure assumes you have already created the `SSOUsers` group and added the desired users to the group. You will grant the permissions listed above to the `SSOUsers` group, not individual users. For instructions on creating the group and assigning users to the group, see Appendix B: Creating Required User Groups.

To grant these permissions:

1. Log on to the target server as an administrator and open a command prompt.
2. Use the following command to grant the `SSOUsers` group read access to the ESSO-LM application partition (note that the command is a single line):

   ```
   dsacls \\<hostname>:<port>\ <sso_partition_dn> /G
    "<domain>\SSOUsers":gr
   ```

3. Use the following command to grant the `SSOUsers` group write access to the `People` OU (note that the command is a single line):

   ```
   dsacls \\<hostname>:<port>\ OU=People,<sso_partition_dn> /G
    "<domain>\SSOUsers":CCWS
   ```

Substitute the variables in the above commands as follows:

- `<hostname>` – the URL of the server running the target ADAM/AD LDS instance.
- `<domain>` - target domain name.
- `<port>` – the port on which the target ADAM/AD LDS instance is listening for connections.
- `<sso_partition_dn>` - the fully qualified DN of the ESSO-LM application partition. Example: `ou=ssopartition,dc=ssolab,dc=com`

## Configuring the ADAM/AD LDS Synchronizer

After you have prepared ADAM/AD LDS for ESSO-LM, you must configure the ADAM/AD LDS 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 ADAM/AD LDS 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.

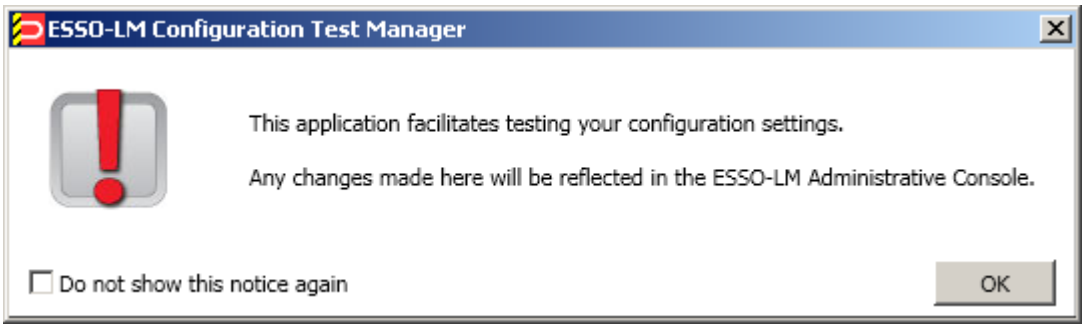
   **Note:** When the check box next to a setting is unchecked, the default value for the setting (shown grayed-out to the right of the check box) is in effect.

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.

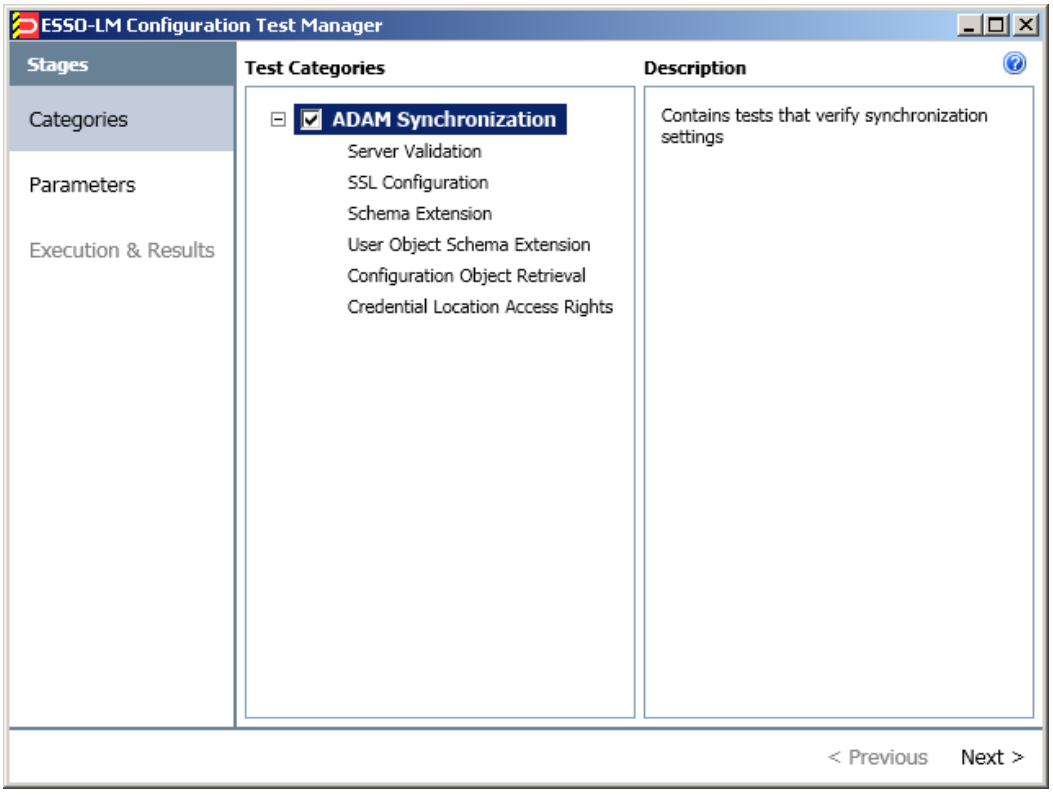
## Testing the ESSO-LM Configuration

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 contains material supplementing the information contained earlier in this guide.
It contains the following appendices:

# Appendix A: Minimum Administrative Rights for ESSO-LM Directory 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 ADAM/AD LDS schema. If necessary, these rights can be manually granted and modified directly in ADAM/AD LDS 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: Creating Required User Groups

This appendix describes how to create the `SSOAdmins` and `SSOUsers` groups in Active Directory for use with ESSO-LM deployed on an ADAM/AD LDS instance.

- **`SSOAdmins`**. This group contains at least two users who hold administrative privileges over the target ADAM/AD LDS instance. This group should also contain users who need to create and push application templates.

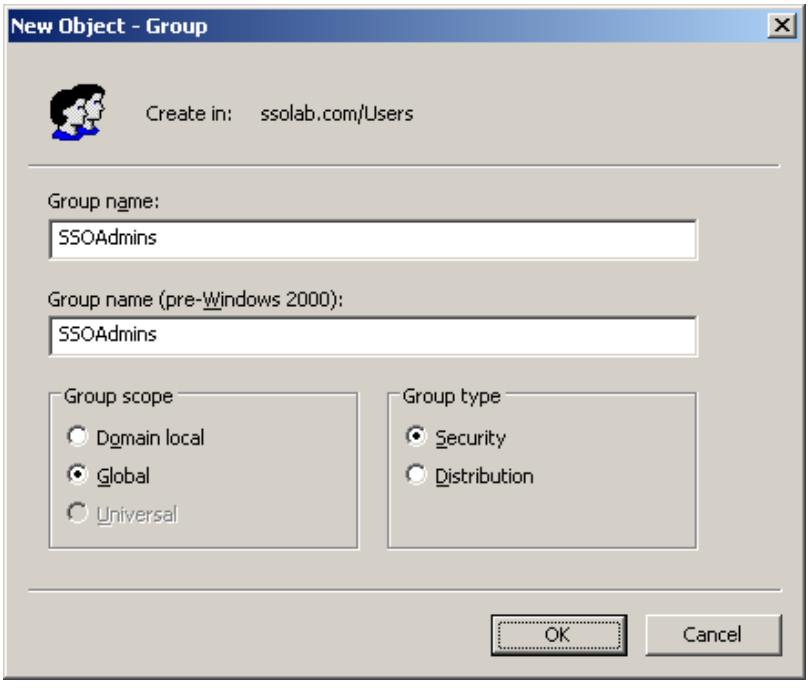
  **Caution:** When creating the instance, specify this group as the administrative user group. If you specify a single user, you risk locking yourself out of your ESSO-LM deployment if the single account becomes inaccessible.

- **`SSOUsers`**. This group contains all other ESSO-LM users.

To create the `SSOAdmins` and `SSOUsers` groups and place the desired users in these groups:

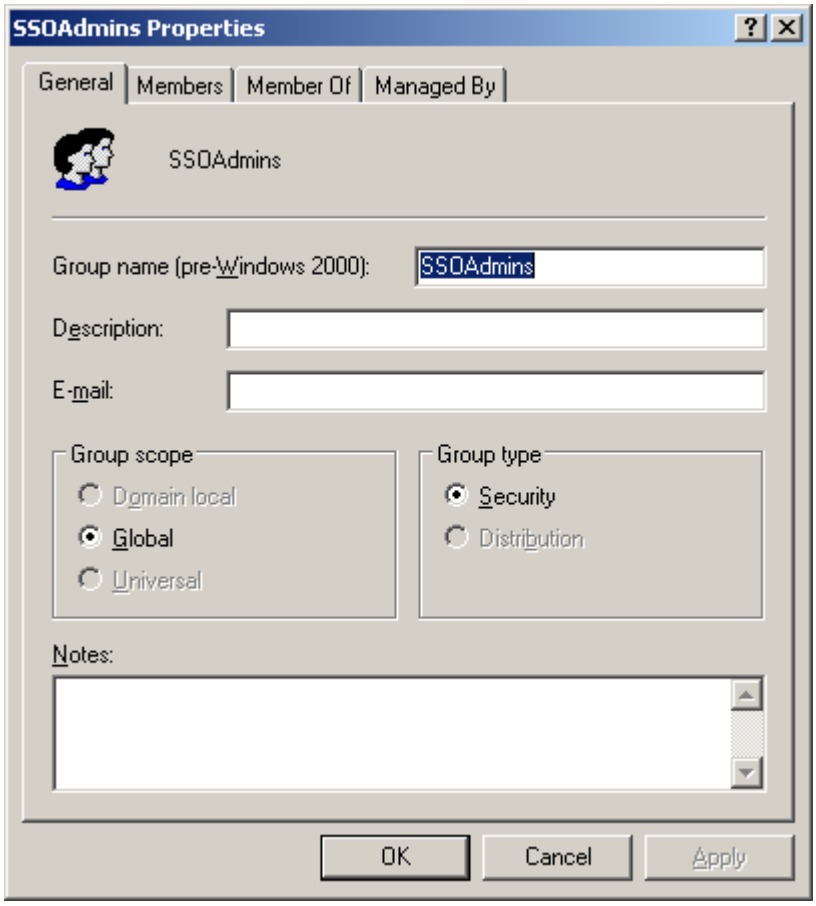
**Note:** This procedure assumes you have decided which users will belong in which groups and that the target user accounts already exist.

1. Log on to your domain controller as the administrator.
2. Open the **Active Directory Users and Computers** console snap-in.
3. In the console, expand the target domain and right-click the **Users** node.
4. In the context menu, select **New → Group**.
5. In the "New Object – Group" dialog, do the following:
   a. Enter the group name shown above.
   b. Select the **Global** group scope.
   c. Select the **Security** group type.
   d. Click **OK**.

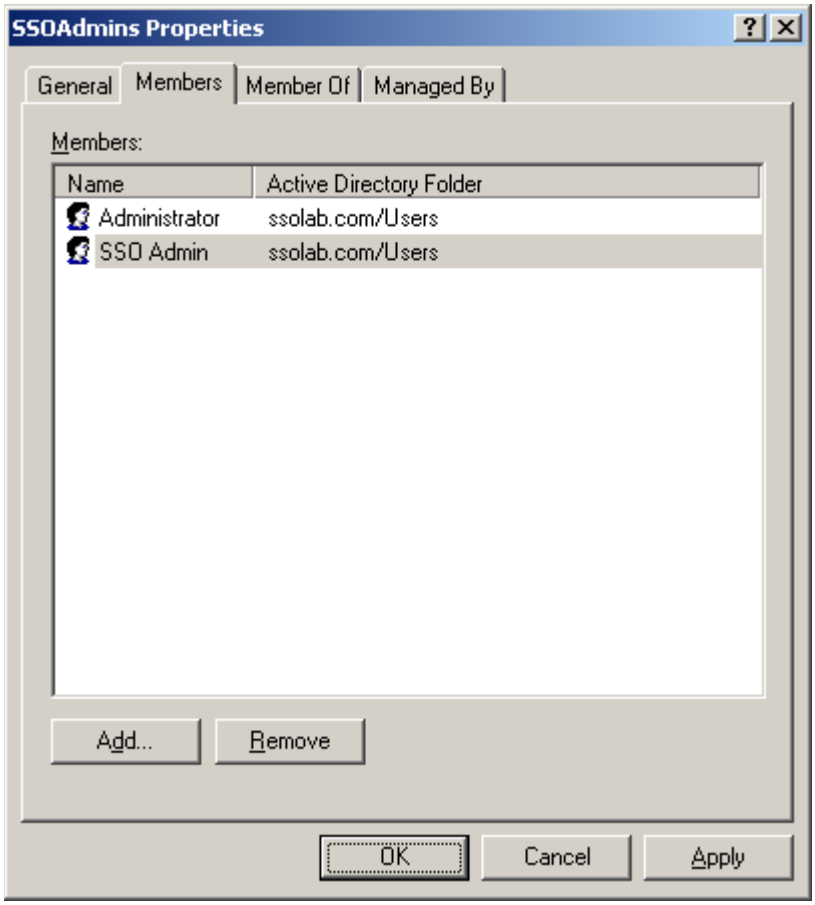


The new group appears in the list of objects in the right-hand pane of the console.

6. In the list of objects, double-click the group you just created. The group properties dialog box appears.



7. In the group properties dialog, do the following:
   a. Select the **Members** tab.
   b. Click **Add**.
   c. In the dialog box that appears, do the following:
      i. Enter the target user name and click **Check Names** to verify the user name. If you receive an error, correct any spelling mistakes and click **Check Names** again.
      ii. When the user name is validated, click **OK**.
   d. Repeat steps 7b and 7c for each additional user you want to include in the group.
   e. When you have added the desired users to the group, click **OK** to close the group properties dialog box.




8. Repeat steps 4–7 to create and configure the `SSOUsers` group.

# Appendix C: ESSO-LM Directory 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.

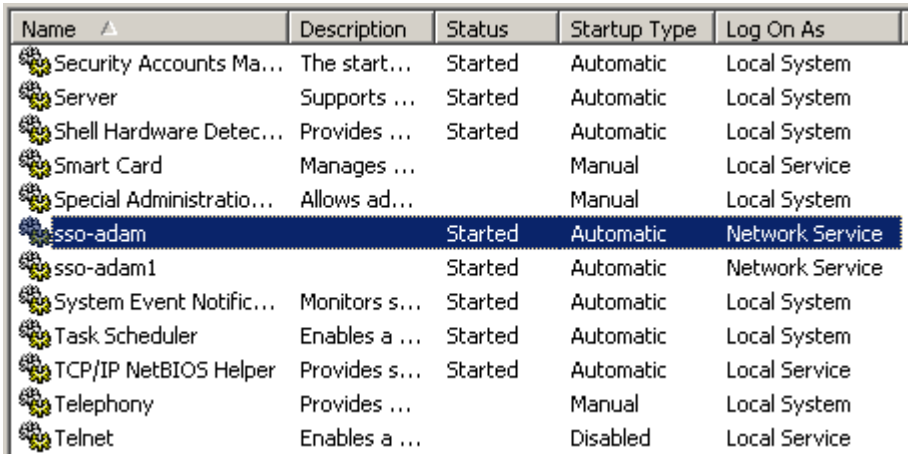
# Appendix D: Troubleshooting ESSO-LM Connecting to ADAM/AD LDS

If ESSO-LM is unable to connect to the target ADAM/AD LDS instance, try connecting to your ADAM/AD LDS instance directly using the ADSIEdit tool. If you still cannot connect, the possible causes are:

## The Target ADAM/AD LDS Instance is Not Running

Your ADAM/AD LDS instance runs as a service on the target server. Use the Computer Management MMC
snap-in on the target server to check whether the ADAM/AD LDS instance is running by doing the following:

1. Open the Computer Management console. (The quickest way is to right-click on **My Computer** and select **Manage** from the context menu.)
2. In the left-hand pane select **Services**. The console displays a list of services installed on the system.
3. Locate your ADAM/AD LDS instance in the list.




4. If the instance's status is "Stopped," start it as follows:
   a. Double-click the instance. The instance's property dialog box appears.
   b. Ensure that the **Startup Type** option is set to **Automatic** (if it isn't, set it).
   c. Click **Start** and wait for the instance to initialize.
   d. Click **OK** to close the property dialog box.

If the instance's status is "Started" and you still cannot connect, you may be connecting to the instance using the wrong port. See the next section for more information.

## ADAM/AD LDS Instance is Running on Non-Default Ports

If you configured your ADAM/AD LDS instance to use custom ports, you must instruct ESSO-LM (and other software, such as ADSIEdit) to use those ports when connecting to the ADAM/AD LDS instance. To troubleshoot this issue, do the following:

- To check the ports on which the target ADAM/AD LDS instance is running, see ADAM/AD LDS documentation.
- To check (and correct) the ports ESSO-LM uses to connect to ADAM/AD LDS, examine the contents of the **Servers** field in the Console. ESSO-LM uses the default port (636 for SSL connections, 389 for non-SSL connections) unless a specific port number is appended to the server URL, for example `dc1.company.com:9448`.

## Account Used to Connect to ADAM/AD LDS Does Not Have the Required Privileges

If ESSO-LM cannot connect to ADAM/AD LDS, check whether the user account used to connect to ADAM/AD LDS has the required privileges. To check and set the privileges for a user account, see the operating system and ADAM/AD LDS documentation.