Oracle® Enterprise Single Sign-On
Logon Manager

Deploying Logon Manager with a Directory-Based Repository

Release 11.1.2

E27161-04

September 2013

Oracle Enterprise Single Sign-On Logon Manager: Deploying Logon Manager with a Directory-Based Repository

Release 11.1.2.1.0

E27161-04

Table of Contents

Preface

Audience

This guide describes best practices and recommended procedures for deploying Oracle Enterprise Single Sign-On Manager (Logon Manager) with Microsoft Active Directory, Microsoft AD LDS (ADAM), and an LDAP directory such as Oracle Internet Directory. Readers of this guide should be experienced system administrators and have a solid understanding of the surrounding technologies and related concepts, such as directory schema, structure, and security.

Oracle highly recommends that you read this guide before planning the deployment of Logon Manager 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.

Access to Oracle Support

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

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

Conventions

The following text conventions are used in this document:

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

Related Documents

We continually strive to keep our documentation accurate and up to date. For the latest version of this and other documents, visit http://docs.oracle.com/cd/E29306_01/index.htm .

For more information, see the other documents in the documentation set for this release:

- **Oracle Enterprise Single Sign-On Suite**
  - *Release Notes*
  - *Installation Guide*
  - *Administrator's Guide*
  - *Secure Deployment Guide*
  - *User's Guide*
- **Oracle Enterprise Single Sign-On Logon Manager**
  - *Configuring and Diagnosing Logon Manager Application Templates*
- **Oracle Enterprise Single Sign-On Provisioning Gateway**
  - *Administrator's Guide*
  - *Command Line Interface Guide*
  - *Oracle Identity Manager Connector Guide*
  - *Sun Java System Identity Manager Connector Guide*
  - *IBM Tivoli Identity Manager Connector Guide*
- **Oracle Enterprise Single Sign-On Universal Authentication Manager**
  - *Administrator's Guide*
  - *User's Guide*

Deploying Logon Manager with Microsoft Active Directory

This part describes best practices for deploying Logon Manager with Microsoft Active Directory. It contains the following sections:

- Logon Manager and Active Directory Environments
- Designing the Logon Manager Active Directory Sub-Tree
- Global Agent Settings vs. Administrative Overrides
- Recommended Global Agent Settings
- Recommended Administrative Overrides
- Overview of the Deployment Process
- Preparing Active Directory for Logon Manager
- Configuring the Active Directory Synchronizer
- Testing the Logon Manager Configuration

Logon Manager and Active Directory Environments

Oracle Enterprise Single Sign-On Logon Manager (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; Logon Manager automatically detects and handles all subsequent requests for user credentials. For more information on Logon Manager, see the *Oracle Enterprise Single Sign-On Suite Technical Overview* white paper available from Oracle Support.

You have the choice to deploy Logon Manager 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 Logon Manager to your existing directory environment provides the following benefits:

- Logon Manager 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.
- Logon Manager data is automatically protected by your existing backup, failover, and disaster recovery plans.
- No dedicated servers or server-side processes are required; Logon Manager'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 Logon Manager is achieved through the native capabilities of the directory.

A directory also enables the organization of Logon Manager 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 Logon Manager administration by permitting more efficient access control.

How Logon Manager Extends Your Active Directory Schema

Before Logon Manager can store data in Active Directory, you must extend your Active Directory schema using the Administrative Console. 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 Logon Manager to store application credentials under user objects (a recommended best practice), Logon Manager will also apply the permissions required by this feature.

Note: Schema extension is a post-installation procedure. For instructions, see Preparing Active Directory for Logon Manager. 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 Logon Manager, see the following appendices:

- Appendix A: Minimum Administrative Rights for Logon Manager Repository Objects
- Appendix B: Logon Manager Repository Object Classes and Attributes

How Logon Manager Synchronizes with Active Directory

The Logon Manager 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 Logon Manager 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 Logon Manager is configured to respond to these events).
- The auto-synchronize interval elapses (if configured).
- The user initiates synchronization via the Logon Manager Logon Manager's "Refresh" function.

During synchronization, the Logon Manager Agent traverses the Logon Manager 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 Logon Manager Handles and Stores Application Credentials

Logon Manager 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. Logon Manager 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 Logon Manager stores per enabled application and per user is trivial (measurable in bytes and small kilobytes).

Note: Logon Manager supports SSL encryption for directory connections. While normally not required, SSL support is necessary in certain scenarios. See SSL Support for details.

Further Reading

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

Designing the Logon Manager Active Directory Sub-Tree

Logon Manager 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 Logon Manager 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

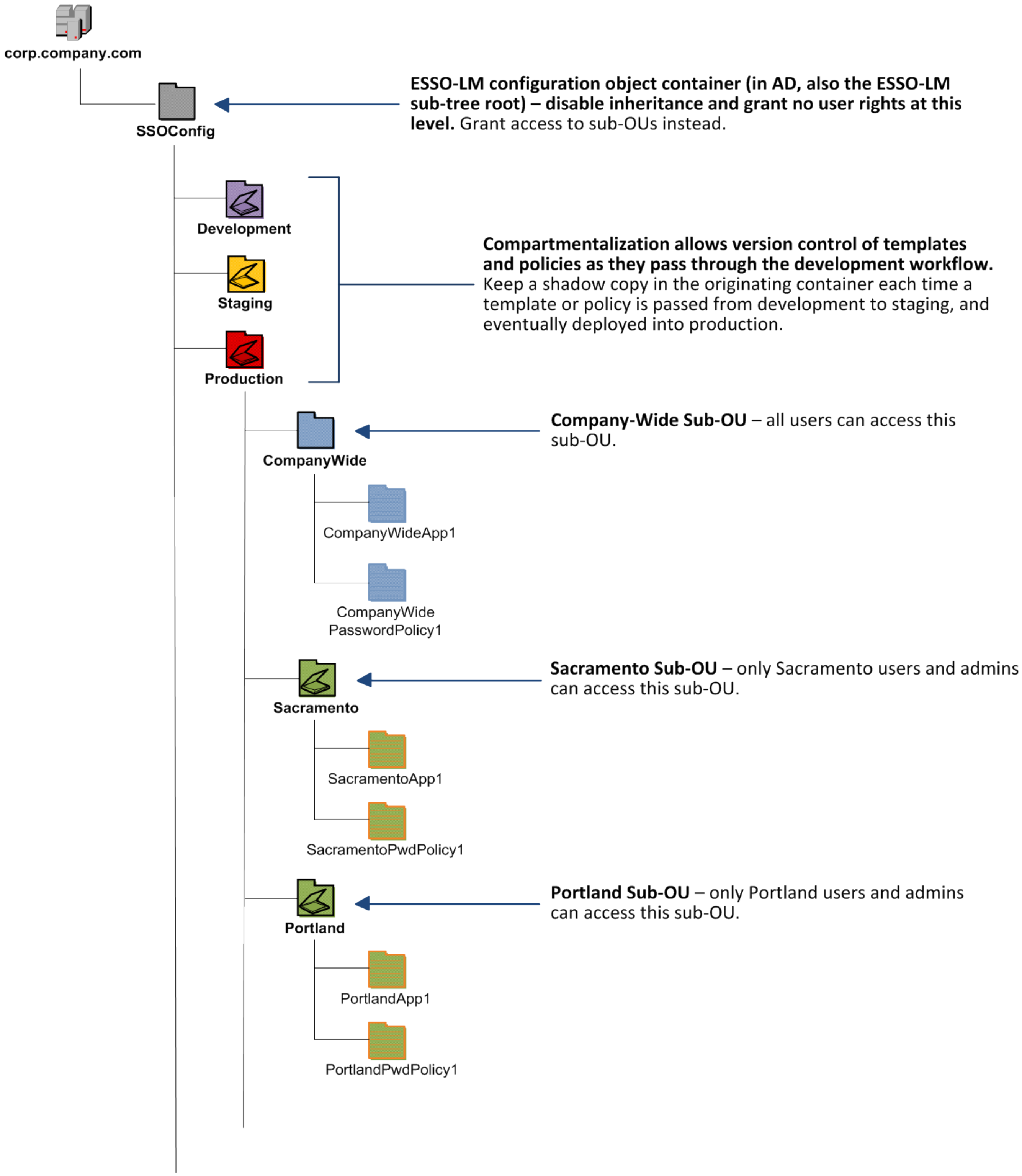
Oracle recommends that you set up your sub-tree as a hierarchy by following the guidelines below:

- 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 Logon Manager 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 Logon Manager Administrative Console; controlling access at the OU level is achieved via delegated administration using Microsoft and third-party management tools.

Figure 1 depicts a sample Logon Manager sub-tree whose design reflects the above best practices.



ESSO-LM configuration object container (in AD, also the ESSO-LM sub-tree root) – disable inheritance and grant no user rights at this level. Grant access to sub-OUs instead.

Compartmentalization allows version control of templates and policies as they pass through the development workflow. Keep a shadow copy in the originating container each time a template or policy is passed from development to staging, and eventually deployed into production.

Company-Wide Sub-OU – all users can access this sub-OU.

Sacramento Sub-OU – only Sacramento users and admins can access this sub-OU.

Portland Sub-OU – only Portland users and admins can access this sub-OU.

Figure 1 Recommended Logon Manager 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: Oracle highly recommends that you store templates and policies in individual OUs. To do this, 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 1. 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 Logon Manager 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 Logon Manager, 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 Logon Manager Agent, including its interaction with the directory, is governed by settings configured and deployed to the end-user machine by the Logon Manager administrator using the Logon Manager Administrative Console. The settings fall into one of the following categories:

- **Global Agent settings** are the "local policy" for the Agent**;** they are stored in the Windows registry on the end-user machine and are included in the Logon Manager MSI package to provide the Agent with an initial configuration during deployment. Global Agent settings are stored in `HKEY_LOCAL_MACHINE\Software\Passlogix` (32-bit systems) or `HKEY_LOCAL_MACHINE\Wow6432Node\Software\Passlogix` (64-bit systems).

  > **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**.

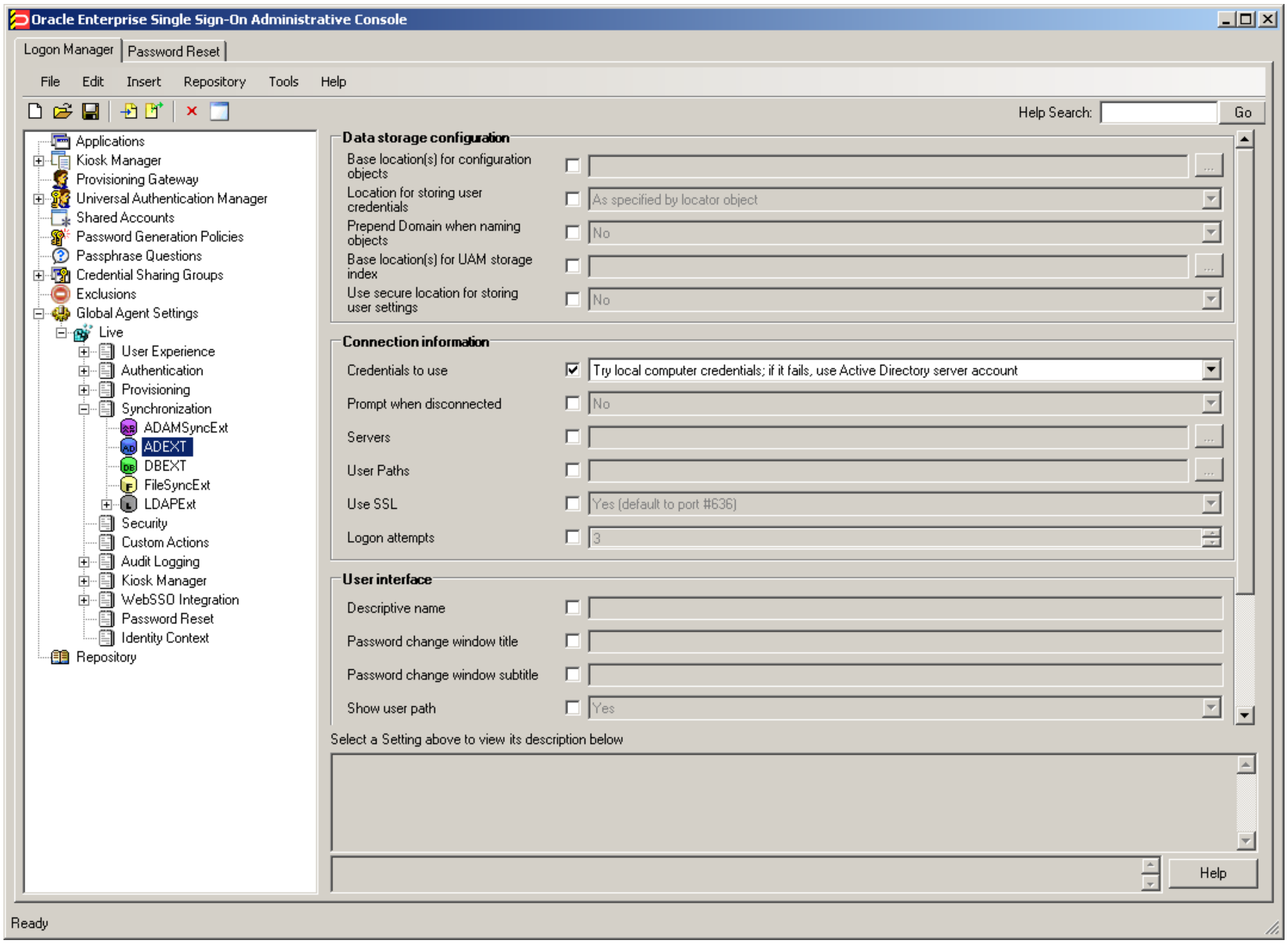
- **Administrative overrides** take precedence over the global Agent settings stored in the Windows registry and constitute the “domain” policy for the Agent. Overrides are downloaded from the central repository by the Agent during synchronization and stored in the Agent’s encrypted and tamper-proof 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 *Logon Manager 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 2 depicts a typical view of the Logon Manager Administrative Console set up for synchronization with Active Directory.



Data storage configuration

Base location(s) for configuration objects □

Location for storing user credentials □ As specified by locator object

Prepend Domain when naming objects □ No

Base location(s) for UAM storage index □

Use secure location for storing user settings □ No

Connection information

Credentials to use ☑ Try local computer credentials; if it fails, use Active Directory server account

Prompt when disconnected □ No

Servers □

User Paths □

Use SSL □ Yes (default to port #636)

Logon attempts □ 3

User interface

Descriptive name □

Password change window title □

Password change window subtitle □

Show user path □ Yes

Select a Setting above to view its description below

Figure 2 The Logon Manager Administrative Console

The next section describes best practices for configuring Logon Manager 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 Logon Manager 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 Logon Manager.

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 *Logon Manager 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 Logon Manager 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 Logon Manager MSI package. (For instructions on creating the package, see the section "Packaging Oracle Enterprise Single Sign-On Suite for Mass Deployment" in the *Enterprise Single Sign-On Suite Installation Guide*.)

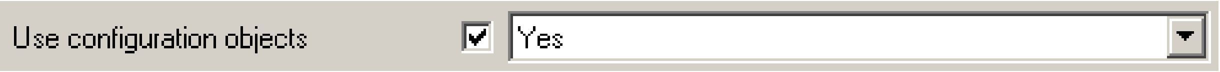
Data Storage Settings

Oracle recommends configuring Logon Manager's data storage settings as described below.

Use Configuration Objects

On Active Directory deployments, Oracle highly recommends that you use 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 Logon Manager Active Directory Sub-Tree. If you disable this feature, Logon Manager will store all template and configuration data as a single flat file under the tree root.

Located in: Global Agent Settings → Live → Synchronization



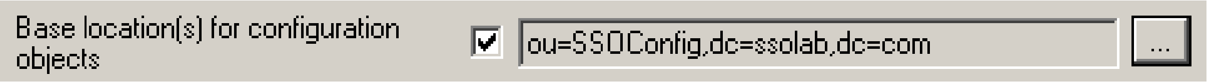
Use configuration objects ☑ Yes

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

Specify the Path to the Logon Manager Configuration Objects

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

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



Base location(s) for configuration objects ☑ ou=SSOConfig,dc=ssolab,dc=com

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

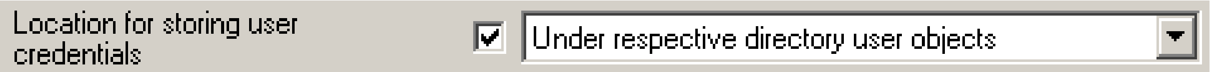
A major benefit of using Logon Manager with Active Directory is the ability to store user credentials under the respective user objects. Doing so simplifies administration as follows:

- 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 Logon Manager.

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 Logon Manager where in the directory to look for templates, credentials, and other objects when using a flat directory model; for more information, see Appendix B: Logon Manager Repository Object Classes and Attributes.)

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



Location for storing user credentials ☑ Under respective directory user objects

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

Repository Connection Settings

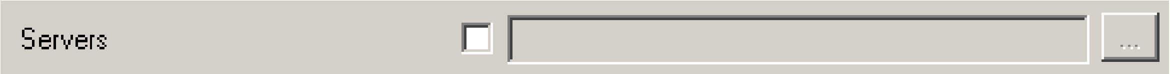
Oracle recommends configuring Logon Manager's repository connection settings as described below.

Note: If users will be synchronizing with the repository from outside of the corporate network, you must allow RPC protocol-based connections through the corporate firewall; otherwise, users will be unable to synchronize with the repository.

Let Logon Manager Find the Nearest Domain Controller

Oracle recommends that you let Logon Manager 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



Servers □

To let Logon Manager find the nearest DC: deselect the check box (default setting).

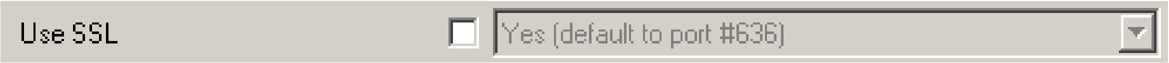
To set: Select the check box, click the (…) button, enter the desired values (one per line) and click **OK**.

SSL Support

Logon Manager repository synchronizers ship with SSL support enabled and Oracle highly recommends that you do not disable it. Your environment should always utilize SSL for all connections to the Logon Manager and other repositories for maximum security.

Note: You must configure your domain controllers to use SSL before deploying Logon Manager. 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



Use SSL □ Yes (default to port #636)

To re-enable (if disabled): Deselect the check box.

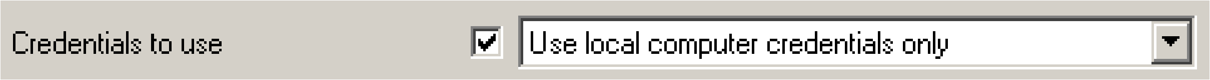
Select the Credentials to Use when Authenticating to the Directory

Use the **Credentials to use** option to select the credentials that Logon Manager 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 Logon Manager 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.

Note: If you are using Smart Cards to authenticate to Logon Manager, you can also use the card's certificate to authenticate to the repository by selecting Use card's certificate from the drop-down menu. For more information, see the *Oracle Enterprise Single Sign-On Suite Administrator's Guide.*

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



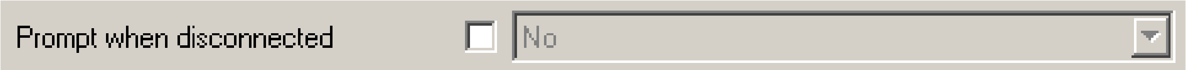
Credentials to use ☑ Use local computer credentials only

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 Logon Manager 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



Prompt when disconnected □ No

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**.

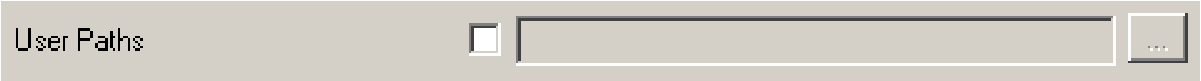
Let Logon Manager Search for User Accounts

Oracle recommends that you let Logon Manager 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 Logon Manager with their Windows password.

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



User Paths □

To let Logon Manager 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**.

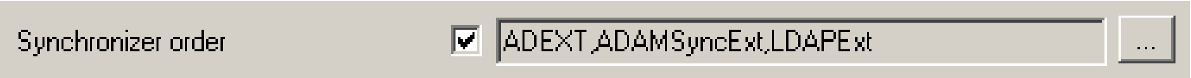
Add the Active Directory Synchronizer to the Synchronizer Order List

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:

- Logon Manager is synchronizing with more than one repository.
- Logon Manager is using roaming synchronization.
- Kiosk Manager is installed in your environment.

> **Note:** Instructions for configuring Logon Manager for multi-repository and roaming synchronization, as well as installing and configuring Logon Manager, are beyond the scope of this guide. For more information, see the *Enterprise Single Sign-On Suite Administrator's Guide*.

Located in: Global Agent Settings → Live → Synchronization



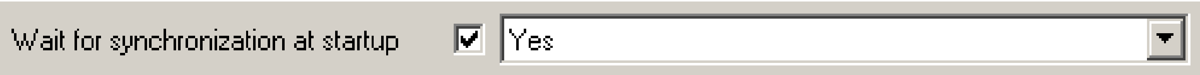
Synchronizer order ☑ ADEXT,ADAMSyncExt,LDAPExt

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 Logon Manager Agent Wait for Synchronization on Startup

To ensure that users always have the most recent credentials, application templates, password policies, and administrative overrides, configure the Agent to wait for synchronization on startup. When this option is enabled, the Agent checks whether the directory is online. 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



Wait for synchronization at startup ☑ Yes

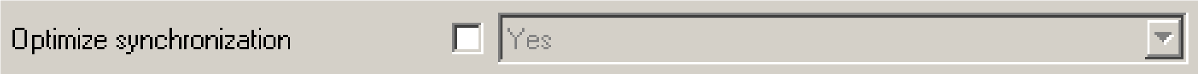
To set: Select the check box, then select **Yes** from the drop-down list.

Use Optimized Synchronization

Optimized synchronization instructs the Logon Manager Agent to synchronize only credentials that have changed since the last synchronization. Do one of the following, depending on your environment:

- Enable this option to improve synchronization performance on deployments with 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



Optimize synchronization □ Yes

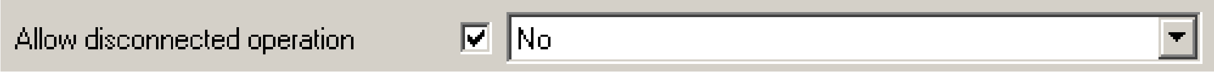
Use the default value (**Yes**) unless your environment requires otherwise.

Restrict Disconnected Operation

During deployment, configure the Logon Manager 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 “Configuring the Logon Manager Agent” section of the *Oracle Enterprise Single Sign-On Suite Administrator’s Guide* for more information on this required best practice.

Located in: Global Agent Settings → Live → Synchronization



Allow disconnected operation ☑ No

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 *Oracle Enterprise Single Sign-On Suite Secure Deployment Guide* and in the “Configuring the Logon Manager Agent” section of the *Oracle Enterprise Single Sign-On Suite Administrator’s Guide*.

Overview of the Deployment Process

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

1. Obtain the following documents:
   - The latest version of this document
   - *Oracle Enterprise Single Sign-On Suite Installation Guide*
   - *Oracle Enterprise Single Sign-On Suite Administrator’s Guide*

2. Install the Logon Manager Agent and the Logon Manager Administrative Console on a machine within your domain, as described in the installation guide for your version of Logon Manager. Make sure you select the Active Directory Synchronizer plug-in when installing the Agent.
3. Complete the steps in Preparing Active Directory for Logon Manager:
   a. Extend the Active Directory schema with Logon Manager 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 Logon Manager 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 Logon Manager Configuration.
   d. Configure the options described in the "Configuring the Logon Manager Agent" section of the *Enterprise Single Sign-On Suite Administrator's Guide*.

> **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 *Packaging Logon Manager for Mass Deployment* section of the *Enterprise Single Sign-On Suite Installation Guide*.
7. Create, test, and deploy the remaining application templates. See the guide *Configuring and Diagnosing Logon Manager Application Templates* for in-depth information on provisioning different types of applications.

Preparing Active Directory for Logon Manager

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

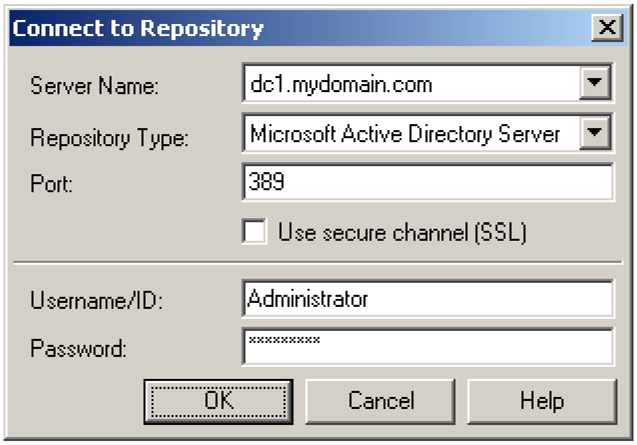
1. Performed a health check on your Active Directory schema. Instructions are provided in the following article: http://www.microsoft.com/technet/opsmgr/2005/library/dirmgmtpack/dirmgmtpackmom_3.mspx
2. Installed the Logon Manager Administrative Console, as described in the *Logon Manager Installation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

Step 1: Extending the Schema

1. Start the Logon Manager Administrative Console. By default, the shortcut to the console is located in **Start → Programs → Oracle → Logon Manager → Logon Manager 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.



Connect to Repository

Server Name: dc1.mydomain.com

Repository Type: Microsoft Active Directory Server

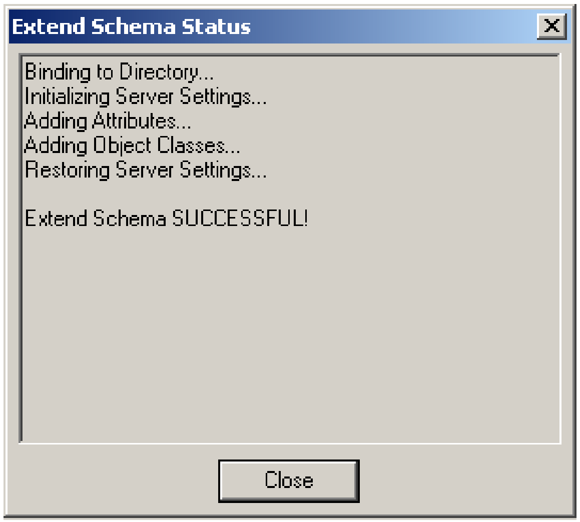
Port: 389

□ Use secure channel (SSL)

Username/ID: Administrator

Password: *********

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 selected; otherwise, deselect it. (See SSL Support for more information.)
7. In the **Username/ID** and **Password** fields, enter the credentials of the account you want Logon Manager 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:



Extend Schema Status

Binding to Directory...
Initializing Server Settings...
Adding Attributes...
Adding Object Classes...
Restoring Server Settings...

Extend Schema SUCCESSFUL!

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

9. Click **Close**.

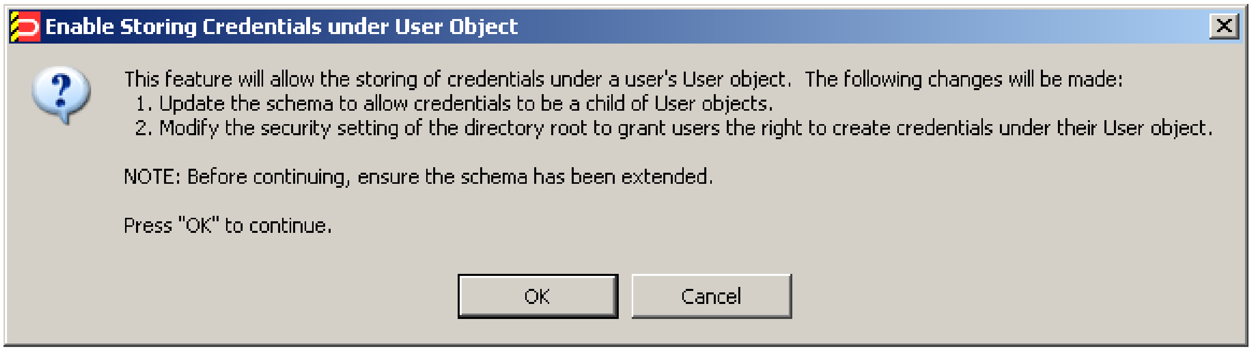
Step 2: Enabling the Storage of User Credentials under User Objects

When you enable the storage of user credentials under respective user objects, Logon Manager 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.



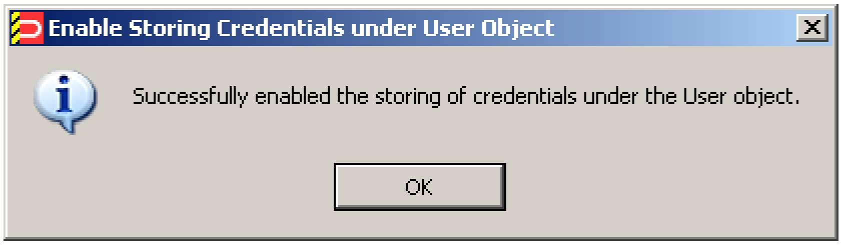
Enable Storing Credentials under User Object

This feature will allow the storing of credentials under a user's User object. The following changes will be made:
1. Update the schema to allow credentials to be a child of User objects.
2. Modify the security setting of the directory root to grant users the right to create credentials under their User object.

NOTE: Before continuing, ensure the schema has been extended.

Press "OK" to continue.

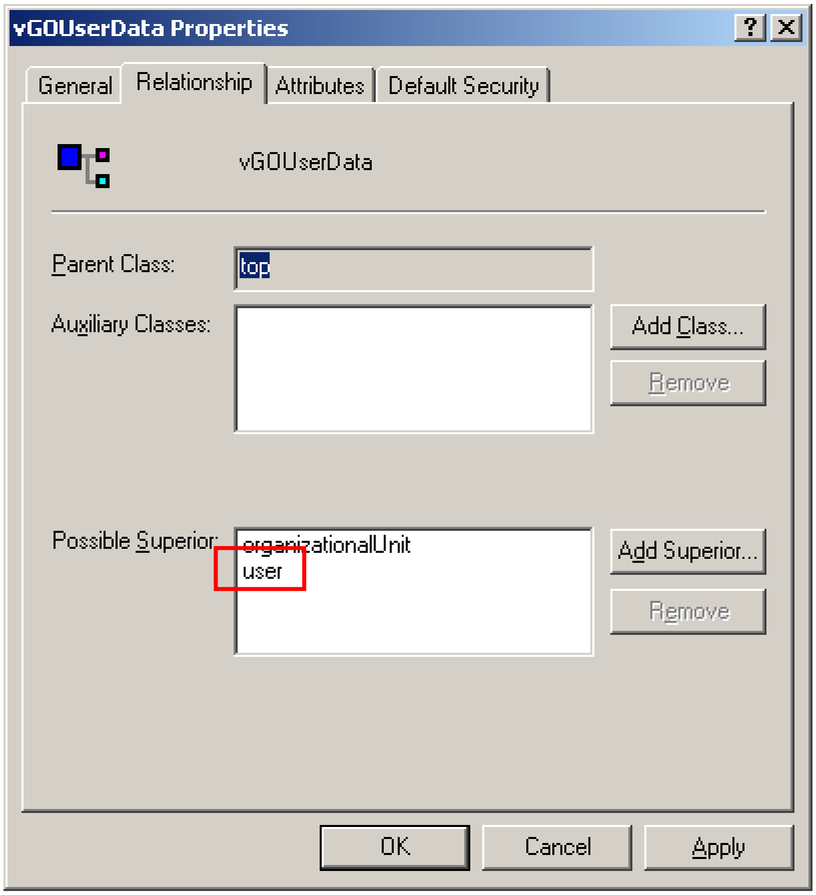
2. Click **OK** and wait for the Console to make the changes. When the changes have been made, the Console displays a confirmation dialog:



Enable Storing Credentials under User Object

Successfully enabled the storing of credentials under the User object.

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:



vGOUserData Properties

vGOUserData

Parent Class: top

Auxiliary Classes:

Possible Superior: organizationalUnit, user

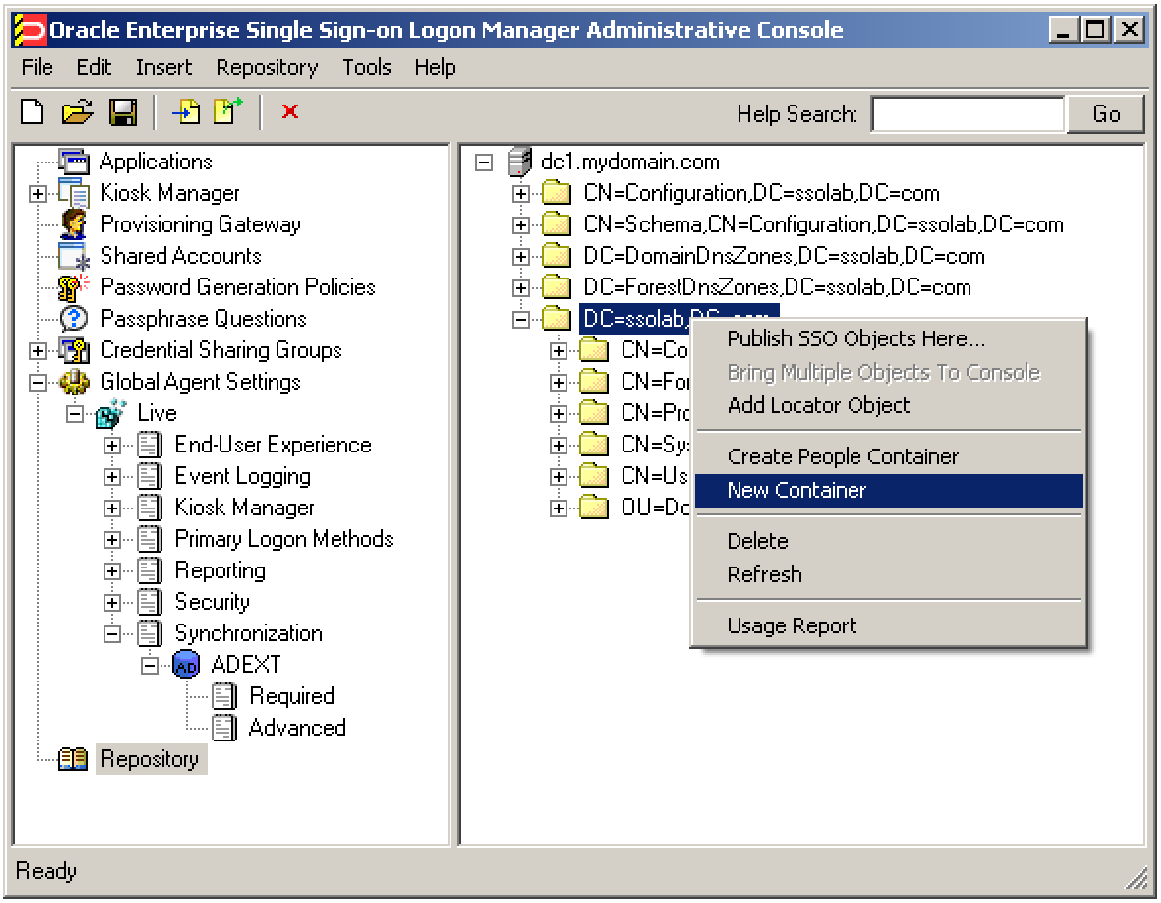
If the user class does not appear as a possible superior, see All Users Unable to Store Credentials under User Objects in Appendix C for possible causes and remedial steps.

> **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.

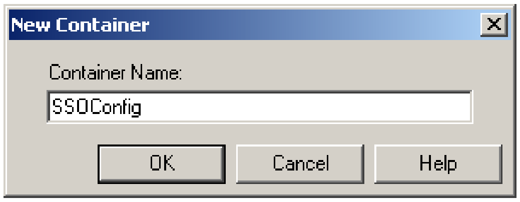
Step 3: Creating the Logon Manager Configuration Object Container and Sub-Tree Structure

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

1. In the Logon Manager 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 Logon Manager, 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 Logon Manager to end-users. Before starting this procedure, make sure that the Logon Manager Administrative Console and the Logon Manager 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 Logon Manager Agent.

> **Note:** If users will be synchronizing with the repository from outside of the corporate network, you must allow RPC protocol-based connections through the corporate firewall; otherwise, users will be unable to synchronize with the repository.

1. Launch the Logon Manager 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.

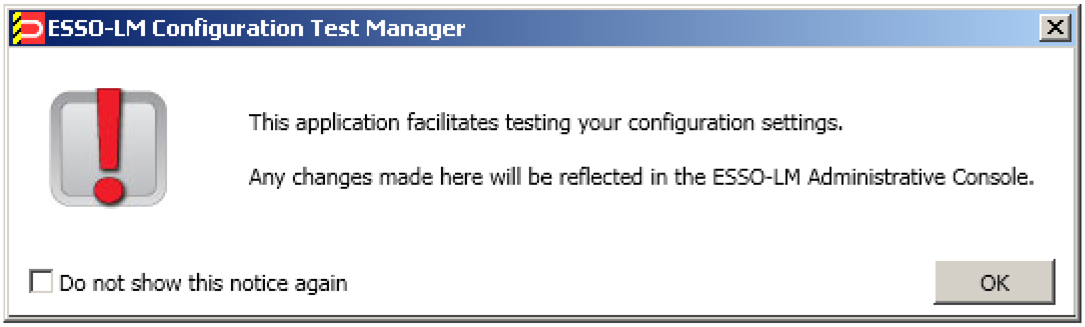
4. Save your configuration to an XML file for future reference. From the **File** menu, select **Save**, enter the desired file name, and click **Save**. If you change your settings, you can load this XML file into the Console to revert back to your original choices.

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 Logon Manager.

Testing the Logon Manager Configuration

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

1. Launch the Logon Manager 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:

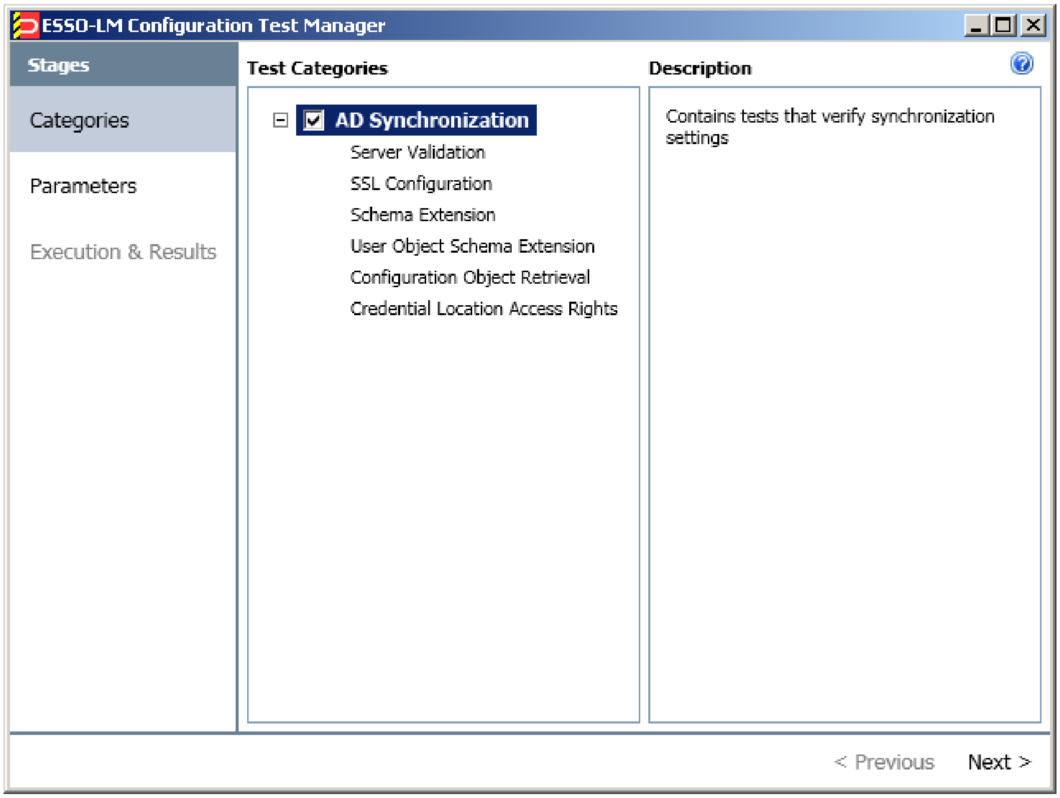


This application facilitates testing your configuration settings.

Any changes made here will be reflected in the ESSO-LM Administrative Console.

☐ Do not show this notice again

5. The “Logon Manager 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.



⊟ ☑ AD Synchronization
- Server Validation
- SSL Configuration
- Schema Extension
- User Object Schema Extension
- Configuration Object Retrieval
- Credential Location Access Rights

Contains tests that verify synchronization settings

Deploying Logon Manager with Microsoft AD LDS (ADAM)

This part describes best practices for deploying Logon Manager with Microsoft AD LDS (ADAM).
It contains the following sections:

Logon Manager and AD LDS (ADAM) Environments

You have the choice to deploy Logon Manager in a directory environment, such as AD LDS (ADAM) 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 Logon Manager to your existing directory environment provides the following benefits:

- Logon Manager 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.
- Logon Manager data is automatically protected by your existing backup and disaster recovery plans.
- No dedicated servers or server-side processes are required; Logon Manager’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 Logon Manager is achieved through the native capabilities of the directory.

A directory also enables the organization of Logon Manager 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 Logon Manager administration by permitting more efficient access control.

Benefits of AD LDS (ADAM)-Based Deployments

AD LDS (ADAM) provides data storage and retrieval for directory-enabled applications, without the dependencies that are required by Active Directory. AD LDS (ADAM) 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 AD LDS (ADAM) is completely independent of the enterprise schema you may be using in an Active Directory domain. You can run multiple instances of AD LDS (ADAM) concurrently on a single server, with an independently managed schema for each AD LDS (ADAM) instance. The following are the benefits of deploying Logon Manager with AD LDS (ADAM):

- **Ideal for pilot and proof-of-concept deployments.** A fully functional AD LDS (ADAM) 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**. AD LDS (ADAM) 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 AD LDS (ADAM) 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 Logon Manager 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 Logon Manager with AD LDS (ADAM) in an existing Active Directory environment provides the following benefits:

- **Retraining is minimized.** Administrative procedures for AD LDS (ADAM) are very similar to those for Active Directory. Administrators skilled with Active Directory will be able to deploy and maintain AD LDS (ADAM) 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 AD LDS (ADAM). You do not need to import, re-create or synchronize your existing configuration and user account data.

Active Directory vs. AD LDS (ADAM)

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

Feature	Active Directory	AD LDS (ADAM)
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 of load balancing, see Load-Balancing a Logon Manager 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 Logon Manager 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 B: Logon Manager Repository Object Classes and Attributes.	**Local**. When deploying Logon Manager on AD LDS (ADAM), you must perform a schema extension against the target AD LDS (ADAM) 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 Logon Manager application credentials under respective user objects.	**No**. All user credentials are stored under a dedicated OU within the AD LDS (ADAM) instance. This OU contains an object for each Logon Manager user.
Usage Reporting	**Yes**. When Logon Manager is deployed on Active Directory, you can obtain point-in-time information on user credentials stored in the directory.	**No**. AD LDS (ADAM) environments do not support point-in-time information reporting for Logon Manager. (Available on AD LDS (ADAM) when Provisioning Gateway is installed.)

For more in-depth information about AD LDS (ADAM) 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 Logon Manager Extends the AD LDS (ADAM) Schema

Before Logon Manager can store data in AD LDS (ADAM), you must extend the schema of the selected AD LDS (ADAM) instance (the Active Directory host's schema is not affected) using the Administrative Console. 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 AD LDS (ADAM) Instance for Logon Manager. 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 Logon Manager, see the following appendices:

- Appendix A: Minimum Administrative Rights for Logon Manager Repository Objects
- Appendix B: Logon Manager Repository Object Classes and Attributes

How Logon Manager Synchronizes with AD LDS (ADAM)

The Logon Manager Agent uses the AD LDS (ADAM) synchronizer plug-in to communicate with AD LDS (ADAM). When properly configured, synchronization occurs whenever one of the following events takes place:

- The Logon Manager 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 Logon Manager 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 Logon Manager Agent traverses the Logon Manager 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 Logon Manager Handles and Stores Application Credentials

Logon Manager 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. Logon Manager 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 Logon Manager stores per enabled application and per user is trivial (measurable in bytes and small kilobytes).

Benefits of Load-Balancing an Logon Manager Deployment

When a directory server fails, Logon Manager 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 AD LDS (ADAM) server, Oracle highly recommends using a load balancer that will evenly and automatically distribute the requests coming from the network among the AD LDS (ADAM) 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.

Further Reading

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

Designing the AD LDS (ADAM) Directory Sub-Tree

Logon Manager 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 Logon Manager will support
- Robustness of the existing infrastructure
- Structure of your organization.

Guidelines for Structuring the AD LDS (ADAM) Sub-Tree for Logon Manager

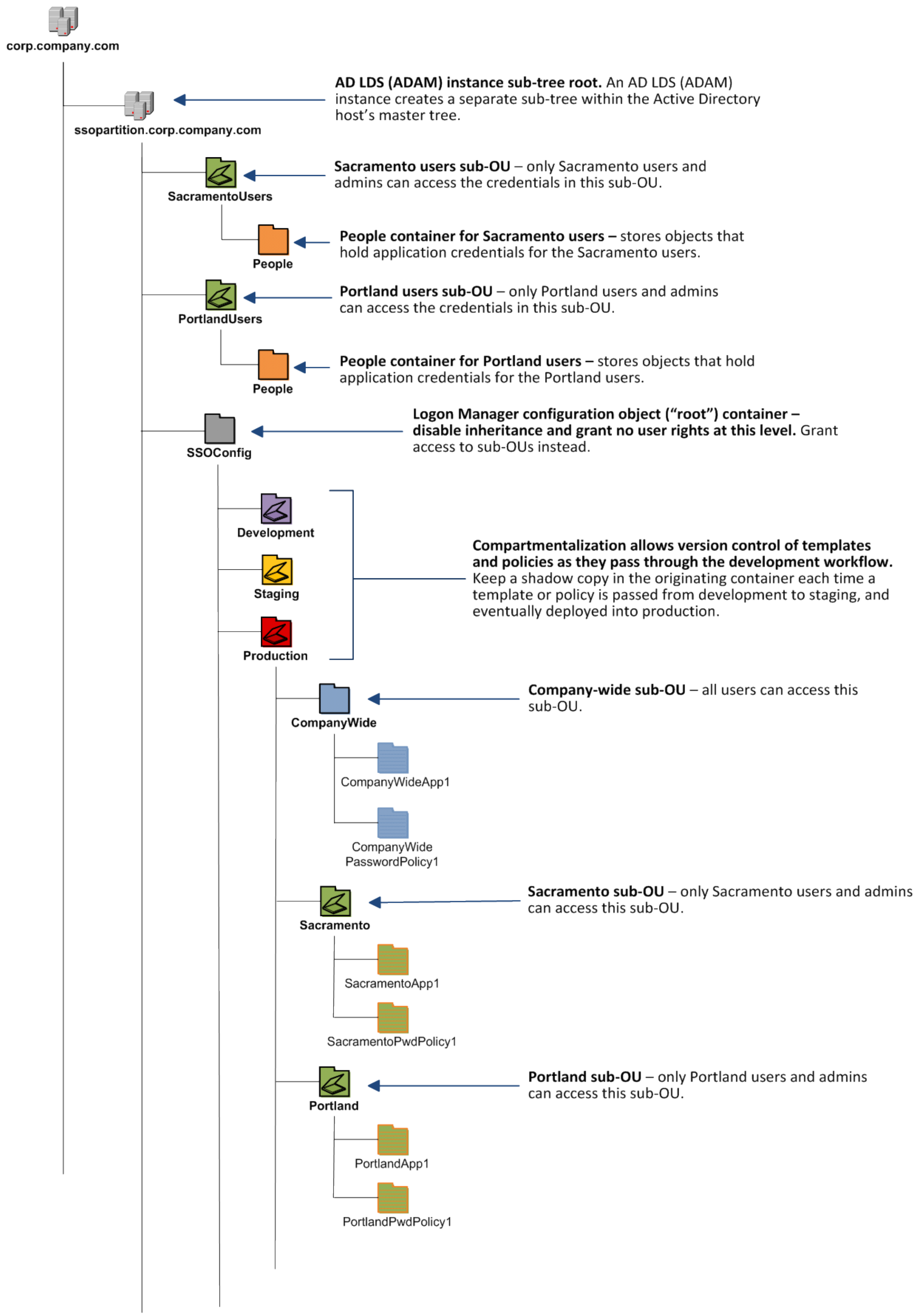
Oracle recommends that you set up your sub-tree as a hierarchy by following the guidelines below:

- Use OUs to group templates, policies, and credentials 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 Logon Manager 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 Logon Manager Administrative Console; controlling access at the OU level is achieved via delegated administration using Microsoft and third-party management tools.

Figure 3 depicts a sample Logon Manager sub-tree whose design reflects the above best practices.



AD LDS (ADAM) instance sub-tree root. An AD LDS (ADAM) instance creates a separate sub-tree within the Active Directory host's master tree.

Sacramento users sub-OU – only Sacramento users and admins can access the credentials in this sub-OU.

People container for Sacramento users – stores objects that hold application credentials for the Sacramento users.

Portland users sub-OU – only Portland users and admins can access the credentials in this sub-OU.

People container for Portland users – stores objects that hold application credentials for the Portland users.

Logon Manager configuration object ("root") container – disable inheritance and grant no user rights at this level. Grant access to sub-OUs instead.

Compartmentalization allows version control of templates and policies as they pass through the development workflow. Keep a shadow copy in the originating container each time a template or policy is passed from development to staging, and eventually deployed into production.

Company-wide sub-OU – all users can access this sub-OU.

Sacramento sub-OU – only Sacramento users and admins can access this sub-OU.

Portland sub-OU – only Portland users and admins can access this sub-OU.

Figure 3 Recommended Logon Manager 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: Oracle highly recommends that you store templates, policies, and application credentials in individual OUs. To do this, you must enable the use of configuration objects.

Unlike Active Directory, AD LDS (ADAM) does not permit Logon Manager to store application credentials under user objects. Instead, when deployed on AD LDS (ADAM), Logon Manager stores application credentials in a flat format inside a special OU called `People`. The `People` container, by default, resides in the root of your AD LDS (ADAM) partition; however, if you require more granular access control, you can create multiple `People` containers (each must have a unique path) for different departments or regions within your organization, just like you would for templates and policies, as shown in Figure 3. You would then configure each department's Logon Manger instances to seek application credentials in that department's `People` OU. You must create the `People` OU and provide its full path to the AD LDS (ADAM) synchronizer as described in Creating the People OU.

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

If you are using Provisioning Gateway and want to take advantage of multiple People OUs, the following limitations apply:

- The `People` OU must reside inside a parent container at the root of the AD LDS (ADAM) partition,
- The parent container's name must be the name of the domain (NT-style) of the users whose application credentials are stored in the corresponding `People` OU. If necessary, create a separate domain for each department or region that requires a separate `People` OU and move the corresponding users to that domain.

Note: It is not possible to use multiple `People` OUs with Provisioning Gateway with a single domain.

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 Logon Manager 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 3. 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 Logon Manager 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 AD LDS (ADAM) 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 Logon Manager, 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 Logon Manager Agent, including its interaction with the directory, is governed by settings configured and deployed to the end-user machine by the Logon Manager administrator using the Logon Manager Administrative Console. The settings fall into one of the following categories:

- **Global Agent settings** are the "local policy" for the Agent**;** they are stored in the Windows registry on the end-user machine and are included in the Logon Manager MSI package to provide the Agent with an initial configuration during deployment. Global Agent settings are stored in `HKEY_LOCAL_MACHINE\Software\Passlogix` (32-bit systems) or `HKEY_LOCAL_MACHINE\Wow6432Node\Software\Passlogix` (64-bit systems).

  > **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**.

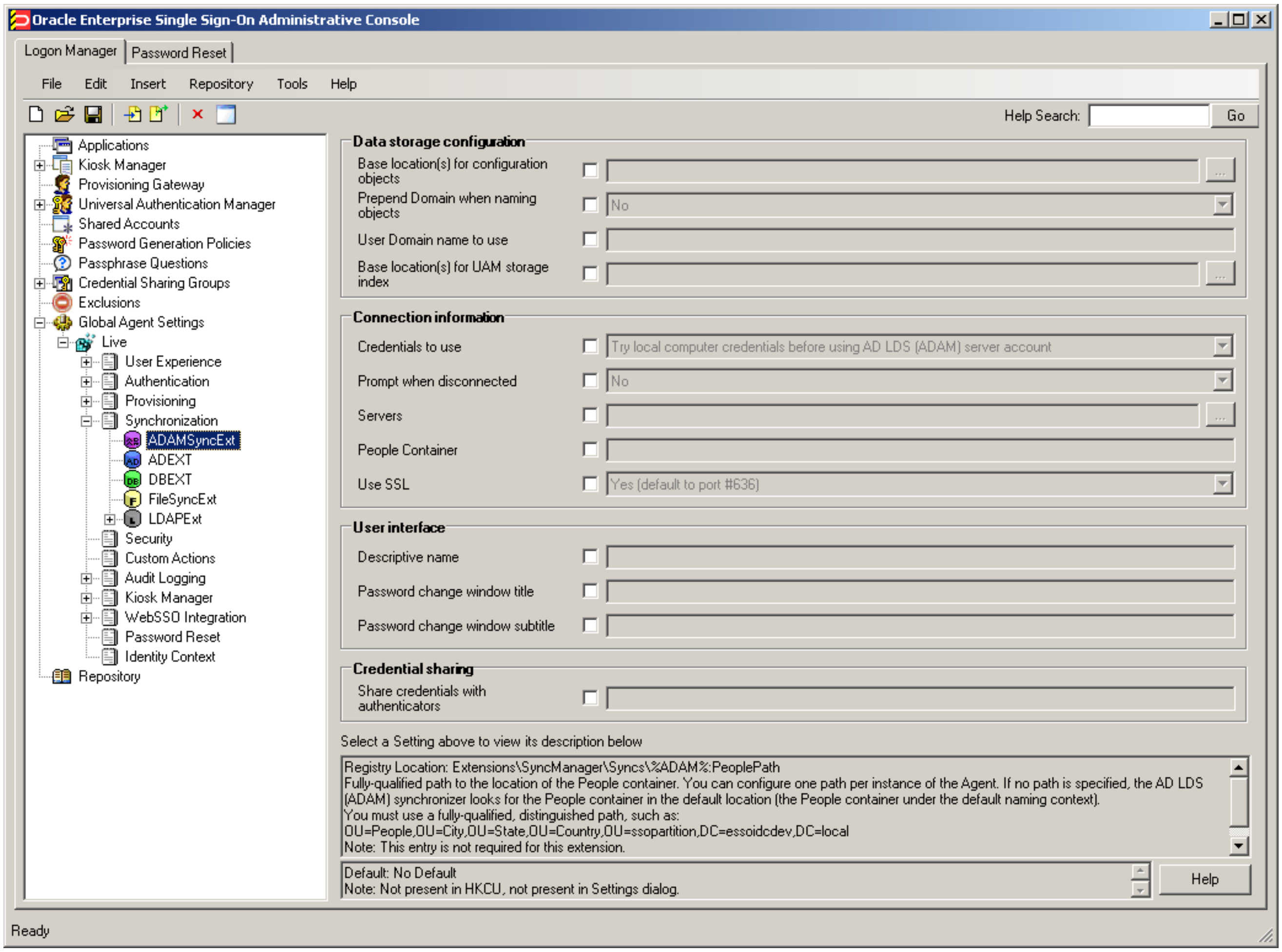
- **Administrative overrides** take precedence over the global Agent settings stored in the Windows registry and constitute the "domain" policy for the Agent. Overrides are downloaded from the central repository by the Agent during synchronization and stored in the Agent's encrypted and tamper-proof 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 *Logon Manager 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 4 depicts a typical view of the Logon Manager Administrative Console set up for synchronization with AD LDS (ADAM).



Data storage configuration

- Base location(s) for configuration objects □
- Prepend Domain when naming objects □ No
- User Domain name to use □
- Base location(s) for UAM storage index □

Connection information

- Credentials to use □ Try local computer credentials before using AD LDS (ADAM) server account
- Prompt when disconnected □ No
- Servers □
- People Container □
- Use SSL □ Yes (default to port #636)

User interface

- Descriptive name □
- Password change window title □
- Password change window subtitle □

Credential sharing

- Share credentials with authenticators □

Select a Setting above to view its description below

Registry Location: Extensions\SyncManager\Syncs\%ADAM%:PeoplePath
Fully-qualified path to the location of the People container. You can configure one path per instance of the Agent. If no path is specified, the AD LDS (ADAM) synchronizer looks for the People container in the default location (the People container under the default naming context).
You must use a fully-qualified, distinguished path, such as:
OU=People,OU=City,OU=State,OU=Country,OU=ssopartition,DC=essoidcdev,DC=local
Note: This entry is not required for this extension.

Default: No Default
Note: Not present in HKCU, not present in Settings dialog.

Figure 4 The Logon Manager Administrative Console

The next section describes best practices for configuring Logon Manager for synchronization with AD LDS (ADAM). 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 Logon Manager Agent and the AD LDS (ADAM) synchronizer plug-in are installed on your machine; otherwise, AD LDS (ADAM)-related settings will not be displayed in the Console. For installation instructions, see the installation guide for your version of Logon Manager.

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 *Logon Manager 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 Logon Manager Administrative Console is *not* checked. The value is visible in the inactive field next to the check box.

Recommended Global Agent Settings

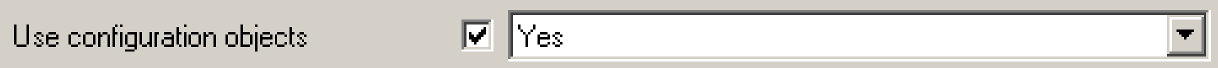
This section lists Oracle-recommended best-practice global Agent settings. Configure the settings as described below and include them in the customized Logon Manager MSI package. (For instructions on creating the package, see the section "Packaging Oracle Enterprise Single Sign-On Suite for Mass Deployment" in the *Enterprise Single Sign-On Suite Installation Guide*.)

Note: If users will be synchronizing with the repository from outside of the corporate network, you must allow RPC protocol-based connections through the corporate firewall; otherwise, users will be unable to synchronize with the repository.

Use Configuration Objects

On AD LDS (ADAM) deployments Oracle highly recommends that you use 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 AD LDS (ADAM) Directory Sub-Tree. If you disable this feature, Logon Manager will store all template and configuration data as a single flat file under the tree root.

Located in: Global Agent Settings → Live → Synchronization



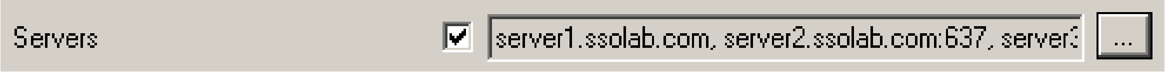
Use configuration objects ☑ Yes ▼

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

Configure a Server List with Desired Failover Order

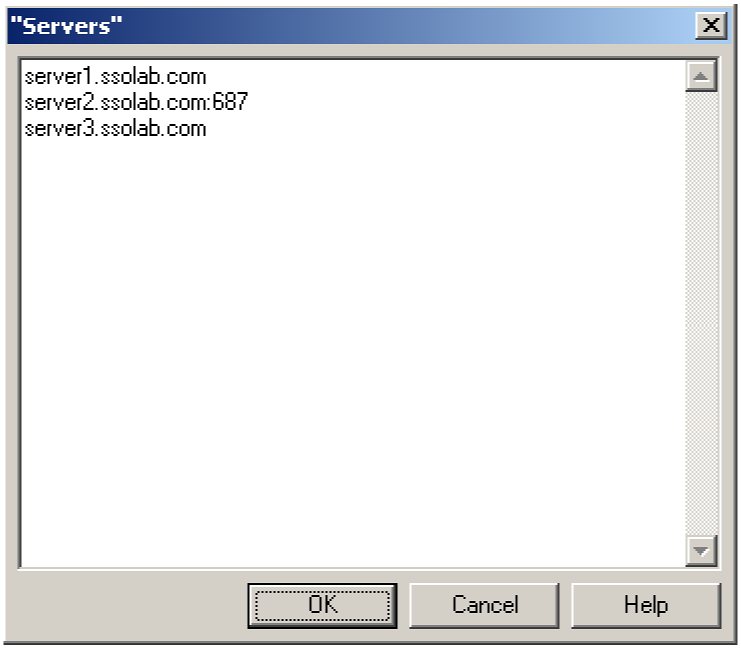
In AD LDS (ADAM) environments, server URLs must be explicitly provided to Logon Manager. Oracle highly recommends using at least two physical AD LDS (ADAM) servers and placing them behind a load balancer for automatic, transparent failover. If you choose not to use a load balancer, arrange the server 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 a Logon Manager Deployment.

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



Servers ☑ server1.ssolab.com, server2.ssolab.com:637, server3

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**.

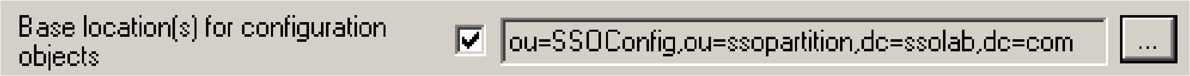


```
server1.ssolab.com
server2.ssolab.com:687
server3.ssolab.com
```

Specify the Path to the Logon Manager Configuration Objects

You must specify the location of the Logon Manager root container (which stores Logon Manager configuration objects) for Logon Manager to store data in AD LDS (ADAM).

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



Base location(s) for configuration objects ☑ ou=SSOConfig,ou=ssopartition,dc=ssolab,dc=com

To set: Select the check box, click the (…) button, and enter the desired value.

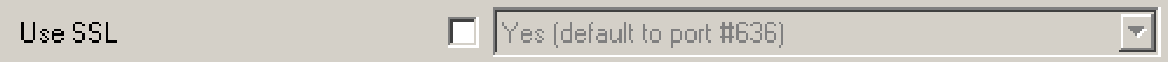
When you are finished, click **OK**.

SSL Support

Logon Manager repository synchronizers ship with SSL support enabled and Oracle highly recommends that you do not disable it. Your environment should always utilize SSL for all connections to the Logon Manager and other repositories for maximum security.

Note: You must configure your domain controllers to use SSL before deploying Logon Manager. 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 → ADAMSyncExt



Use SSL □ Yes (default to port #636)

To re-enable (if disabled): Deselect the check box.

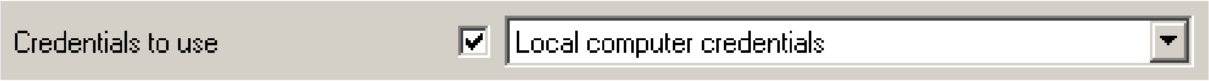
Select the Credentials to Use when Authenticating to the Repository

Use the **Credentials to use** option to select the credentials Logon Manager 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 Logon Manager is unable to authenticate to the repository.

Note: Do **not** leave this at the default setting, **Try local computer credentials before using AD LDS (ADAM) 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.

Note: If you are using Smart Cards to authenticate to Logon Manager, you can also use the card's certificate to authenticate to the repository by selecting Use card's certificate from the drop-down menu. For more information, see the *Oracle Enterprise Single Sign-On Suite Administrator's Guide.*

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



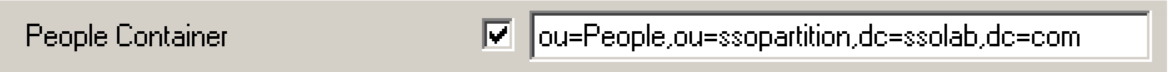
Credentials to use ☑ Local computer credentials

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

Configure Logon Manager to Use a Specific People OU

If you created a People OU in a location other than default (root of the AD LDS (ADAM) partition), or you have created multiple People OUs for more granular control of access to application credentials, you must configure the target Logon Manager instances to use the corresponding People OUs, as explained in Designing the AD LDS (ADAM) Directory Sub-Tree.

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



People Container ☑ ou=People,ou=ssopartition,dc=ssolab,dc=com

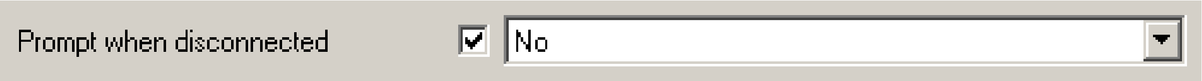
To set: select the check box next to the **People container** option and enter the fully qualified path to the specific `People` OU you want Logon Manager to use into the field. For example:

```
OU=People,OU=City,OU=State,OU=Country,OU=ssopartition,DC=company,DC=com
```

Choose Whether to Prompt the User when Disconnected from the Repository

Use the **Prompt when disconnected** option to decide whether Logon Manager 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



Prompt when disconnected ☑ No

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**.

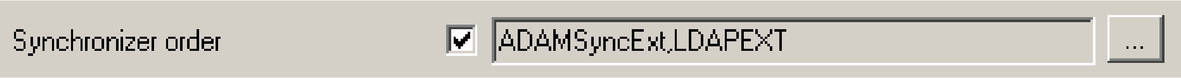
Add the AD LDS (ADAM) Synchronizer to the Synchronizer Order List

Ensure that the AD LDS (ADAM) (`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:

- Logon Manager is synchronizing with more than one repository,
- Logon Manager is using roaming synchronization,
- Kiosk Manager is installed in your environment.

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

Located in: Global Agent Settings → Synchronization



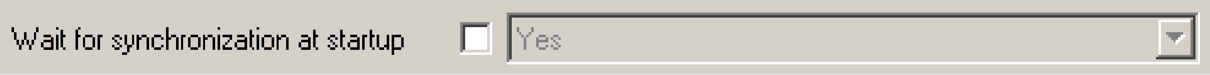
Synchronizer order ☑ ADAMSyncExt,LDAPEXT

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 Logon Manager Agent Wait for Synchronization on Startup

To ensure that users always have the most recent credentials, application templates, password policies, and administrative overrides, configure the Agent to wait for synchronization on startup. When this option is enabled, the Agent checks whether the directory is online. 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



Wait for synchronization at startup □ Yes

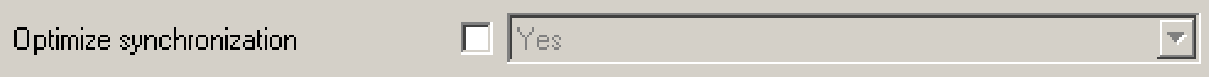
Use the default value (**Yes**) unless your environment requires otherwise.

Use Optimized Synchronization

Optimized synchronization instructs the Logon Manager Agent to synchronize only credentials that have changed since the last synchronization. Do one of the following, depending on your environment:

- Enable this option to improve synchronization performance on deployments with 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



Optimize synchronization □ Yes

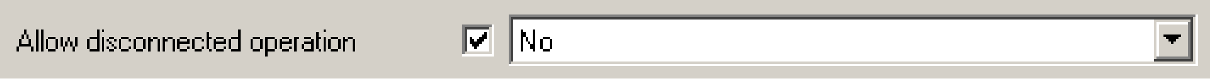
Use the default value (**Yes**) unless your environment requires otherwise.

Restrict Disconnected Operation

During deployment, configure the Logon Manager 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 *Logon Manager Best Practices: Configuring the Logon Manager Agent* for more information on this required best practice.

Located in: Global Agent Settings → Live → Synchronization



Allow disconnected operation ☑ No

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 *Oracle Enterprise Single Sign-On Suite Secure Deployment Guide* and in the "Configuring the Logon Manager Agent" section of the *Oracle Enterprise Single Sign-On Suite Administrator's Guide*.

Overview of the Deployment Process

This section provides a brief high-level overview of the Logon Manager deployment process on AD LDS (ADAM). Make sure you have read all of the preceding sections of this document before proceeding with deployment. Deploying Logon Manager with MS AD LDS (ADAM) requires you to:

1. Obtain the following documents:
   - The latest version of this document
   - *Oracle Enterprise Single Sign-On Suite Installation Guide*
   - *Oracle Enterprise Single Sign-On Suite Administrator's Guide*
2. If you have not already done so, install AD LDS (ADAM) on the target server. The AD LDS (ADAM) installer and installation instructions are available on the Microsoft Web site.
3. Create groups for Logon Manager administrators and Logon Manager users. Basic instructions are provided in Appendix E: Creating the Required User Groups on AD LDS (ADAM) Deployments.
4. Create a new AD LDS (ADAM) instance that will be used by Logon Manager, as described in Creating an AD LDS (ADAM) Instance.
5. Install the Logon Manager Agent and the Logon Manager Administrative Console on a machine within your domain, as described in the installation guide for your version of Logon Manager. Make sure you select the AD LDS (ADAM) Synchronizer when installing the Agent.
6. Complete the steps in Preparing the AD LDS (ADAM) Instance for Logon Manager:
   a. Extend the AD LDS (ADAM) instance schema with Logon Manager classes and attributes.
   b. Create the `People` OU, which will store each user's application credentials.
   c. Create the Logon Manager configuration object container and desired tree structure.
   d. Grant the required permissions.
7. Configure Logon Manager as follows:
   a. Complete the steps in Configuring the AD LDS (ADAM) Synchronizer.
   b. Configure the options described in Recommended Global Agent Settings in this guide.
   c. Test your configuration as described in Testing the Logon Manager Configuration.
   d. Configure the options described in the "Configuring the Logon Manager Agent" section of the *Enterprise Single Sign-On Suite Administrator's Guide*.

> **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 *Packaging Logon Manager for Mass Deployment* section of the *Enterprise Single Sign-On Suite Installation Guide*.
10. Create, test, and deploy the remaining application templates. See the guide *Configuring and Diagnosing Logon Manager Application Templates* for in-depth information on provisioning different types of applications.

Creating an AD LDS (ADAM) Instance

This section describes how to create an AD LDS (ADAM) instance on which you will deploy Logon Manager. If you have not already done so, install AD LDS (ADAM) on the target server. The AD LDS (ADAM) 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. (AD LDS (ADAM) does not support Windows 2000). Deployment on Windows XP or Windows 7 is discouraged.
- To simplify deployment, Oracle highly recommends creating an AD LDS (ADAM) instance that runs on the default port (636 for SSL connections; non-SSL connections to AD LDS (ADAM) are supported but not recommended). 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 AD LDS (ADAM) 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 Logon Manager on a member server instead of a domain controller.

To create the target AD LDS (ADAM) instance:

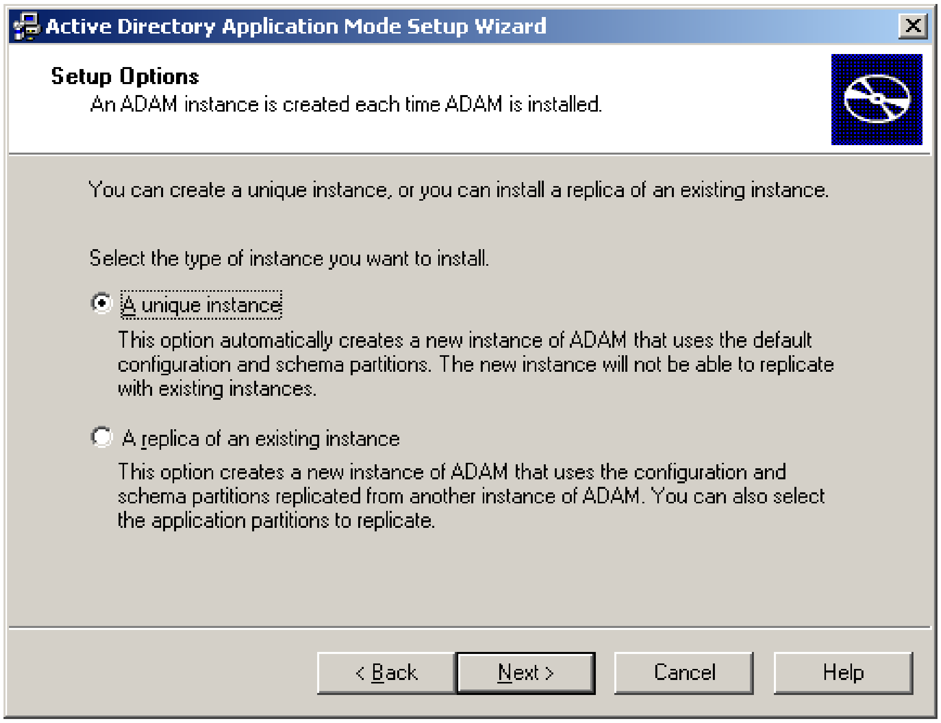
> **Note:** The AD LDS (ADAM) setup wizard screens depicted in this guide may differ visually across the supported versions of the Windows Server operating system family; however, the procedure is identical for all supported versions.

1. Launch the AD LDS (ADAM) 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**.



Setup Options

An ADAM instance is created each time ADAM is installed.

You can create a unique instance, or you can install a replica of an existing instance.

Select the type of instance you want to install.

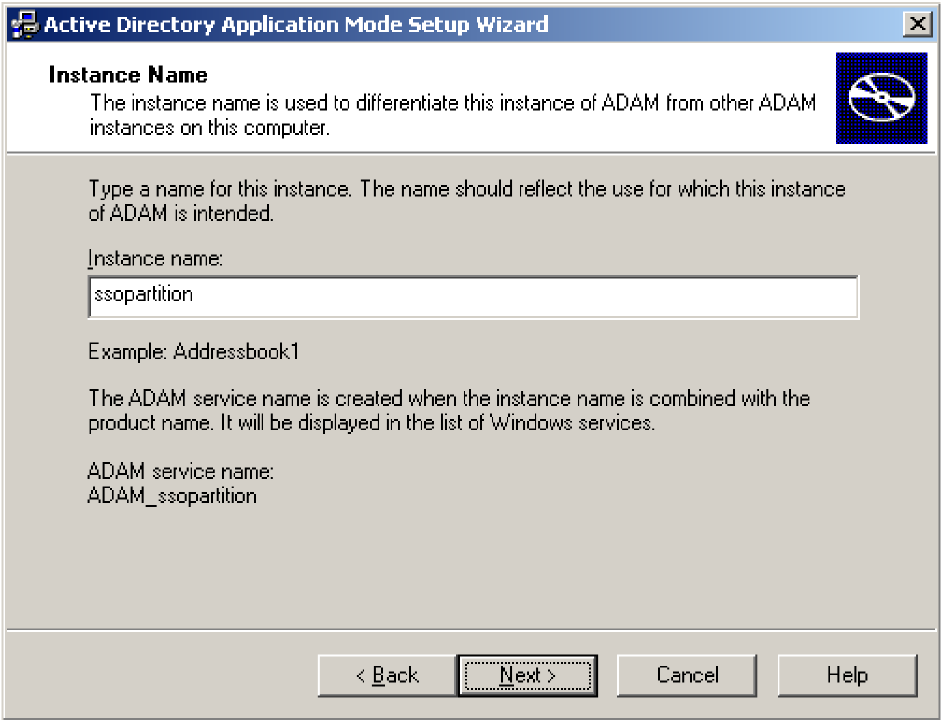
● A unique instance

This option automatically creates a new instance of ADAM that uses the default configuration and schema partitions. The new instance will not be able to replicate with existing instances.

○ A replica of an existing instance

This option creates a new instance of ADAM that uses the configuration and schema partitions replicated from another instance of ADAM. You can also select the application partitions to replicate.

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



Instance Name

The instance name is used to differentiate this instance of ADAM from other ADAM instances on this computer.

Type a name for this instance. The name should reflect the use for which this instance of ADAM is intended.

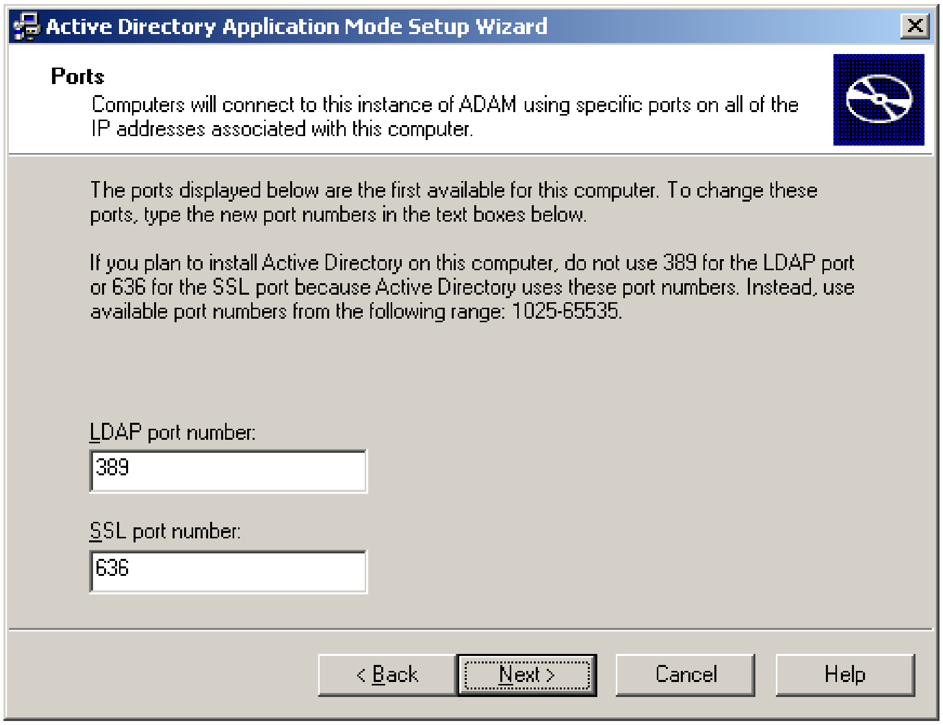
Instance name: ssopartition

Example: Addressbook1

The ADAM service name is created when the instance name is combined with the product name. It will be displayed in the list of Windows services.

ADAM service name:
ADAM_ssopartition

5. Enter the desired port numbers for this AD LDS (ADAM) 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 Logon Manager.



Active Directory Application Mode Setup Wizard

Ports

Computers will connect to this instance of ADAM using specific ports on all of the IP addresses associated with this computer.

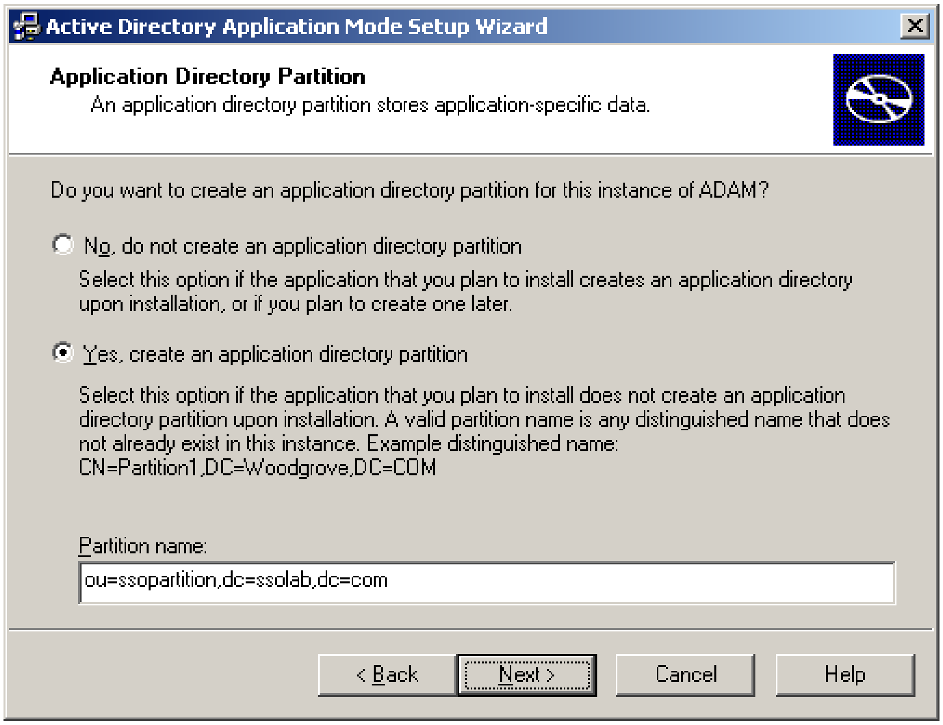
The ports displayed below are the first available for this computer. To change these ports, type the new port numbers in the text boxes below.

If you plan to install Active Directory on this computer, do not use 389 for the LDAP port or 636 for the SSL port because Active Directory uses these port numbers. Instead, use available port numbers from the following range: 1025-65535.

LDAP port number: 389

SSL port number: 636

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



Active Directory Application Mode Setup Wizard

Application Directory Partition

An application directory partition stores application-specific data.

Do you want to create an application directory partition for this instance of ADAM?

○ No, do not create an application directory partition

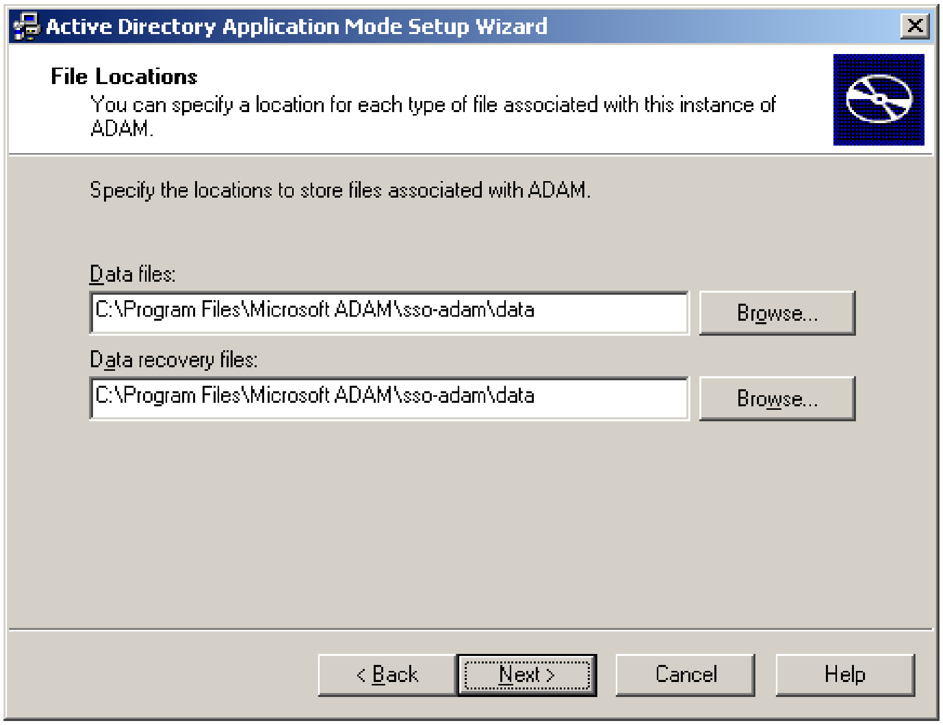
Select this option if the application that you plan to install creates an application directory upon installation, or if you plan to create one later.

● Yes, create an application directory partition

Select this option if the application that you plan to install does not create an application directory partition upon installation. A valid partition name is any distinguished name that does not already exist in this instance. Example distinguished name:
CN=Partition1,DC=Woodgrove,DC=COM

Partition name: ou=ssopartition,dc=ssolab,dc=com

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



Active Directory Application Mode Setup Wizard

File Locations

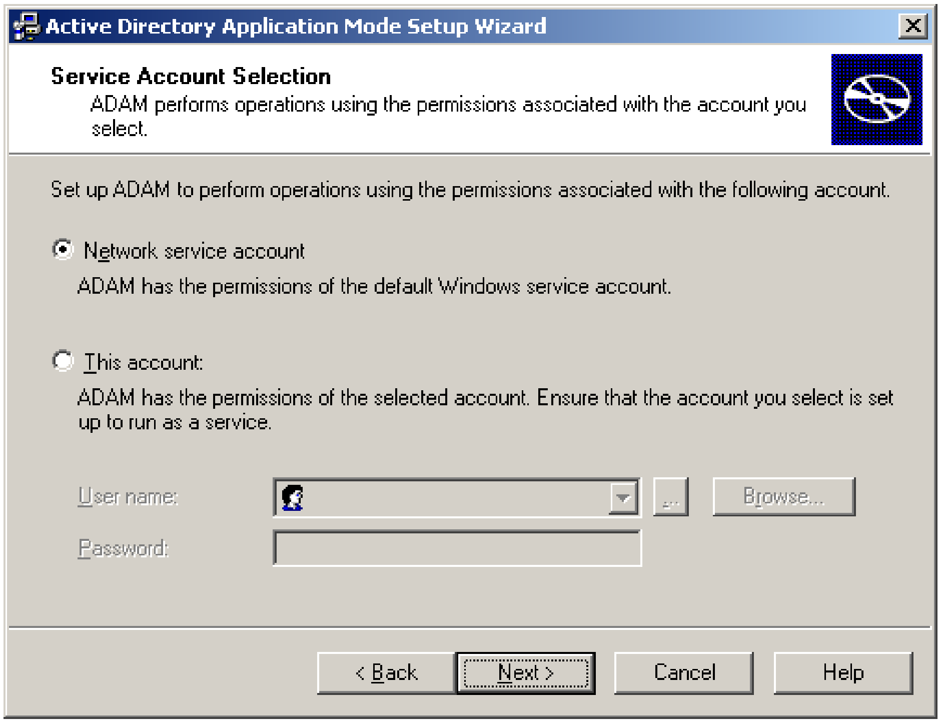
You can specify a location for each type of file associated with this instance of ADAM.

Specify the locations to store files associated with ADAM.

Data files: C:\Program Files\Microsoft ADAM\sso-adam\data

Data recovery files: C:\Program Files\Microsoft ADAM\sso-adam\data

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



Active Directory Application Mode Setup Wizard

Service Account Selection

ADAM performs operations using the permissions associated with the account you select.

Set up ADAM to perform operations using the permissions associated with the following account.

● Network service account

ADAM has the permissions of the default Windows service account.

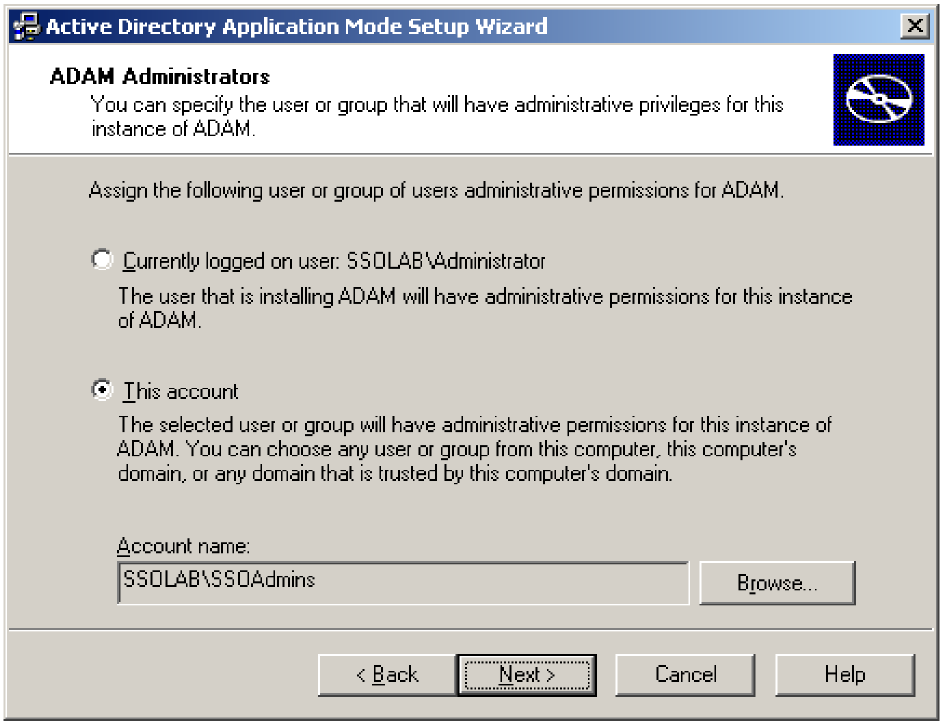
○ This account:

ADAM has the permissions of the selected account. Ensure that the account you select is set up to run as a service.

User name:

Password:

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



Active Directory Application Mode Setup Wizard

ADAM Administrators

You can specify the user or group that will have administrative privileges for this instance of ADAM.

Assign the following user or group of users administrative permissions for ADAM.

○ Currently logged on user: SSOLAB\Administrator

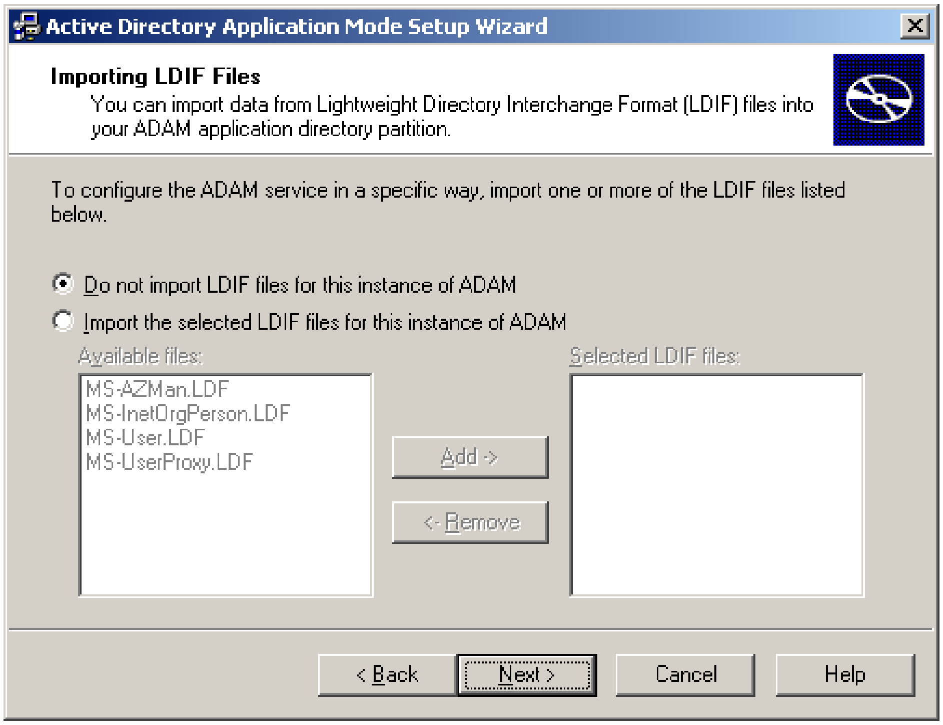
The user that is installing ADAM will have administrative permissions for this instance of ADAM.

● This account

The selected user or group will have administrative permissions for this instance of ADAM. You can choose any user or group from this computer, this computer's domain, or any domain that is trusted by this computer's domain.

Account name: SSOLAB\SSOAdmins

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



Active Directory Application Mode Setup Wizard

Importing LDIF Files

You can import data from Lightweight Directory Interchange Format (LDIF) files into your ADAM application directory partition.

To configure the ADAM service in a specific way, import one or more of the LDIF files listed below.

● Do not import LDIF files for this instance of ADAM

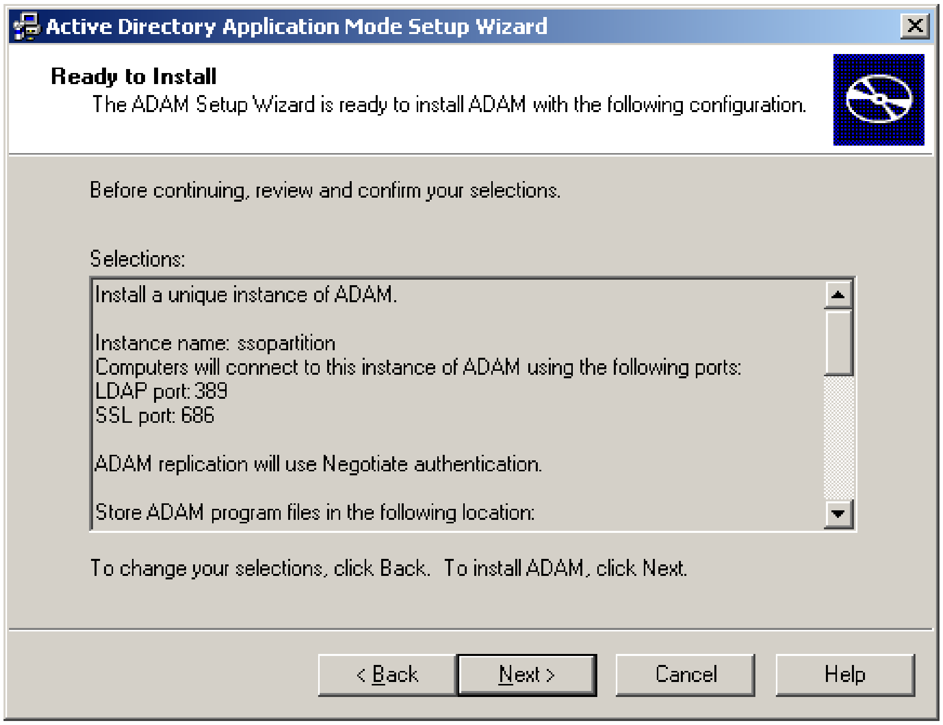
○ Import the selected LDIF files for this instance of ADAM

Available files:

MS-AZMan.LDF
MS-InetOrgPerson.LDF
MS-User.LDF
MS-UserProxy.LDF

Selected LDIF files:

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



Active Directory Application Mode Setup Wizard

Ready to Install

The ADAM Setup Wizard is ready to install ADAM with the following configuration.

Before continuing, review and confirm your selections.

Selections:

Install a unique instance of ADAM.

Instance name: ssopartition
Computers will connect to this instance of ADAM using the following ports:
LDAP port: 389
SSL port: 686

ADAM replication will use Negotiate authentication.

Store ADAM program files in the following location:

To change your selections, click Back. To install ADAM, click Next.

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

Preparing the AD LDS (ADAM) Instance for Logon Manager

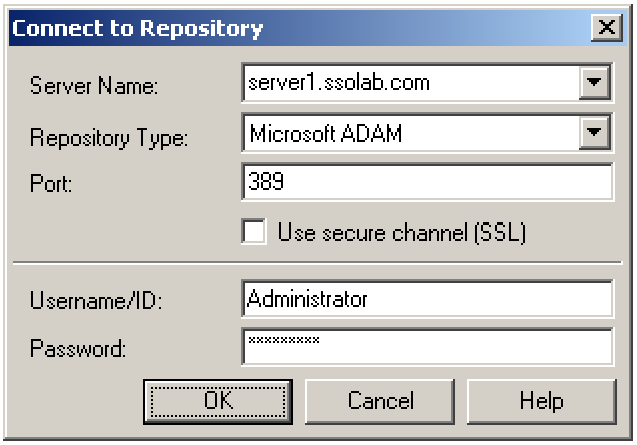
This section describes the basic procedures for preparing AD LDS (ADAM) for use with Logon Manager. The preparation consists of extending your AD LDS (ADAM) schema with Logon Manager classes and attributes, allowing Logon Manager to store credentials under respective user objects, and creating the desired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

Step 1: Extending the Schema

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

> **Note:** In a development or staging environment, disable the option **Check for publisher's certificate revocation** in Internet Explorer to eliminate a delay when the 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.



Connect to Repository

Server Name: server1.ssolab.com

Repository Type: Microsoft ADAM

Port: 389

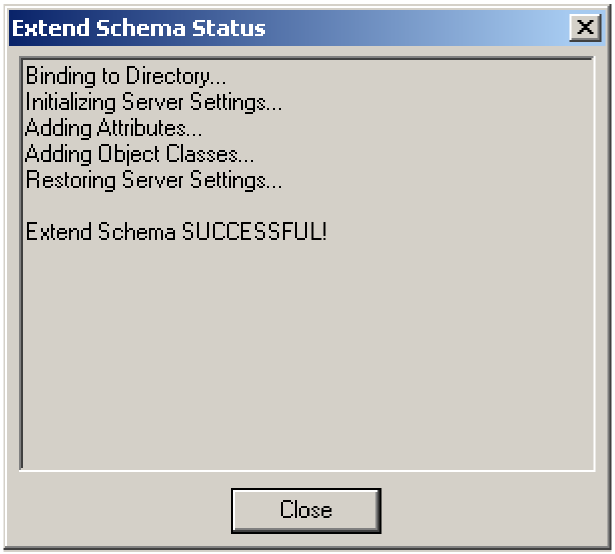
☐ Use secure channel (SSL)

Username/ID: Administrator

Password: **********

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 AD LDS (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 domain controllers to use SSL, leave the **Use secure channel (SSL)** option selected; otherwise, deselect it. (See SSL Support for more information.)

7. In the **Username/ID** and **Password** fields, enter the credentials of the account you want Logon Manager to use to connect to AD LDS (ADAM). 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:



```
Binding to Directory...
Initializing Server Settings...
Adding Attributes...
Adding Object Classes...
Restoring Server Settings...

Extend Schema SUCCESSFUL!
```

9. Click **Close**.

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

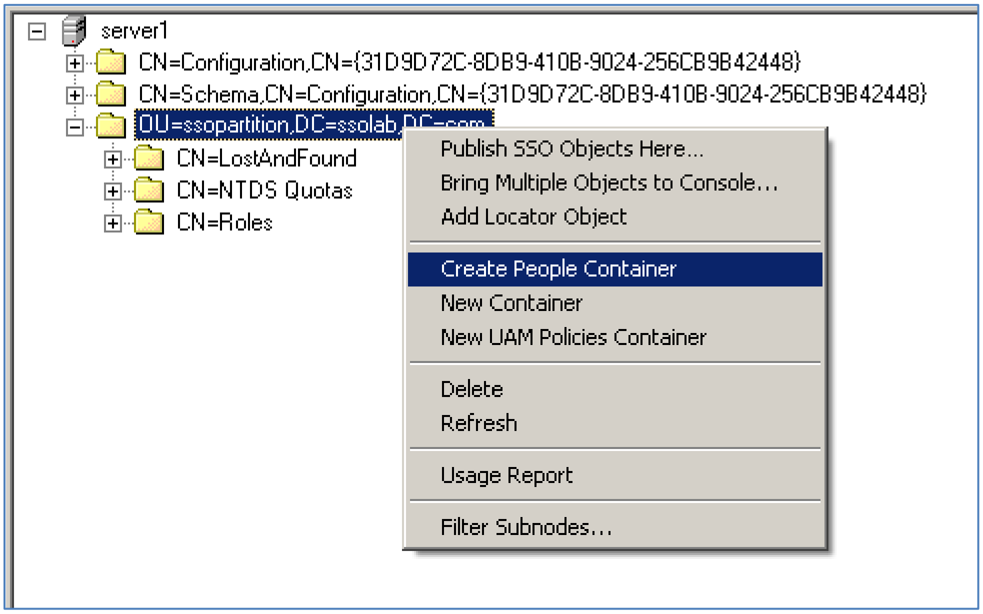
Step 2: Creating the People OU

After extending the AD LDS (ADAM) instance schema, you must create at least one People OU, which Logon Manager will use to store application credentials. By default, Logon Manager expects the People OU to reside at the root of the target AD LDS (ADAM) partition.

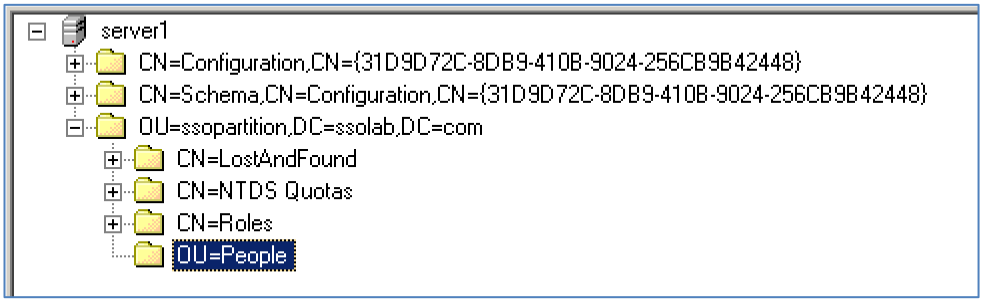
However, if you desire more granular control, you can create one or more People OUs anywhere in the directory and provide different instances of Logon Manager with the fully qualified paths to different People OUs, based on the requirements of your organization, as described in Configure Logon Manager to Use a Specific People OU (optional).

To create the People OU:

1. In the ESSO Suite 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 54 and click **OK** to connect.
3. In the tree, right-click the root of the target AD LDS (ADAM) instance, and select **Create People Container** from the context menu.


server1
CN=Configuration,CN={31D9D72C-8DB9-410B-9024-256CB9B42448}
CN=Schema,CN=Configuration,CN={31D9D72C-8DB9-410B-9024-256CB9B42448}
OU=ssopartition,DC=ssolab,DC=com
CN=LostAndFound
CN=NTDS Quotas
CN=Roles
Publish SSO Objects Here...
Bring Multiple Objects to Console...
Add Locator Object
Create People Container
New Container
New UAM Policies Container
Delete
Refresh
Usage Report
Filter Subnodes...

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

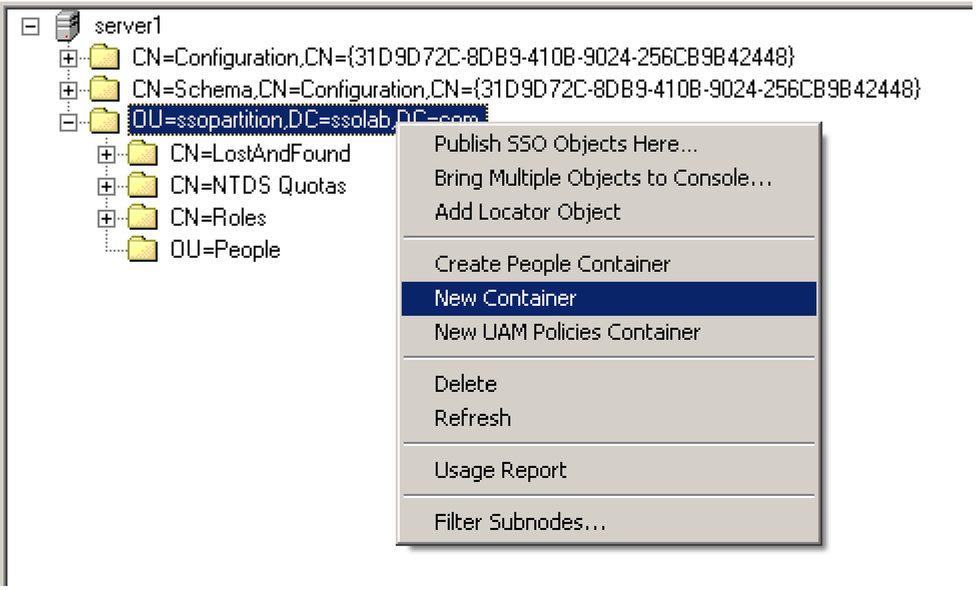

server1
CN=Configuration,CN={31D9D72C-8DB9-410B-9024-256CB9B42448}
CN=Schema,CN=Configuration,CN={31D9D72C-8DB9-410B-9024-256CB9B42448}
OU=ssopartition,DC=ssolab,DC=com
CN=LostAndFound
CN=NTDS Quotas
CN=Roles
OU=People

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 AD LDS (ADAM) documentation for possible causes and remedies.

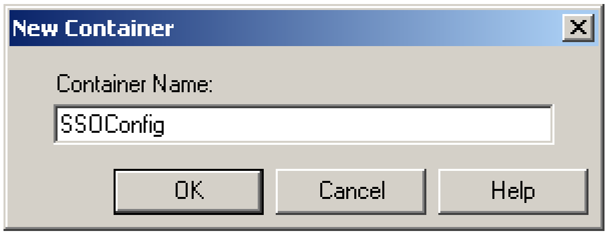
Step 3: Creating the Logon Manager Configuration Object Container and Sub-Tree Structure

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

1. In the Logon Manager 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:


server1
CN=Configuration,CN={31D9D72C-8DB9-410B-9024-256CB9B42448}
CN=Schema,CN=Configuration,CN={31D9D72C-8DB9-410B-9024-256CB9B42448}
OU=ssopartition,DC=ssolab,DC=com
CN=LostAndFound
CN=NTDS Quotas
CN=Roles
OU=People
Publish SSO Objects Here...
Bring Multiple Objects to Console...
Add Locator Object
Create People Container
New Container
New UAM Policies Container
Delete
Refresh
Usage Report
Filter Subnodes...

The Console displays the “New Container” dialog:



Container Name: SSOConfig

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 Logon Manager Users

You must grant Logon Manager users the following permissions in order to enable them to use Logon Manager:

- **Read access to the Logon Manager 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 Logon Manager 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 AD LDS (ADAM) instance.
- <domain> - target domain name.
- <port> – the port on which the target AD LDS (ADAM) instance is listening for connections.
- <sso_partition_dn> - the fully qualified DN of the Logon Manager application partition. Example: ou=ssopartition,dc=ssolab,dc=com

Configuring the AD LDS (ADAM) Synchronizer

After you have prepared AD LDS (ADAM) for Logon Manager, you must configure the AD LDS (ADAM) synchronizer for your environment. Configure these settings on your "template" client machine and include them in the MSI package you will use to deploy Logon Manager to end-users. Before starting this procedure, make sure that the Logon Manager Administrative Console and the Logon Manager Agent (including the AD LDS (ADAM) 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 Logon Manager Agent.

Note: If users will be synchronizing with the repository from outside of the corporate network, you must allow RPC protocol-based connections through the corporate firewall; otherwise, users will be unable to synchronize with the repository.

1. Launch the Logon Manager 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 Logon Manager.

Deploying Logon Manager with an LDAP Directory

This part describes best practices for deploying Logon Manager with an LDAP directory.
It contains the following sections:

Logon Manager and LDAP Environments

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; Logon Manager automatically detects and handles all subsequent requests for user credentials. For more information on Logon Manager, see the *Oracle Enterprise Single Sign-On Suite Technical Overview* white paper available from Oracle Support.

You have the choice to deploy Logon Manager in a directory environment, 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 Logon Manager to your existing directory environment provides the following benefits:

- Logon Manager 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.
- Logon Manager data is automatically protected by your existing backup and disaster recovery plans.
- No dedicated servers or server-side processes are required; Logon Manager'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 Logon Manager is achieved through the native capabilities of the directory.

A directory also enables the organization of Logon Manager 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 Logon Manager administration by permitting more efficient access control.

Note: To deploy Logon Manager with Oracle Identity Manager, you must enable the "Anonymous Bind" option in Oracle Identity Manager; Logon Manager will not bind to Oracle Identity Manager when "Anonymous Bind" is disabled.

How Logon Manager Extends Your Directory Schema

Before Logon Manager can store data in your directory, you must extend your directory schema using the Administrative Console. 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 Directory for Logon Manager. 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 Logon Manager, see the following appendices:

- Appendix A: Minimum Administrative Rights for Logon Manager Repository Objects
- Appendix B: Logon Manager Directory Repository Object Classes and Attributes

How Logon Manager Synchronizes with Your Directory

The Logon Manager Agent uses the LDAP synchronizer plug-in to communicate with your LDAP directory. When properly configured, synchronization occurs whenever one of the following events takes place:

- The Logon Manager 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 Logon Manager 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 Logon Manager Agent traverses the Logon Manager 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.

Note: Since Logon Manager does not support server autolocation nor use Windows credentials when authenticating to an LDAP directory other than Active Directory or AD LDS (ADAM), end-users will be prompted to authenticate to the directory in addition to authenticating to Windows and Logon Manager. In certain scenarios, it is possible to eliminate this extra prompt. See Selecting and Configuring an Authenticator for more information.

How Logon Manager Handles and Stores Application Credentials

Logon Manager 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. Logon Manager 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 Logon Manager stores per enabled application and per user is trivial (measurable in bytes and small kilobytes).

Note: Oracle highly recommends enabling SSL support so that the credentials sent by the user to the directory during authentication are encrypted. If SSL is not enabled, those credentials will be sent in clear text and can be intercepted by a packet sniffer. For more information, see SSL Support.

Benefits of Load-Balancing a Logon Manager Deployment

When a directory server fails, Logon Manager 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 directory server, Oracle highly recommends using a load balancer that will evenly and automatically distribute the requests coming from the network among the servers behind it. If a machine goes offline, the rest can temporarily absorb its workload, providing failover transparency to the end-user and adequate time to bring the faulty machine back online.

Warning: Deploying Logon Manager with multiple LDAP servers that use replication for synchronization behind a load balancer is not supported for high availability in an active-active (load balanced) scenario; it is only supported in an active-passive (failover) scenario. For more information, contact Oracle Support.

Further Reading

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

Designing the Logon Manager Directory Sub-Tree

Logon Manager 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 Logon Manager to support
- Robustness of the existing infrastructure
- Structure of your organization.

Guidelines for Structuring the Logon Manager Sub-Tree

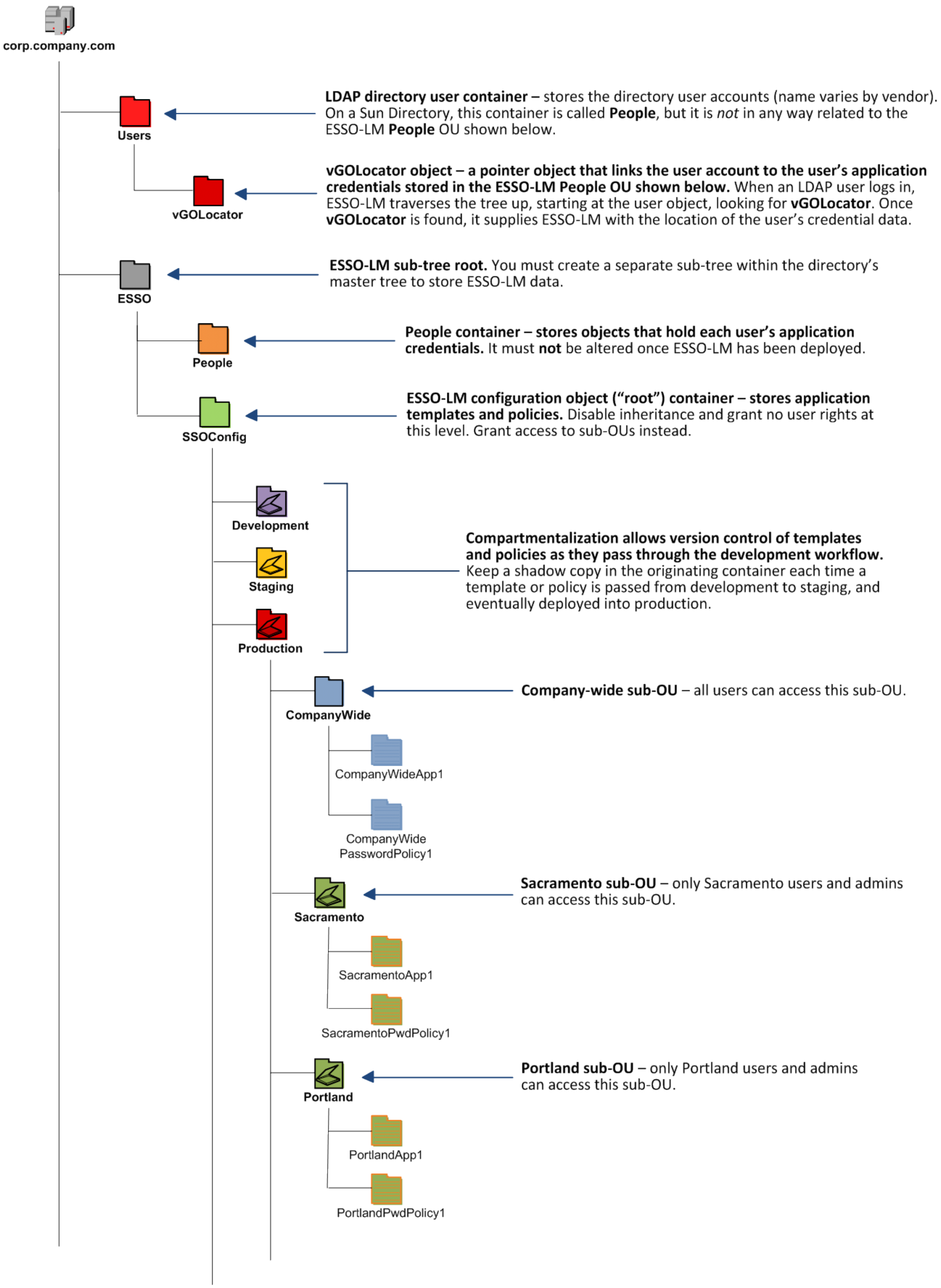
Oracle recommends that you set up your sub-tree as a hierarchy by following the guidelines below:

- 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 Logon Manager 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 Logon Manager Administrative Console; controlling access at the OU level is achieved via delegated administration using Microsoft and third-party management tools.

Figure 5 depicts a sample Logon Manager sub-tree whose design reflects the above best practices.



LDAP directory user container – stores the directory user accounts (name varies by vendor). On a Sun Directory, this container is called **People**, but it is *not* in any way related to the ESSO-LM **People** OU shown below.

vGOLocator object – a pointer object that links the user account to the user's application credentials stored in the ESSO-LM People OU shown below. When an LDAP user logs in, ESSO-LM traverses the tree up, starting at the user object, looking for **vGOLocator**. Once **vGOLocator** is found, it supplies ESSO-LM with the location of the user's credential data.

ESSO-LM sub-tree root. You must create a separate sub-tree within the directory's master tree to store ESSO-LM data.

People container – stores objects that hold each user's application credentials. It must **not** be altered once ESSO-LM has been deployed.

ESSO-LM configuration object ("root") container – stores application templates and policies. Disable inheritance and grant no user rights at this level. Grant access to sub-OUs instead.

Compartmentalization allows version control of templates and policies as they pass through the development workflow. Keep a shadow copy in the originating container each time a template or policy is passed from development to staging, and eventually deployed into production.

Company-wide sub-OU – all users can access this sub-OU.

Sacramento sub-OU – only Sacramento users and admins can access this sub-OU.

Portland sub-OU – only Portland users and admins can access this sub-OU.

Figure 5 Recommended Logon Manager 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: Oracle highly recommends that you store templates and policies in individual OUs. To do this, 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. When transitioning to a hierarchy, use the existing container as your new Logon Manager root container and create sub-OUs underneath it.

Special Directory Objects Required by Logon Manager

To successfully synchronize with an LDAP directory, Logon Manager requires that the following directory objects are configured before attempting synchronization:

- **`People` OU.** When deploying Logon Manager with a directory other than Active Directory, application credentials cannot be stored under user objects. Instead, credentials are stored in flat format inside a special OU called `People`. You must create this OU as described in Creating the People OU.

  Note: This OU is *not* in any way related to the `People` container used by Sun Directory Server to store LDAP user accounts.

  Note: Do *not* place the `People` OU inside the Logon Manager configuration object container (`SSOConfig`). Doing so will cause Logon Manager to parse the credentials of every Logon Manager user when loading templates, placing a significant, unnecessary load on the directory.

- **`vGOLocator` object.** This object links an LDAP user account to the user's application credentials stored in the `People` OU. When the user logs in, Logon Manager traverses the tree up from the user's object until the `vGOLocator` object is found. The `vGOLocator` object provides Logon Manager with the path to the `People` OU.

  Note: Oracle recommends placing this object inside your directory user accounts container, as shown in the diagram on page 13. If necessary, it can also be placed in the root of the directory tree, although this option is not recommended.
  At the very least, `vGOLocator` must be placed at the same level as the container that holds your user accounts.

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 5. 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 Logon Manager 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 LDAP 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 Logon Manager, 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 Logon Manager Agent, including its interaction with the directory, is governed by settings configured and deployed to the end-user machine by the Logon Manager administrator using the Logon Manager Administrative Console. The settings fall into one of the following categories:

- **Global Agent settings** are the "local policy" for the Agent**;** they are stored in the Windows registry on the end-user machine and are included in the Logon Manager MSI package to provide the Agent with an initial configuration during deployment. Global Agent settings are stored in `HKEY_LOCAL_MACHINE\Software\Passlogix` (32-bit systems) or `HKEY_LOCAL_MACHINE\Wow6432Node\Software\Passlogix` (64-bit systems).

  > **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**.

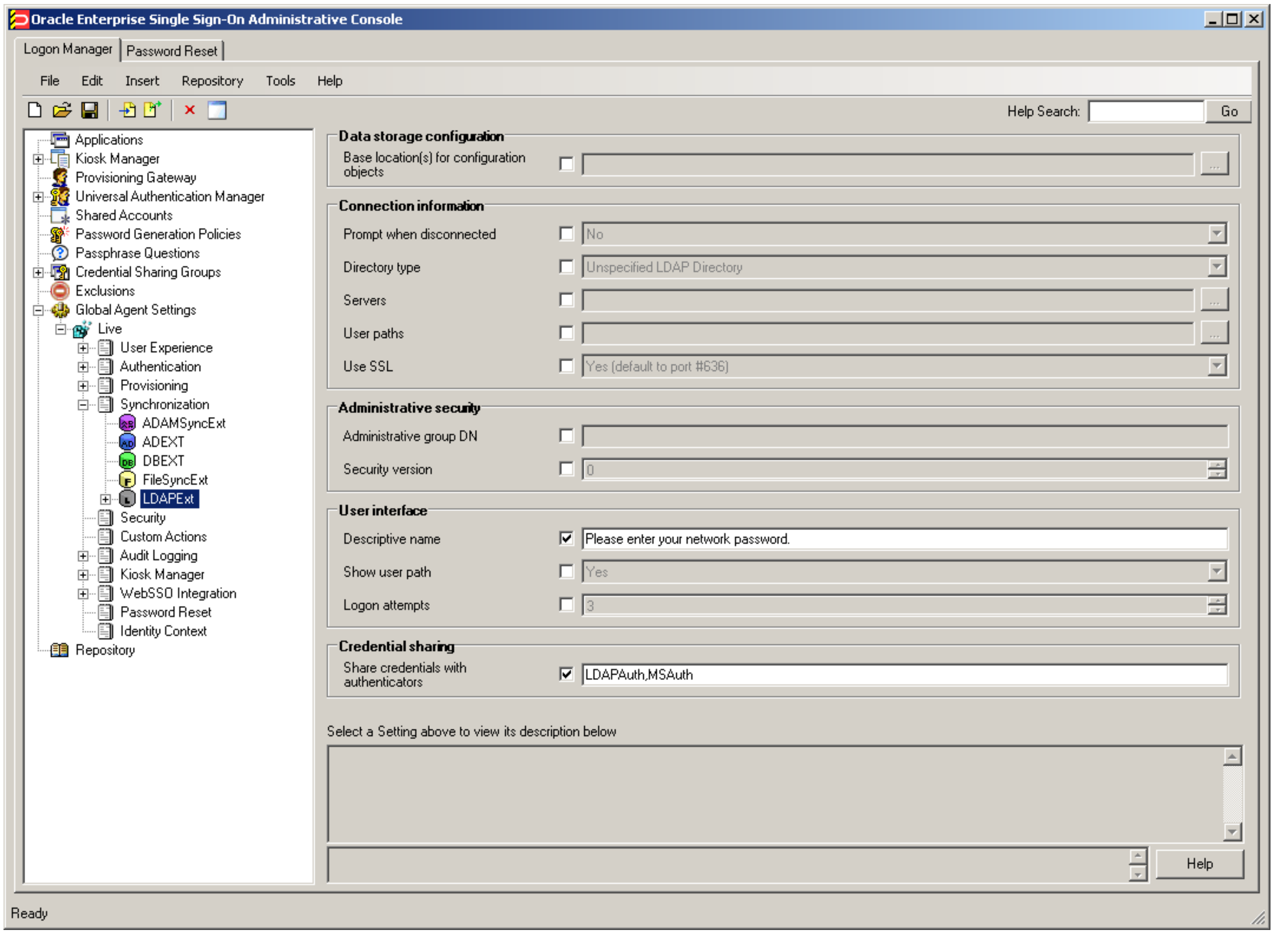
- **Administrative overrides** take precedence over the global Agent settings stored in the Windows registry and constitute the "domain" policy for the Agent. Overrides are downloaded from the central repository by the Agent during synchronization and stored in the Agent's encrypted and tamperproof local 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 *Logon Manager 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 6 depicts a typical view of the Logon Manager Administrative Console set up for synchronization with an LDAP directory.



Data storage configuration

Base location(s) for configuration objects ☐

Connection information

Prompt when disconnected ☐ No

Directory type ☐ Unspecified LDAP Directory

Servers ☐

User paths ☐

Use SSL ☐ Yes (default to port #636)

Administrative security

Administrative group DN ☐

Security version ☐ 0

User interface

Descriptive name ☑ Please enter your network password.

Show user path ☐ Yes

Logon attempts ☐ 3

Credential sharing

Share credentials with authenticators ☑ LDAPAuth,MSAuth

Select a Setting above to view its description below

Figure 6 The Logon Manager Administrative Console

The next section describes best practices for configuring Logon Manager for synchronization with LDAP. 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 Logon Manager Agent and the LDAP synchronizer plug-in are installed on your machine; otherwise, AD settings will not be displayed in the Console. For installation instructions, see the installation guide for your version of Logon Manager.

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 *Logon Manager 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 Logon Manager 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 Logon Manager MSI package. (For instructions on creating the package, see the section "Packaging Oracle Enterprise Single Sign-On Suite for Mass Deployment" in the *Enterprise Single Sign-On Suite Installation Guide*.)

Note: If users will be synchronizing with the repository from outside of the corporate network, you must allow RPC protocol-based connections through the corporate firewall; otherwise, users will be unable to synchronize with the repository.

Select the Correct Repository Type

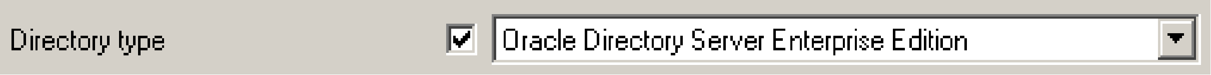
Before you begin configuring Logon Manager's synchronization settings, you must inform Logon Manager which supported directory you are using. This allows Logon Manager to correctly interpret the repository structure and store its data without interfering with the repository's built-in data structures.

The available choices are:

- Unspecified LDAP Directory (default)
- Generic LDAP Directory
- Novell eDirectory
- Oracle Directory Server Enterprise Edition
- IBM Tivoli Directory Server
- Oracle Internet Directory
- Siemens DirX Directory Server

Note: If your repository is not listed above, select **Unspecified LDAP Directory** (default) from the drop-down list for backwards compatibility in upgrade scenarios; otherwise select **Generic LDAP Directory**.

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



Directory type ☑ Oracle Directory Server Enterprise Edition

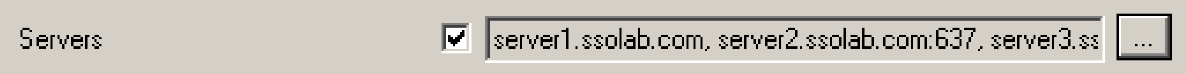
To set: Select the check box, then select your repository from the drop-down list.

Configure a Server List with Desired Failover Order

In LDAP environments, server URLs must be explicitly provided to Logon Manager. Oracle highly recommends using at least two physical directory 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

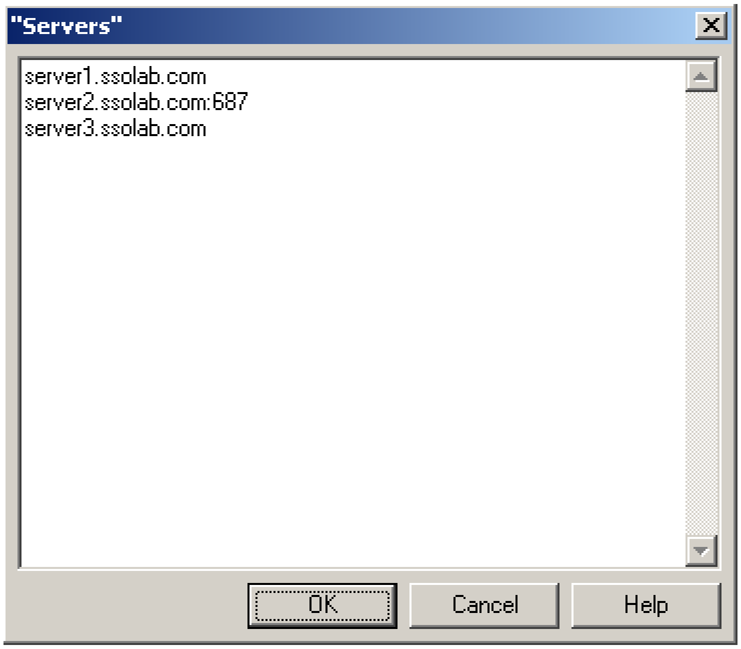
the end-user and the next available server is minimized. For more information on load balancing, see Benefits of Load-Balancing a Logon Manager Deployment.

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



Servers ☑ server1.ssolab.com, server2.ssolab.com:637, server3.ss

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**.



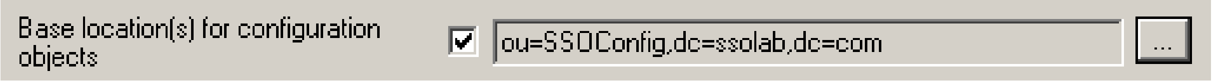
"Servers"

```
server1.ssolab.com
server2.ssolab.com:687
server3.ssolab.com
```

Specify the Path to the Logon Manager Configuration Objects

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

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



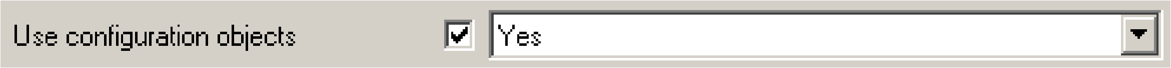
Base location(s) for configuration objects ☑ ou=SSOConfig,dc=ssolab,dc=com

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

Use Configuration Objects

When deploying with an LDAP directory, Oracle highly recommends that you use 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 Logon Manager Directory Sub-Tree. If you disable this feature, Logon Manager will store all template and configuration data as a single flat file in the Logon Manager root container.

Located in: Global Agent Settings → Live → Synchronization



Use configuration objects ☑ Yes

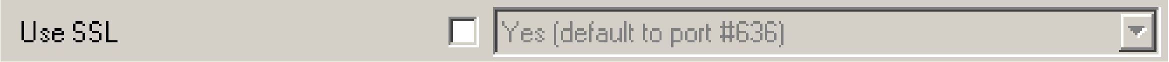
To enable: Select the check box, then select **Yes** from the drop-down list.

SSL Support

Logon Manager repository synchronizers ship with SSL support enabled and Oracle highly recommends that you do not disable it. Your environment should always utilize SSL for all connections to the Logon Manager and other repositories for maximum security.

Note: You must configure your environment for SSL connectivity before enabling this option.

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



Use SSL □ Yes (default to port #636)

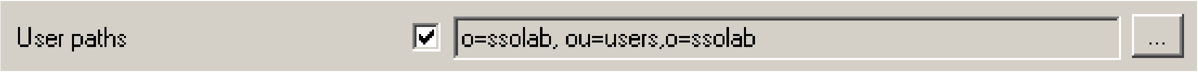
To re-enable (if disabled): Deselect the check box.

Specify the Path(s) to User Accounts

You must specify the location of the container(s) holding user accounts in your directory. If your directory stores user accounts in multiple locations, you can specify multiple paths. Follow the guidelines below when configuring this option:

- When the Enable Directory Search for Users option is enabled, do not specify the directory root as a value here. Doing so will cause Logon Manager to parse the entire directory if a user enters an invalid user name.
- When specifying paths, be as specific as possible to avoid extra account searches if the path you specify happens to be too broad. On the other hand, if the number of locations is excessive, it can help to specify a common parent container here to reduce the complexity of your configuration.

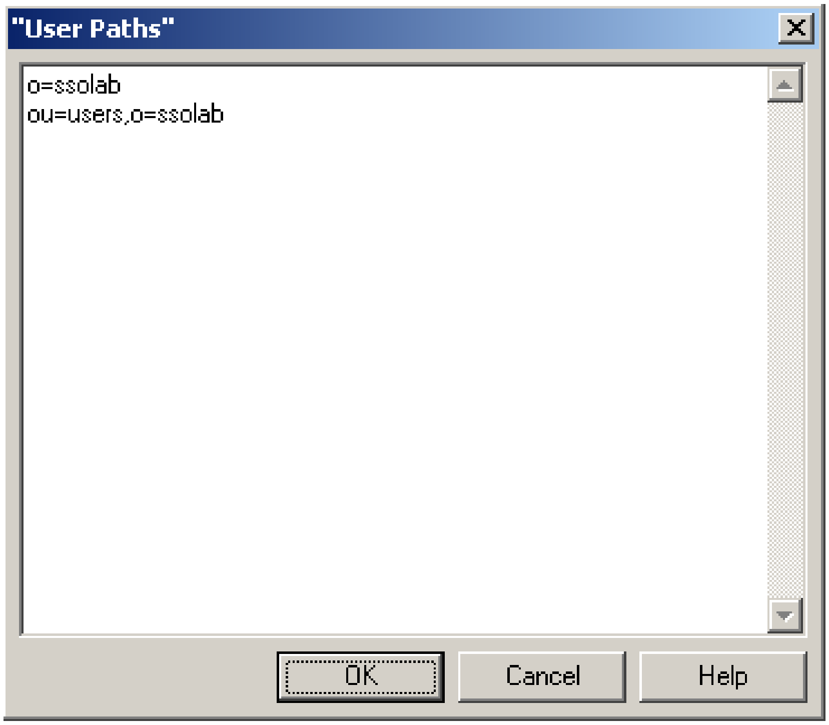
Located in: Global Agent Settings → Live → Synchronization → LDAPEXT



User paths ☑ o=ssolab, ou=users,o=ssolab

To let Logon Manager search for user accounts: deselect the check box (default setting).

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**.

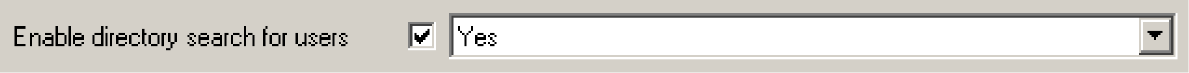


o=ssolab
ou=users,o=ssolab

Enable Directory Search for Users

If you do not want to specify exact paths to user accounts in your directory (for example, if they are spread out over a large number of locations), enable this option to allow Logon Manager to search for user accounts within one or more locations set in Specify the Path(s) to User Accounts. This feature requires anonymous bind access to the directory; if you do not wish to grant anonymous bind access to your directory, but still want to enable the directory search feature, you must specify a user with directory search rights using the **Bind User DN** and **Bind User Password** fields.

Located in: Global Agent Settings → Live → Synchronization → LDAPEXT → Special Purpose



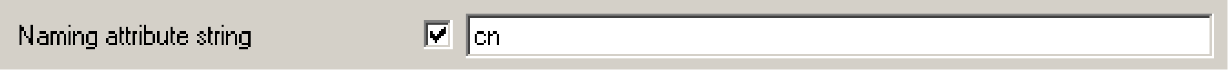
Enable directory search for users ☑ Yes

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

Set the Naming Attribute String

If you are using Novel eDirectory, you must set the value of the **Naming attribute string** option to cn. For other LDAP directories, consult your directory team to find out how to configure this option.

Located in: Global Agent Settings → Live → Synchronization → LDAPEXT → Special Purpose



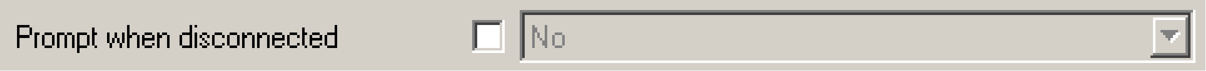
Naming attribute string ☑ cn

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

Decide Whether to Prompt the User when Disconnected from the Directory

Use the **Prompt when disconnected** option to decide whether Logon Manager 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**; doing so will avoid unnecessary confusion and helpdesk calls.

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



Prompt when disconnected □ No

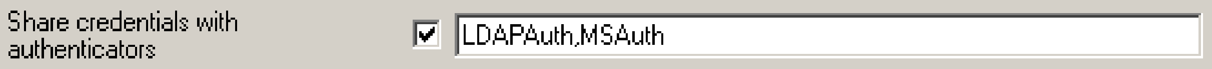
To set: Select the check box, then select the appropriate option from the drop-down list.

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**.

Share LDAP Synchronizer Credentials with Authenticators

In certain scenarios, you can reduce the number of authentication prompts end users receive by sharing the LDAP synchronization credentials with one or more authenticators. See Selecting and Configuring an Authenticator for more information.

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



Share credentials with authenticators ☑ LDAPAuth,MSAuth

To set: Select the check box, then enter the names of target authenticators, separated by commas.

Use the following authenticator identification strings, depending on the authenticator(s) in use:

Authenticator	Identification String
Windows v1 (deprecated)	`WinAuth`
Windows v2	`MSAuth`
LDAP v1	`LDAP`
LDAP v2	`LDAPAuth`

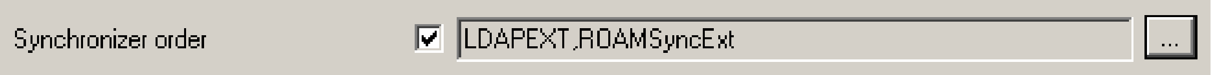
Add the LDAP Synchronizer to the Synchronizer Order List

Ensure that the LDAP (LDAPEXT) synchronizer plug-in is present and enabled in the **Synchronizer Order** list if at least one of the following is true for your environment:

- Logon Manager is synchronizing with more than one repository.
- Logon Manager is using roaming synchronization.
- Kiosk Manager is installed in your environment.

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

Located in: Global Agent Settings → Live → Synchronization



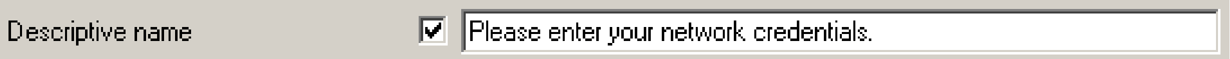
Synchronizer order ☑ LDAPEXT,ROAMSyncExt

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

Set the Authentication Prompt Window Title

Oracle recommends that you use this option to give the directory authentication prompt a descriptive title so that end users know what credentials to enter when the prompt appears.

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

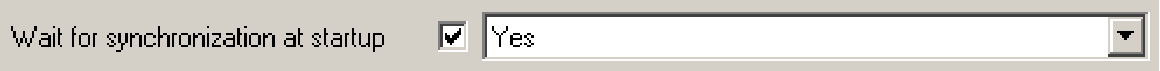

Descriptive name ☑ Please enter your network credentials.

To set: Select the check box, then enter the desired text.

Make the Logon Manager Agent Wait for Synchronization on Startup

To ensure that users always have the most recent credentials, application templates, password policies, and administrative overrides, configure the Agent to wait for synchronization on startup. When this option is enabled, the Agent checks whether the directory is online. 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


Wait for synchronization at startup ☑ Yes

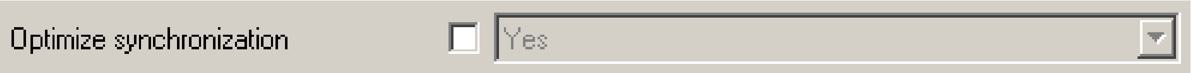
To set: Select the check box, then select **Yes** from the drop-down list.

Use Optimized Synchronization

Optimized synchronization instructs the Logon Manager Agent to synchronize only credentials that have changed since the last synchronization. Do one of the following, depending on your environment:

- Enable this option to improve synchronization performance on deployments with 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


Optimize synchronization ☐ Yes

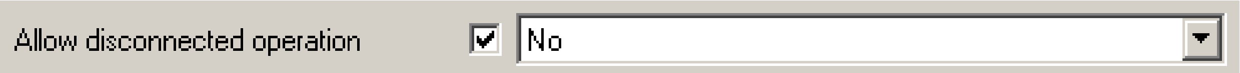
Use the default value (**Yes**) unless your environment requires otherwise.

Restrict Disconnected Operation

During deployment, configure the Logon Manager 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 *Logon Manager Best Practices: Configuring the Logon Manager Agent* for more information on this required best practice.

Located in: Global Agent Settings → Synchronization



Allow disconnected operation ☑ No

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 *Oracle Enterprise Single Sign-On Suite Secure Deployment Guide* and in the “Configuring the Logon Manager Agent” section of the *Oracle Enterprise Single Sign-On Suite Administrator’s Guide*.

Overview of the Deployment Process

This section provides a brief high-level overview of the Logon Manager deployment process an LDAP directory. Make sure you have read all of the preceding sections of this document before proceeding with deployment. Deploying Logon Manager with an LDAP directory requires you to:

1. Obtain the following documents:
   - The latest version of this document
   - *Oracle Enterprise Single Sign-On Suite Installation Guide*
   - *Oracle Enterprise Single Sign-On Suite Administrator’s Guide*
2. Install the Logon Manager Agent and the Logon Manager Administrative Console on a machine within your domain, as described in the installation guide for your version of Logon Manager. Make sure you select the LDAP Synchronizer plug-in when installing the Agent.
3. Complete the steps in Preparing the Directory for Logon Manager:
   a. Extend the directory schema with Logon Manager classes and attributes.
   b. Create the `People` OU, which will store each user’s application credentials.
   c. Create the `vGOLocator` object.
   d. Create the configuration object container and the desired tree structure.

4. Configure Logon Manager as follows:
   a. Complete the steps in Selecting and Configuring an Authenticator.
   b. Complete the steps in Configuring the LDAP Synchronizer.
   c. Configure the options described in Recommended Global Agent Settings in this guide.
   d. Configure the options described in the "Configuring the Logon Manager Agent" section of the *Enterprise Single Sign-On Suite Administrator's Guide*.
   e. Test your configuration, as described in Testing the Logon Manager Configuration.

> **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 *Packaging Logon Manager for Mass Deployment* section of the *Enterprise Single Sign-On Suite Installation Guide*.
7. Create, test, and deploy the remaining application templates. See the guide *Configuring and Diagnosing Logon Manager Application Templates* for in-depth information on provisioning different types of applications.

Preparing the Directory for Logon Manager

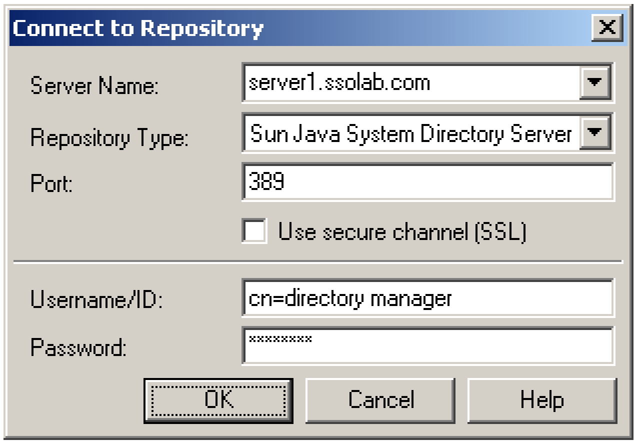
This section describes the basic procedures for preparing the directory for use with Logon Manager. The preparation consists of extending your directory schema with Logon Manager classes and attributes, allowing Logon Manager to store credentials under respective user objects, and creating the desired tree structure. Before starting this procedure, make sure that you have installed the Logon Manager Administrative Console, as described in the *Installation and Setup* guide for your version of Logon Manager.

Step 1: Extending the Schema

1. Start the Logon Manager Administrative Console. By default, the shortcut to the console is located in **Start → Programs → Oracle → Logon Manager 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.



Server Name: server1.ssolab.com

Repository Type: Sun Java System Directory Server

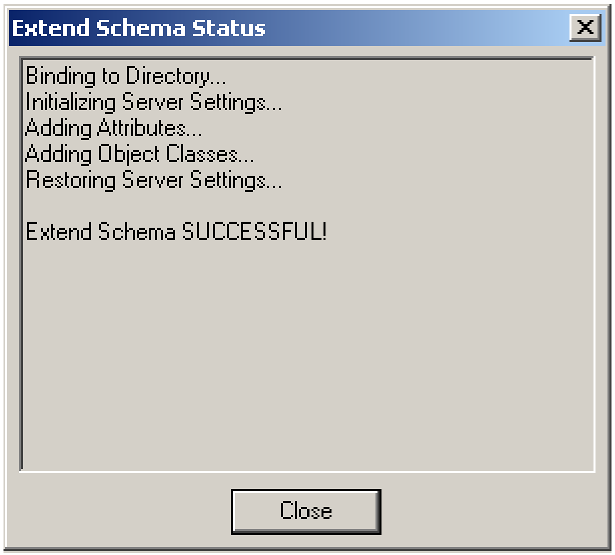
Port: 389

□ Use secure channel (SSL)

Username/ID: cn=directory manager

Password: ********

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 the desired LDAP directory type.
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 the directory server has been configured to use SSL, leave the **Use secure channel (SSL)** option selected; otherwise, deselect it. (See SSL Support for more information.)
7. In the **Username/ID** and **Password** fields, enter the credentials of the account you want Logon Manager to use to connect to the directory. 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:



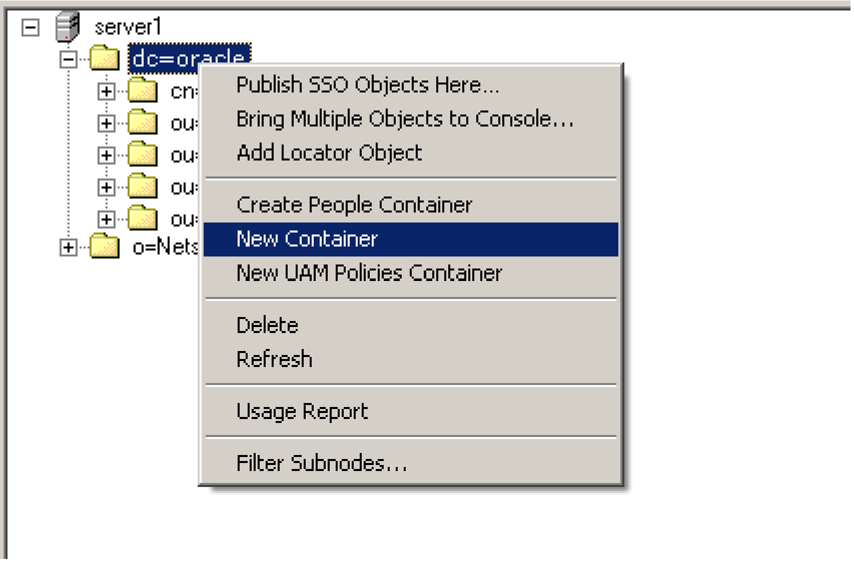
```
Binding to Directory...
Initializing Server Settings...
Adding Attributes...
Adding Object Classes...
Restoring Server Settings...

Extend Schema SUCCESSFUL!
```

9. Click **Close**.

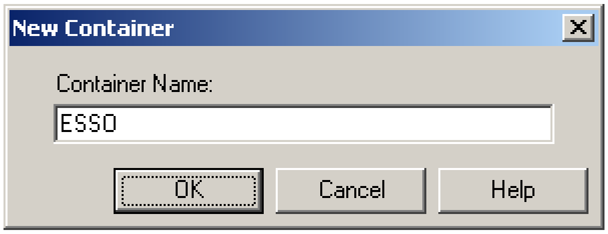
Step 2: Creating the Logon Manager Sub-Tree Root and the Configuration Object Container

Note: While it is possible to use an existing container for storing Logon Manager data, doing so may impair directory performance. Oracle highly recommends that you create a dedicated container as the sub-tree root.

1. In the Logon Manager 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.
3. Fill in the fields as explained in steps 3–7 on page 29 and click **OK** to connect.
4. Create the container that will serve as the Logon Manager sub-tree root:
   a. 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:

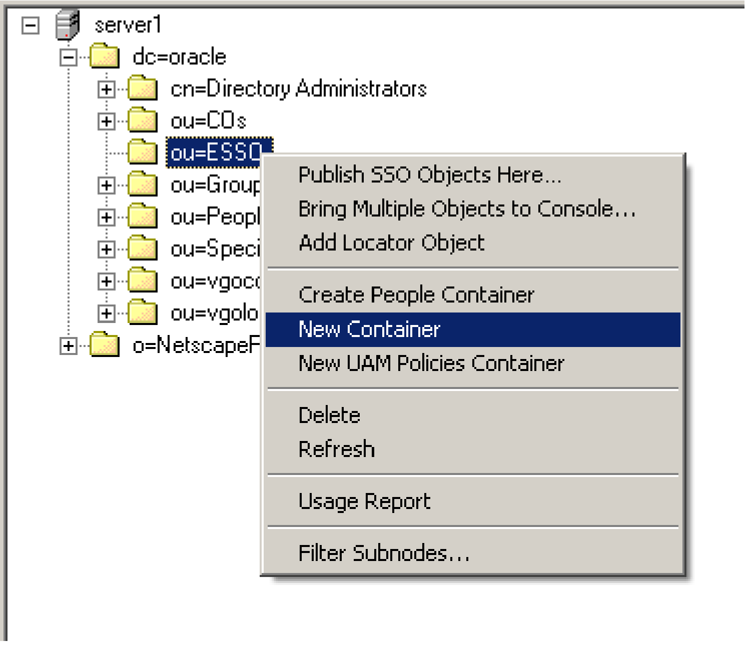


Container Name: ESSO

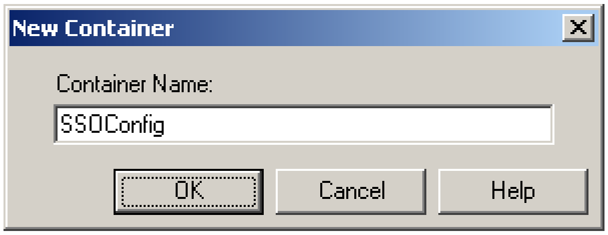
   b. In the “New Container” dialog, enter the desired name and click **OK**.

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

5. Create the Logon Manager configuration object container (`SSOConfig`):
    a. In the tree, right-click Logon Manager sub-tree root and select **New Container** from the context menu, as shown below:



    b. The Console displays the "New Container" dialog:



Container Name: SSOConfig

    c. 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 step 5 to create any additional containers you may need.

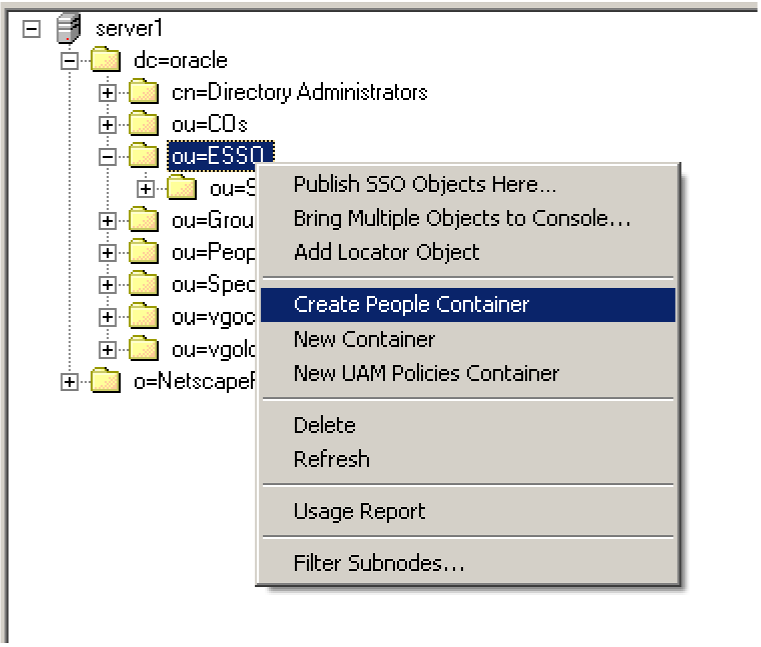
Step 3: Creating the `People` OU

You must create the `People` OU that will hold application credentials for Logon Manager users. Oracle recommends placing the `People` OU inside the Logon Manager sub-tree root.

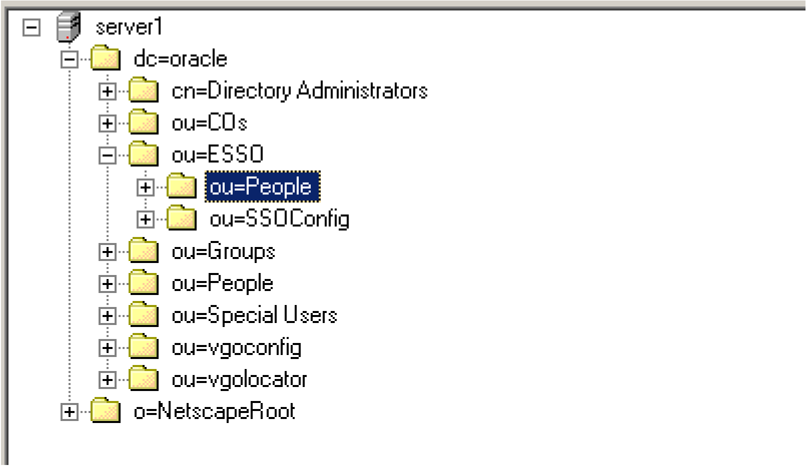
> **Note:** Do *not* place the `People` OU inside the Logon Manager configuration object container (`SSOConfig`). Doing so will cause Logon Manager to parse the credentials of every Logon Manager user when loading templates, placing a significant, unnecessary load on the directory.
>
> **Note:** Sun Directory Server stores user accounts in a container named `People` in the root of the directory. You must not use that container to store Logon Manager application credentials; instead, create the Logon Manager `People` OU in another parent container.

To create the `People` OU:

1. In the Logon Manager 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. Fill in the fields as explained in steps 3–7 on page 29 and click **OK** to connect.
3. In the tree, right-click the root of the Logon Manager sub-tree, and select **Create People Container**.



4. Verify that the `People` OU now exists at the target location.



```
server1
  dc=oracle
    cn=Directory Administrators
    ou=COs
    ou=ESSO
      ou=People
      ou=SSOConfig
    ou=Groups
    ou=People
    ou=Special Users
    ou=vgoconfig
    ou=vgolocator
  o=NetscapeRoot
```

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 vendor documentation for your directory for possible causes and remedies.

Step 4: Creating the `vGOLocator` Pointer Object

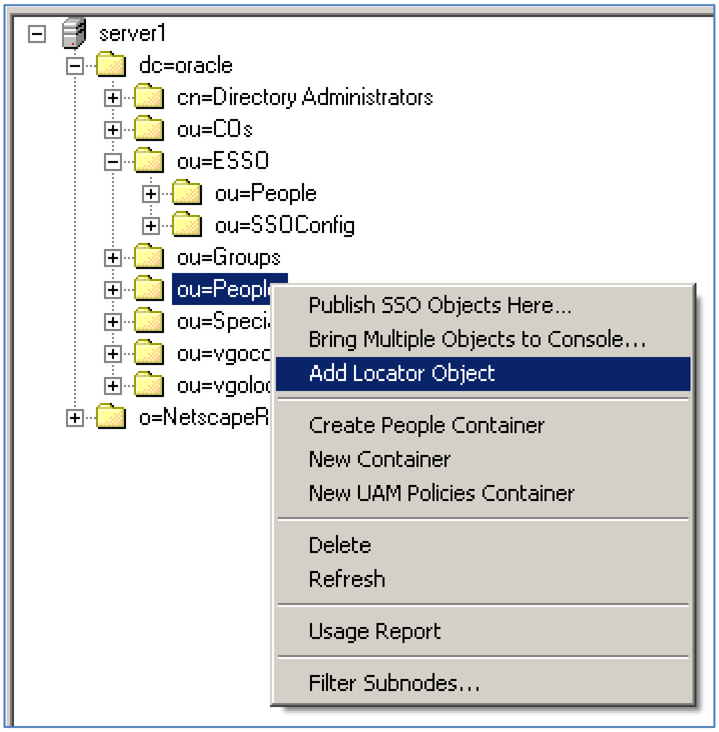
Once you have created the `People` OU, you must create the `vGOLocator` pointer object that will link user accounts to user application credentials stored in the `People` OU.

> **Note:** You *must* create the `vGOLocator` object at least at the same level as the container that holds user accounts. Ideally, `vGOLocator` should exist inside the directory's user accounts container.

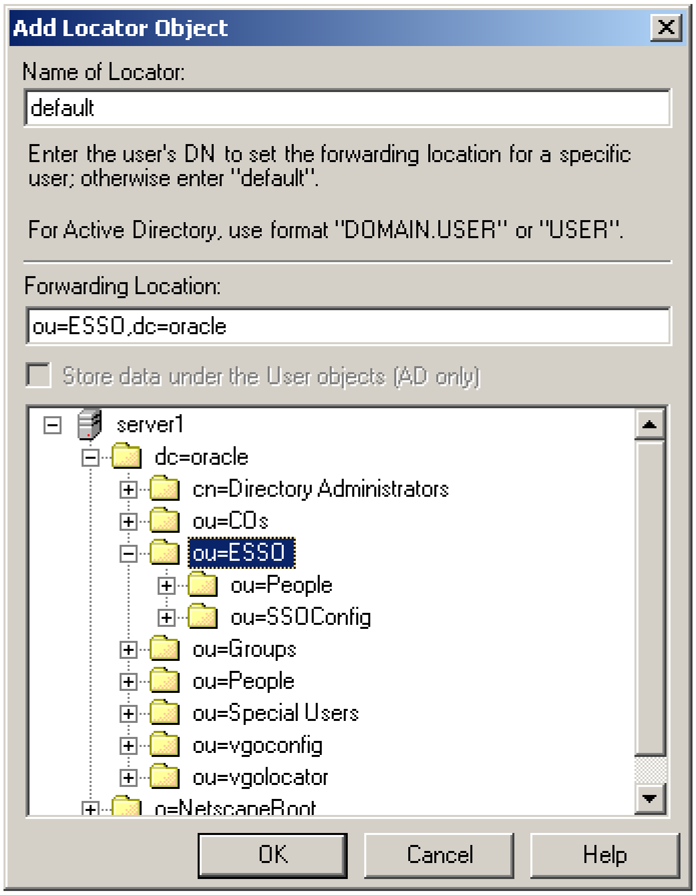
To create the `vGOLocator` object:

1. In the Logon Manager 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 your directory's user account container (`dc=oracle,ou=People` in our Sun Directory Server-based example) and select **Add Locator Object** from the context menu, as shown below:



4. In the “Add Locator Object” dialog that appears, do the following:
   a. In the **Name** field, enter `default`.
   b. In the **Forwarding Location** field, enter the full path to the container that holds the `People` OU. (Alternatively, you may navigate to and select the target container using the tree.)
   c. Click **OK**.



Add Locator Object

Name of Locator: default

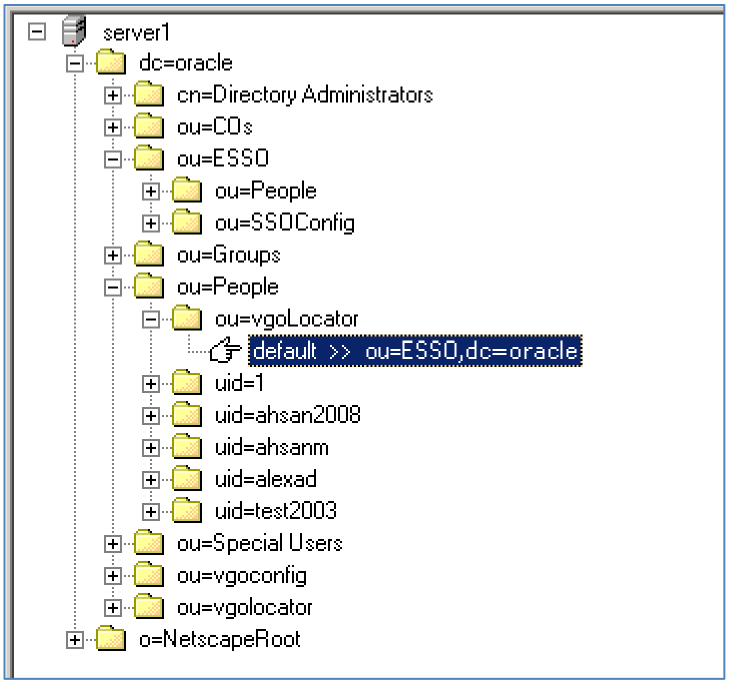
Enter the user's DN to set the forwarding location for a specific user; otherwise enter "default".

For Active Directory, use format "DOMAIN.USER" or "USER".

Forwarding Location: ou=ESSO,dc=oracle

☐ Store data under the User objects (AD only)

5. Verify that the `vGOLocator` object appears at the destination location.



Selecting and Configuring an Authenticator

An authenticator is necessary to uniquely authenticate the user to Logon Manager. In an LDAP environment, you have the choice to select one of the following authenticators, based on your configuration:

- **Windows Password Authenticator (Version 2).** Oracle highly recommends using this authenticator, as it allows to eliminate authentication prompts when the following conditions are met (see Share LDAP Synchronizer Credentials with Authenticators for more information):
    - The user has an Active Directory or NT domain account.
    - The LDAP directory credentials are synchronized with Active Directory or the NT domain.
- **LDAP Authenticator (Version 2).** Use this authenticator if you cannot uniquely identify the user based on the machine logon, for example in kiosk or other environments where users are logged in generically, or when the user has no Active Directory or NT domain account. Users will receive additional authentication prompts in this scenario unless their synchronization and user credentials are identical (see Share LDAP Synchronizer Credentials with Authenticators for more information).

Configuring the LDAP Synchronizer

After you have prepared LDAP for Logon Manager, you must configure the LDAP synchronizer for your environment. Configure these settings on your "template" client machine and include them in the MSI package you will use to deploy Logon Manager to end-users. Before starting this procedure, make sure that the Logon Manager Administrative Console and the Logon Manager Agent (including the LDAP 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 Logon Manager Agent.

> **Note:** If users will be synchronizing with the repository from outside of the corporate network, you must allow RPC protocol-based connections through the corporate firewall; otherwise, users will be unable to synchronize with the repository.

1. Launch the Logon Manager 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 Logon Manager.

Part 4: Appendices

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

- Appendix A: Minimum Administrative Rights for Logon Manager Repository Objects
- Appendix B: Logon Manager Repository Object Classes and Attributes
- Appendix C: Troubleshooting Logon Manager on Active Directory
- Appendix D: Troubleshooting Logon Manager on Microsoft AD LDS (ADAM)
- Appendix E: Creating the Required User Groups on AD LDS (ADAM) Deployments
- Appendix F: Configuring Oracle Internet Directory for Use with Logon Manager
- Appendix G: Configuring Oracle Virtual Directory for Use with Logon Manager

Appendix A: Minimum Administrative Rights for Logon Manager Repository Objects

This appendix lists the minimum administrative rights that must be granted to specific Logon Manager objects for Logon Manager to function.

Note: Information in this appendix is provided for your reference. By default, Logon Manager automatically sets the appropriate rights when you extend your repository schema.
If necessary, these rights can be manually granted and modified directly the repository.

Minimum Administrative Rights Required by Logon Manager Containers

You must grant the following administrative rights to each container in which you want Logon Manager 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: Logon Manager Repository Object Classes and Attributes

This appendix describes the directory classes, attributes, and access rights that Logon Manager 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 Logon Manager 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 Logon Manager 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 Logon Manager on Active Directory

This appendix contains descriptions of issues that may arise during deployment of Logon Manager, 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 Logon Manager 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, Logon Manager 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 Logon Manager to set the necessary rights by selecting **Enable storage of credentials under the user object (AD only)** from the **Repository** menu in the Logon Manager 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.

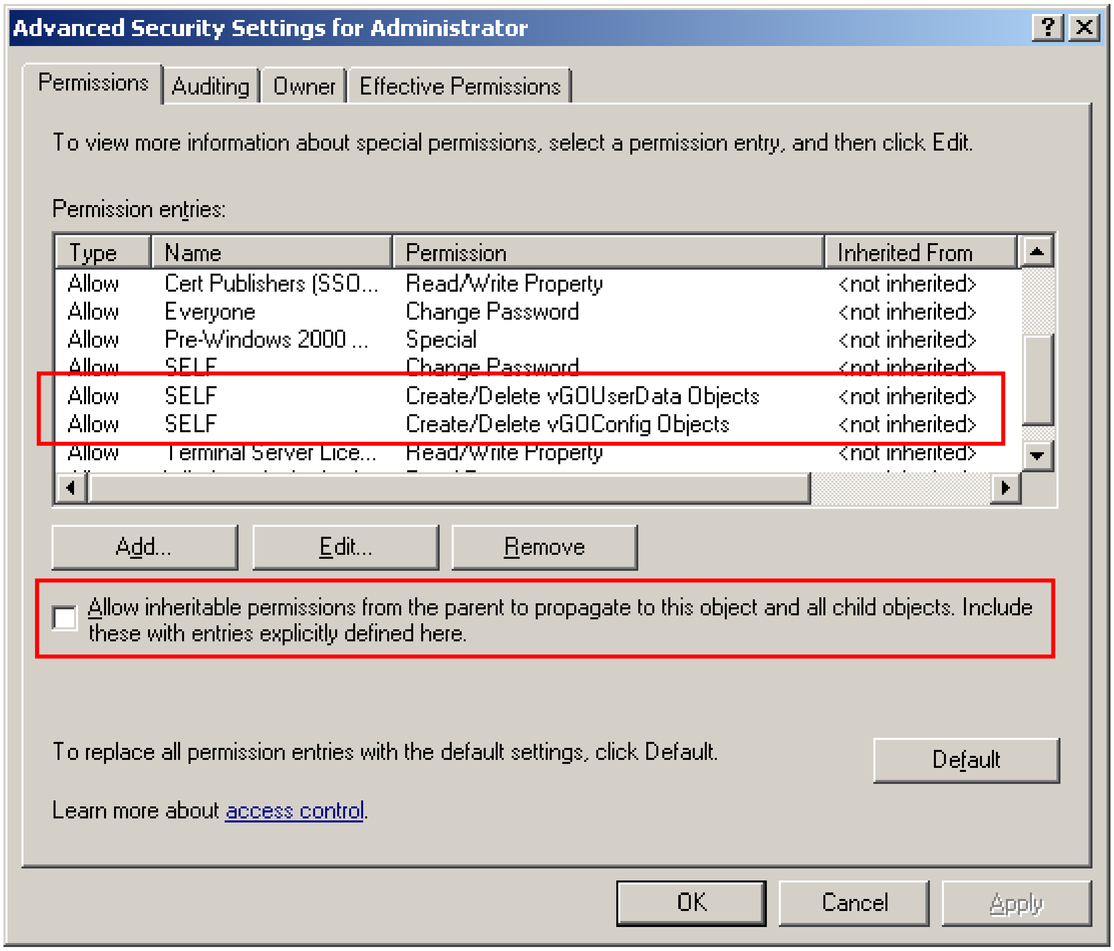
The following protected user groups are known to be affected by this problem:

- 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 Microsoft Management Console and load the **Active Directory Users and Computers** 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:



To view more information about special permissions, select a permission entry, and then click Edit.

Permission entries:

Type	Name	Permission	Inherited From
Allow	Cert Publishers (SSO...	Read/Write Property	<not inherited>
Allow	Everyone	Change Password	<not inherited>
Allow	Pre-Windows 2000 ...	Special	<not inherited>
Allow	SELF	Change Password	<not inherited>
Allow	SELF	Create/Delete vGOUserData Objects	<not inherited>
Allow	SELF	Create/Delete vGOConfig Objects	<not inherited>
Allow	Terminal Server Lice...	Read/Write Property	<not inherited>

□ Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly defined here.

To replace all permission entries with the default settings, click Default.

Learn more about access control.

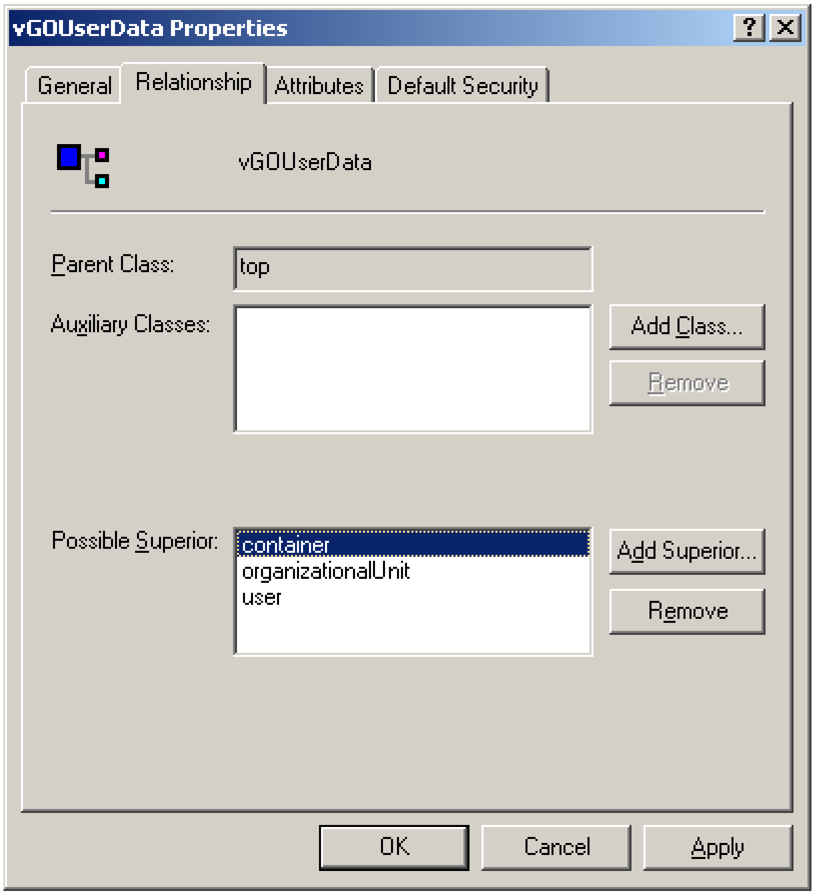
7. In the dialog, check whether:
   a. The **Allow inheritable permissions…** check box is not selected.
   b. The permissions highlighted in the figure in step 6 are not present in the list.

   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 Schema** snap-in.
3. In the left-hand tree, drill down the **Classes** node and locate the **vGOUserData** node.
4. Right-click the **vGOUserData** class and select **Properties** from the context menu.
5. In the dialog that appears, select the **Relationship** tab.
6. Click the **Add Superior** button.

7. In the dialog that appears, select **container** from the drop-down list and click **OK**.
   The “container” class appears in the Possible Superior field.



vGOUserData Properties

vGOUserData

Parent Class: top

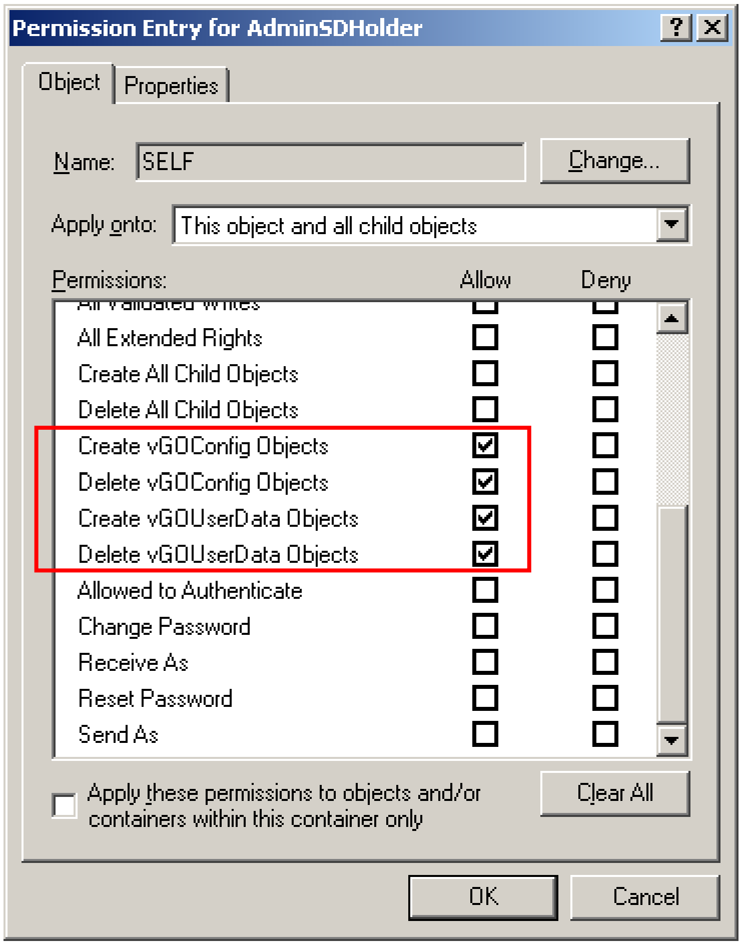
Auxiliary Classes:

Possible Superior: container
organizationalUnit
user

8. Click **OK** to close the properties dialog.
9. In the Microsoft Management Console, open the **Active Directory Users and Computers** snap-in.
10. From the **View** menu, select **Advanced Features**.
11. Navigate to the `AdminSDHolder` container located in:
    `cn=AdminSDHolder,cn=System,dc=<domainName>,dc=<domainSuffix>`
12. Right-click the `AdminSDHolder` container and select **Properties**.
13. In the “Properties” dialog, select the **Security** tab and click **Advanced**.
14. In the “Advanced Security Settings” dialog, click **Add…** .
15. In the “Select User, Computer, or Group” dialog, enter **SELF** and click **OK**.
16. 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:



Permission Entry for AdminSDHolder

Name: SELF

Apply onto: This object and all child objects

Permissions:	Allow	Deny
All Validated Writes	□	□
All Extended Rights	□	□
Create All Child Objects	□	□
Delete All Child Objects	□	□
Create vGOConfig Objects	☑	□
Delete vGOConfig Objects	☑	□
Create vGOUserData Objects	☑	□
Delete vGOUserData Objects	☑	□
Allowed to Authenticate	□	□
Change Password	□	□
Receive As	□	□
Reset Password	□	□
Send As	□	□

□ Apply these permissions to objects and/or containers within this container only

c. Click **OK**.

17. 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.

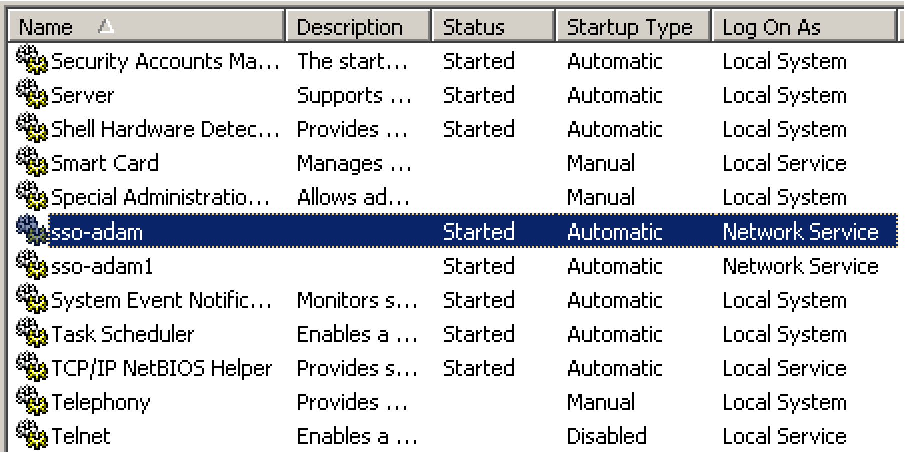
Appendix D: Troubleshooting Logon Manager on Microsoft AD LDS (ADAM)

If Logon Manager is unable to connect to the target AD LDS (ADAM) instance, try connecting to your AD LDS (ADAM) instance directly using the ADSIEdit tool. If you still cannot connect, the possible causes are described below.

The Target AD LDS (ADAM) Instance is Not Running

Your AD LDS (ADAM) instance runs as a service on the target server. Use the Computer Management MMC
snap-in on the target server to check whether the AD LDS (ADAM) 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 AD LDS (ADAM) instance in the list.



Name	Description	Status	Startup Type	Log On As
Security Accounts Ma...	The start...	Started	Automatic	Local System
Server	Supports ...	Started	Automatic	Local System
Shell Hardware Detec...	Provides ...	Started	Automatic	Local System
Smart Card	Manages ...		Manual	Local Service
Special Administratio...	Allows ad...		Manual	Local System
sso-adam		Started	Automatic	Network Service
sso-adam1		Started	Automatic	Network Service
System Event Notific...	Monitors s...	Started	Automatic	Local System
Task Scheduler	Enables a ...	Started	Automatic	Local System
TCP/IP NetBIOS Helper	Provides s...	Started	Automatic	Local Service
Telephony	Provides ...		Manual	Local System
Telnet	Enables a ...		Disabled	Local Service

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.

AD LDS (ADAM) Instance is Running on Non-Default Ports

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

- To check the ports on which the target AD LDS (ADAM) instance is running, see AD LDS (ADAM) documentation.
- To check (and correct) the ports Logon Manager uses to connect to AD LDS (ADAM), examine the contents of the **Servers** field in the Console. Logon Manager 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 AD LDS (ADAM) Does Not Have the Required Privileges

If Logon Manager cannot connect to AD LDS (ADAM), check whether the user account used to connect to AD LDS (ADAM) has the required privileges. To check and set the privileges for a user account, see the operating system and AD LDS (ADAM) documentation.

Appendix E: Creating the Required User Groups on AD LDS (ADAM) Deployments

This appendix describes how to create the `SSOAdmins` and `SSOUsers` groups in Active Directory for use with Logon Manager deployed on an AD LDS (ADAM) instance.

- **`SSOAdmins`**. This group contains at least two users who hold administrative privileges over the target AD LDS (ADAM) 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 Logon Manager deployment if the single account becomes inaccessible.

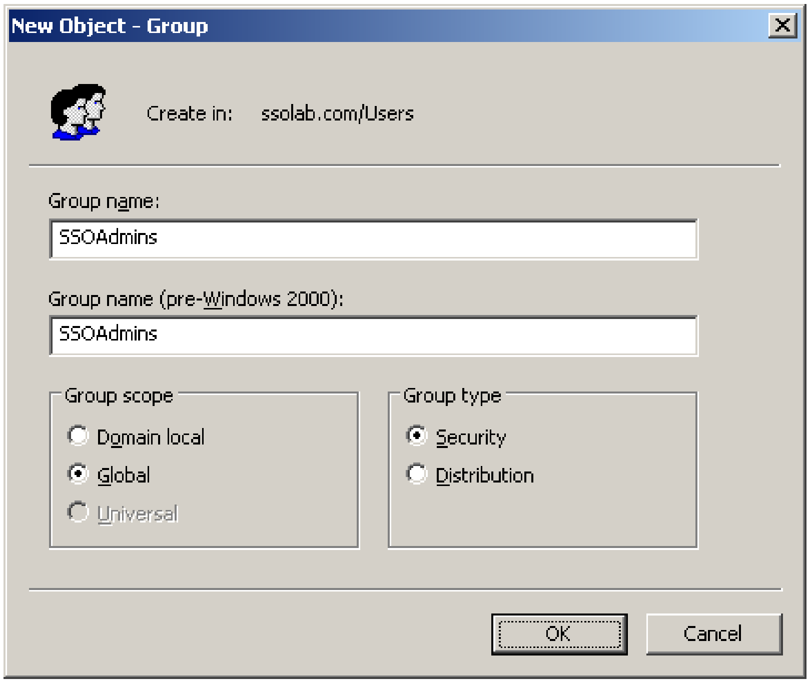
- **`SSOUsers`**. This group contains all other Logon Manager users.

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**.



New Object - Group

Create in: ssolab.com/Users

Group name: SSOAdmins

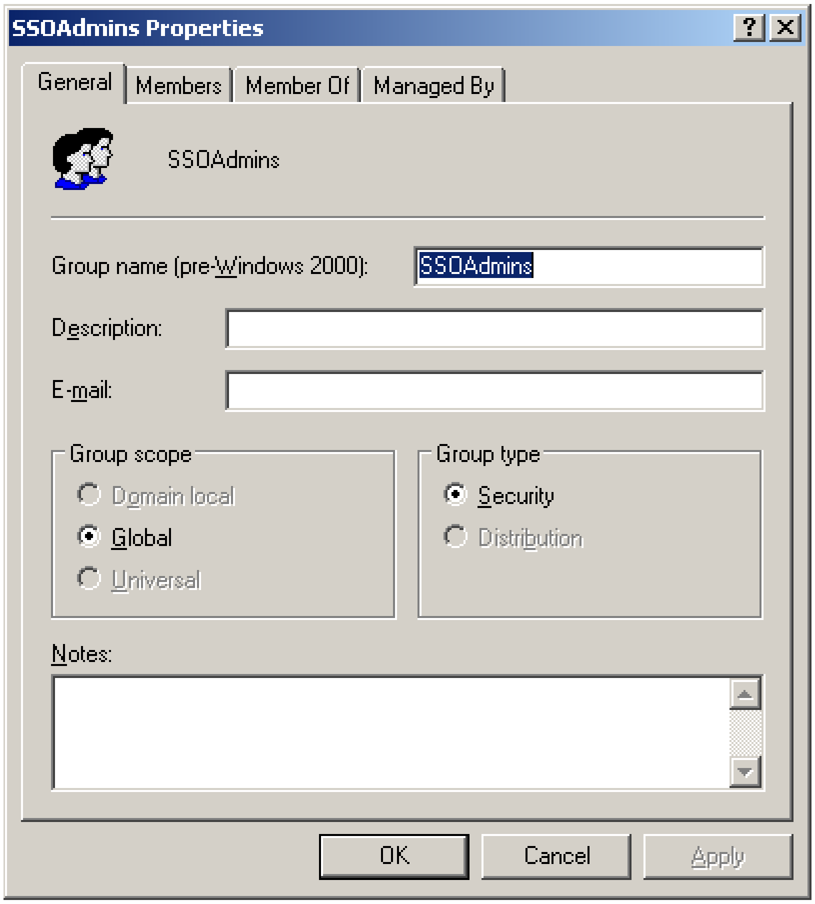
Group name (pre-Windows 2000): SSOAdmins

Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

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.



SSOAdmins

Group name (pre-Windows 2000): SSOAdmins

Description:

E-mail:

Group scope

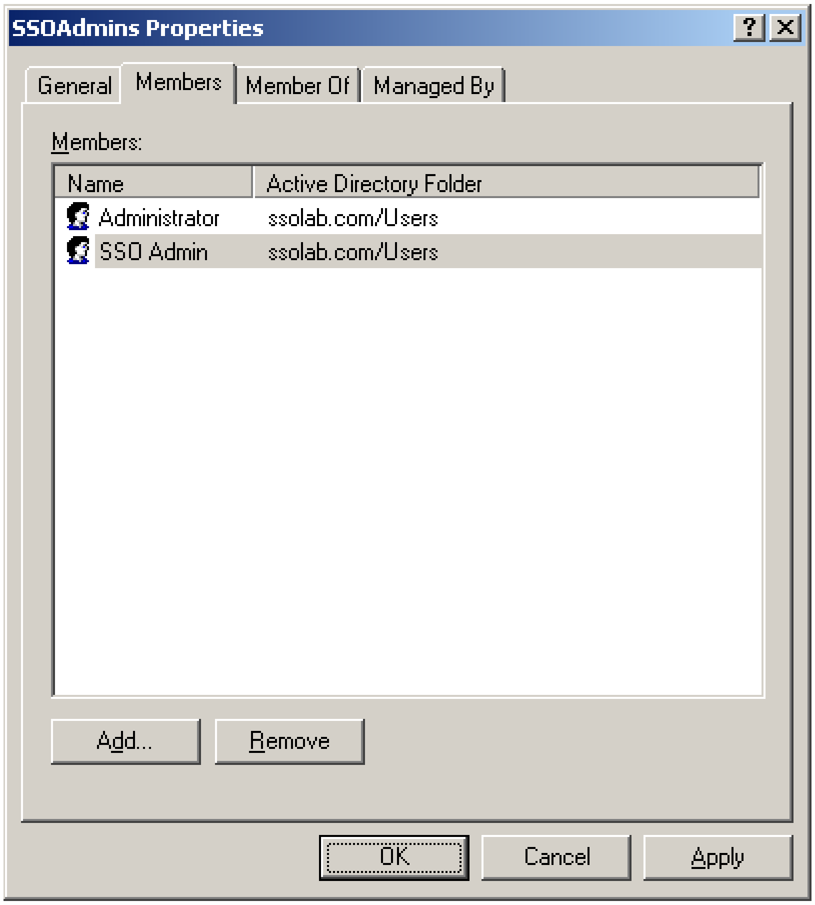
○ Domain local
● Global
○ Universal

Group type

● Security
○ Distribution

Notes:

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.



Name	Active Directory Folder
Administrator	ssolab.com/Users
SSO Admin	ssolab.com/Users

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

Appendix F: Configuring Oracle Internet Directory for Use with Logon Manager

To use Logon Manager with Oracle Internet Directory, you must enable anonymous binding and disable the access control check feature in Oracle Internet Directory as follows:

- Launch a browser and open Oracle Directory Services Manager.
- Log on as the super user, `orcladmin`.
- Click **Connect to a directory** and select the target instance.
- Click the **Data Browser** tab.
- Navigate to the following location: `cn=oid1,cn=osdldapd,cn=subconfigsubentry`
  Change the value of the `orclanonymousbindsflag` from 2 to `1`, then click **Apply**.
- Disable the "Enable Access Control Check" feature:
  a. In the Oracle Enterprise Manager Fusion Middleware Control application, locate the target Oracle Internet Directory instance.
  b. From the **Oracle Internet Directory** menu, select **Administration → Server Properties**.
  c. On the **Server Properties** screen, disable the **Enable Access Control Check** option.
  d. Click **Apply**.

Appendix G: Configuring Oracle Virtual Directory for Use with Logon Manager

To use Logon Manager with Oracle Virtual Directory, you must enable anonymous binding and disable the access control check feature in Oracle Internet Directory as follows:

- Map the user containers of all LDAP servers to the same subtree of the Oracle Virtual Directory directory information tree. For example, the following is the correct layout for DSEE and OID servers mapped to the same OVD instance:
  - `ou=dsee,ou=users,dc=corp,dc=com` (for Oracle DSEE user entries)
- `ou=oid,ou=users,dc=corp,dc=com` (for OID users entries)
  This ensures that the Logon Manager locator-based user lookup mechanism is able to locate users on different servers.
- Ensure anonymous binding is enabled on the mapped LDAP server. Grant search permissions for user list entries to the anonymous user.
- Disable the "Enable Access Control Check" feature:
  a. In the Oracle Enterprise Manager Fusion Middleware Control application, locate the target Oracle Virtual Directory instance.
  b. From the **Oracle Virtual Directory** menu, select **Administration → Server Properties**.
  c. On the **Server Properties** screen, disable the **Enable Access Control Check** option.
  d. Click **Apply**.