ORACLE®

PRIMAVERA

Primavera Portfolio Management 8.0
Using LDAP

Copyright © 1999-2010, Oracle and/or its affiliates.

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

This document describes the integration of Primavera® Portfolio Management with the Lightweight Directory Access Protocol (LDAP). This integration enables organizations to manage users and user groups to be used within Primavera® Portfolio Management, in one central location.

The document contains the following sections:

1. What is LDAP?
2. Properties that are being synchronized
3. Using the Primavera® Portfolio Management Active Directory Synchronization Tool
4. Configuring Primavera® Portfolio Management for automatic, scheduled synchronization

1. What is LDAP?

Lightweight Directory Access Protocol (LDAP) is a system and protocol that enables various applications to exchange information with an organization's central directory of information. Several vendors offer implementations of LDAP; Microsoft's LDAP implementation is called Active Directory. While the Primavera® Portfolio Management Active Directory Synchronization Tool should work properly with any compliant LDAP system, it has been tested only with Microsoft Active Directory.

LDAP implementations such as Microsoft Active Directory allow organizations to define, organize, modify and manage objects such as domains, organizational units, servers and computers, groups of users and users, and others, in one central location. LDAP-aware applications can connect to the central LDAP directory and manage objects that are relevant to them there, or they can periodically connect to the central LDAP directory and synchronize their local lists of relevant objects with the objects found in LDAP.

Note that the functionality of Single Sign-On is not handled through LDAP. LDAP is simply a repository of objects, including users. Allowing those users to login once and then have access to all of their (authorized) applications is a different issue. For more information about the support for Single Sign-On in Primavera® Portfolio Management, see the document "Primavera ProSight 8.0 Enabling Single Sign-On".

LDAP systems arrange the objects of an entire enterprise in tree-like structures. Usually it is not appropriate for specific applications to access or synchronize with the entire content of the LDAP system. A given application typically looks at a specific sub tree within the LDAP system.

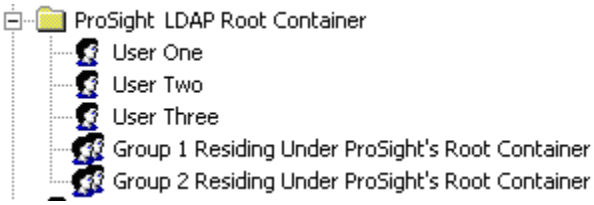
Synchronization typically takes place based on a strict "master-slave" pattern: the LDAP system is the "master", and the application is the "slave".

Primavera® Portfolio Management follows this same pattern and hence can be configured to synchronize with a sub tree residing under a specific container in the LDAP system. Any object within the LDAP system can be considered a container for this purpose; therefore, Primavera® Portfolio Management can be made to synchronize with a sub tree residing under an Organizational Unit, a group, a folder, or any other object. When synchronizing, all users and user groups residing under this container will be created within Primavera® Portfolio Management (if they did not exist) or will be updated to have the same properties as their counterparts in LDAP (if they already existed). Users in Primavera® Portfolio Management that do not exist under the specified container in LDAP will be disabled in Primavera® Portfolio Management, whereas Primavera® Portfolio Management groups that do not exist under the

specified LDAP container will be deleted in Primavera® Portfolio Management (except for specific users and groups that the synchronization process was instructed to ignore).

Note that for the purposes of LDAP synchronization, users that are members of a group which is going to be synchronized according to the rules outlined above, will be synchronized, even if the users themselves really reside elsewhere in the LDAP system (i.e. reside under a different Organizational Unit). In other words, users belonging to a group are considered to "reside" under that group, even though, strictly speaking, the user objects reside elsewhere and the group only contains a reference to these objects.

The above is not true for user groups: user groups that are members of another user group which is going to be synchronized according to the rules outlined above, will not be synchronized unless they themselves also reside under the container that Primavera® Portfolio Management is going to synchronize with. In other words, user groups belonging to a user group will be synchronized only if these groups actually reside under the specified LDAP container.



As an example, given the hierarchy shown above, in which:

- "ProSight LDAP Root Container" is a container created somewhere in the LDAP hierarchy;
- "User One", "User Two" and "User Three" are users that reside under the "ProSight LDAP Root Container";
- "User Four" and "User Five" (not shown above) are users residing elsewhere in the LDAP hierarchy;
- "Group 1 Residing Under ProSight's Root Container" and "Group 2 Residing Under ProSight's Root Container" are user groups that reside under the "ProSight LDAP Root Container";
- "Group 3 Not Residing Under ProSight's Root Container" (not shown above) is a group that resides elsewhere in the LDAP hierarchy;
- "Group 1 Residing Under ProSight's Root Container" has as members: "Group 2 Residing Under ProSight's Root Container", "Group 3 Not Residing Under ProSight's Root Container", "User One" and "User Four";
- "Group 2 Residing Under ProSight's Root Container" has as member: "User Two";
- "Group 3 Not Residing Under ProSight's Root Container" has as members: "User Three" and "User Five";

In this example, the following users will be created/updated in Primavera® Portfolio Management: "User One", "User Two", "User Three" and "User Four", and the following user groups will be created/updated in Primavera® Portfolio Management: "Group 1 Residing Under ProSight's Root Container" and "Group 2 Residing Under ProSight's Root Container". Note that "User Five" will not be created in Primavera® Portfolio Management, and if this user already existed it will be deleted. Also note that "Group 3 Not Residing Under ProSight's Root Container" will not be created in Primavera® Portfolio Management, and if it already existed it will be deleted. Within Primavera® Portfolio Management, "Group 1 Residing Under ProSight's Root Container" will contain "Group 2 Residing Under ProSight's Root Container" and "User One" and "User Four". "Group 2 Residing Under ProSight's Root Container" will contain "User Two". "User Three" will not be residing in any user group in Primavera® Portfolio Management because the

group it is a member of (“Group 3 Not Residing Under ProSight’s Root Container”) does not reside under the “ProSight LDAP Root Container”.

Synchronization is one-way only: users created in Primavera® Portfolio Management that do not exist under the specified container in LDAP will be disabled upon the next synchronization. Properties of users and/or groups that were updated in Primavera® Portfolio Management will be overwritten by the values of these same properties in LDAP upon the next synchronization.

2. Properties that are being synchronized

The following table shows which properties of Primavera® Portfolio Management users are being synchronized with which LDAP properties:

Primavera® Portfolio Management User property	LDAP user property
Login*	sAMAccountName
Whether the user is a user or a contact	ObjectType.Contact
First Name	givenName
Last Name	sn
Title	title
Department	department
Company	company
Telephone number	telephoneNumber
Fax number	facsimileTelephoneNumber
Address	concatenated from LDAP properties “streetAddress”, “postOfficeBox”, “l”, “st”, “postalCode”, and “co”
Email address	mail

*Note: a Primavera® Portfolio Management user and a LDAP user are considered the same user (and will be synchronized) if the Primavera® Portfolio Management user's login name matches the LDAP user's SAMAccountName property.

An existing Primavera® Portfolio Management user that is not present under the LDAP container which is being synchronized with, or which is present but disabled in LDAP, will be disabled, unless listed as a user that should be ignored during LDAP synchronization.

An existing Primavera® Portfolio Management user that is present under the LDAP container which is being synchronized with and is enabled in LDAP, will be enabled.

Users that exist and are enabled in LDAP but do not exist in Primavera® Portfolio Management will be created in Primavera® Portfolio Management, up to the licensed number of named users.

The following table shows which properties of Primavera® Portfolio Management groups are being synchronized with which LDAP properties:

Primavera® Portfolio Management group property	LDAP group property
Name*	name
Description	description

*Note: a Primavera® Portfolio Management group and a LDAP group are considered the same group (and will be synchronized) if the Primavera® Portfolio Management group's name matches the LDAP group's name property.

An existing Primavera® Portfolio Management group that is not present under the LDAP container which is being synchronized with, will be deleted in Primavera® Portfolio Management, unless listed as a group that should be ignored during LDAP synchronization.

Groups that exist in LDAP but do not exist in Primavera® Portfolio Management will be created in Primavera® Portfolio Management.
All members of the group in LDAP will be made members of the group in Primavera® Portfolio Management. Members of the group in Primavera® Portfolio Management that are not members of the group in LDAP will be removed from the group in Primavera® Portfolio Management.

Groups in LDAP which have the property isCriticalSystemObject set to TRUE will not be synchronized with Primavera® Portfolio Management. This includes most built-in groups such as Domain Admins, Domain Users, etc.

3. Using the Primavera® Portfolio Management Active Directory Synchronization Tool

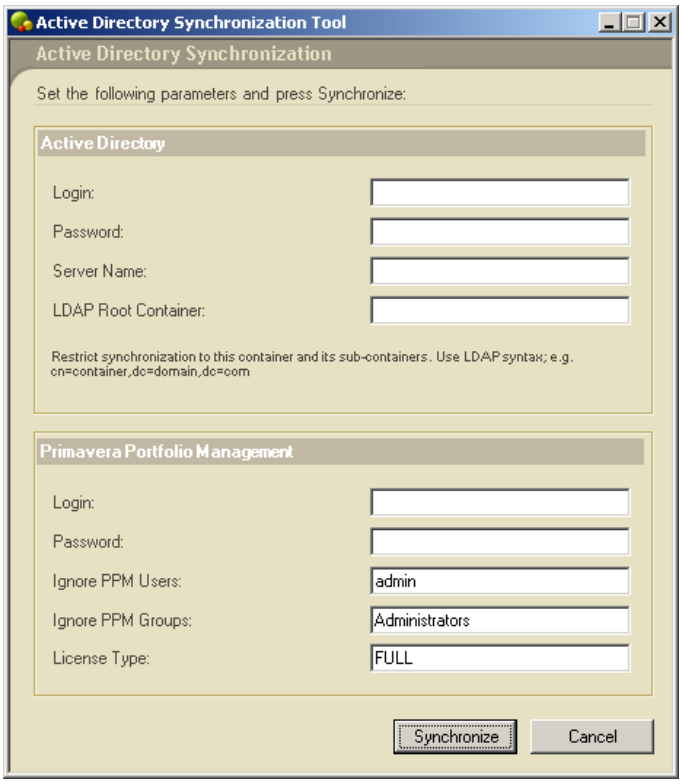
Note: in a distributed installation of Primavera® Portfolio Management ("Scale Out"), the below described tool can be used from any one of the Primavera® Portfolio Management application servers.

This section outlines the use of the Primavera® Portfolio Management Active Directory Synchronization Tool.

3.1 Double-click the file **psActiveDirectorySync.exe** located in the "bin" subfolder of the Primavera® Portfolio Management installation directory. By default, this is located at C:\Program Files\Oracle\Primavera Portfolio Management\Portfolios\bin.

The Active Directory Synchronization Tool, depicted on the right, will appear.

This tool is used for one-time, user-driven synchronization with LDAP.



3.2 The group box **Active Directory** in the Active Directory Synchronization Tool contains the fields relevant to Active Directory that must be filled in for Primavera® Portfolio Management to connect successfully to LDAP. Within this group box, the following fields can be found:

Login:	the Windows login name of a user with access to the LDAP server.
Password:	the password of the user with access to the LDAP server.
Server Name:	the name of the LDAP server
LDAP Root Container:	the container within LDAP that contains the sub tree of users and user groups relevant to Primavera® Portfolio Management. The container is specified using LDAP syntax such as `cn=container,dc=domain,dc=com`. Any object can be specified in this field using this syntax.

3.3 The group box **Primavera Portfolio Management** in the Active Directory Synchronization Tool contains the fields relevant to Primavera® Portfolio Management that must be filled in for the tool to be able to connect successfully to Primavera® Portfolio Management. Within this group box, the following fields can be found:

Login:	the Primavera® Portfolio Management login name of a user with administrative rights to Primavera® Portfolio Management.
Password:	the Primavera® Portfolio Management password of this user.
Ignore PPM Users:	a list of Primavera® Portfolio Management login names, separated by semicolons, that will not be synchronized with LDAP. By default, the login name of the Primavera® Portfolio Management System Administrator, “admin”, is listed here, to avoid causing this user to become disabled upon running a LDAP synchronization.
Ignore PPM Groups:	a list of Primavera® Portfolio Management group names, separated by semicolons, that will not be synchronized with LDAP. By default, the group name “Administrators” is listed here to avoid causing this group to either get deleted or contain the names of (Windows) Administrators as defined in LDAP.
License Type:	the license type that will be assigned to each new user synchronized with LDAP. The options are: FULL – new users will be assigned full licenses READ – new users will be assigned read-only licenses FORM – new users will be assigned forms-only licenses

3.4 When the required information in all fields has been entered, click **Synchronize** to start the LDAP synchronization process. Click **Cancel** to exit the tool without performing synchronization.

Note that the information entered in these fields is not saved to the database and does not affect any other, scheduled, LDAP synchronization.

4. Configuring Primavera® Portfolio Management for automatic, scheduled synchronization

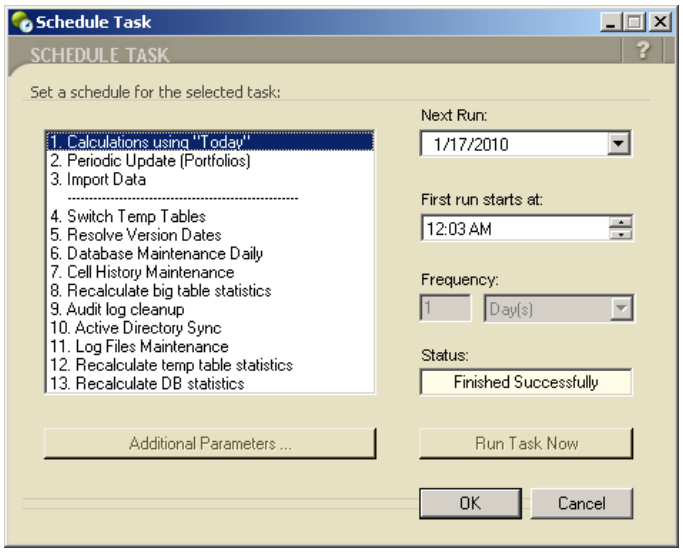
Note: in a distributed installation of Primavera® Portfolio Management ("Scale Out"), the below described tool can be used from any one of the Primavera® Portfolio Management application servers.

This section outlines configuring for automatic scheduled LDAP synchronization.

4.1 Double-click the file **psScheduleTasks.exe** located in the "bin" subfolder of the Primavera® Portfolio Management installation directory. By default, this is located at C:\Program Files\Oracle\Primavera Portfolio Management\Portfolios\bin.

Log in with a Primavera® Portfolio Management user name and password.

The Schedule Tasks tool, depicted on the right, will appear.

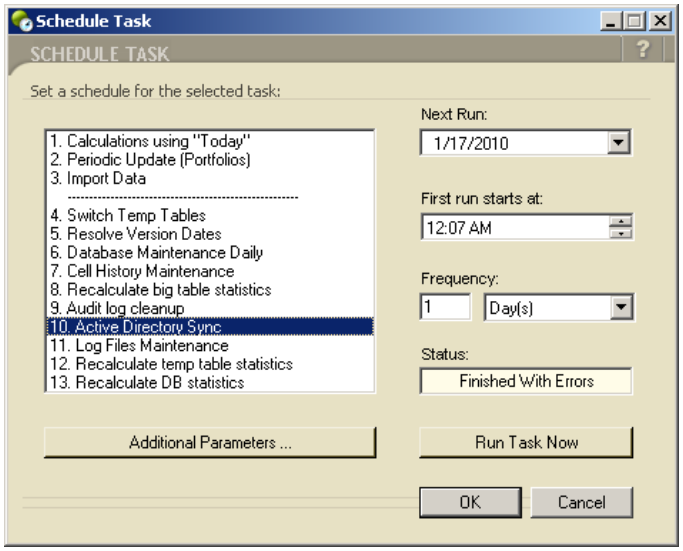


4.2 Select **10. Active Directory Sync**, in the list of tasks.

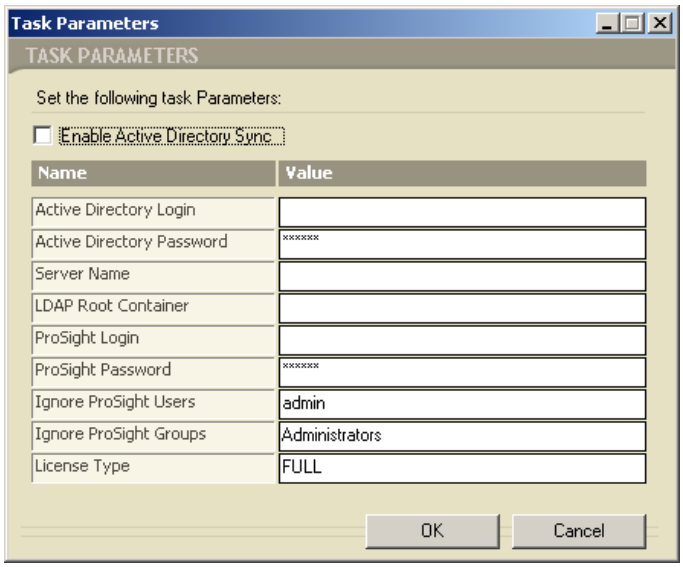
4.3 Next to **Next Run**, select the date for the next synchronization.

4.4 Next to **First run starts at**, select the time of day at which the synchronizations should start running.

4.5 Next to **Frequency**, select the frequency with which the synchronization should take place.



4.6 Click **Additional Parameters**.



4.7 Place a checkmark in the checkbox next to **Enable Active Directory Sync**. To temporarily disable this task, it is possible to clear this checkbox without the need to clean out the other fields.

4.8 Next to **Active Directory Login**, enter the Windows login name of a user with access to the LDAP server.

4.9 Next to **Active Directory Password**, enter the password of the user with access to the LDAP server.

4.10 Next to **Server Name**, enter the name of the LDAP server with which the synchronization should take place.

4.11 Next to **LDAP Root Container**, enter the container within LDAP that contains the sub tree of users and user groups relevant to Primavera® Portfolio Management. The container is specified using LDAP syntax such as `cn=container,dc=domain,dc=com`. Any object can be specified in this field using this syntax.

4.12 Next to **ProSight Login**, enter the Primavera® Portfolio Management login name of a user with administrative rights to Primavera® Portfolio Management.

4.13 Next to **ProSight Password**, enter the Primavera® Portfolio Management password of this user.

4.14

Next to **Ignore ProSight Users**, enter a list of Primavera® Portfolio Management login names, separated by semicolons, that will not be synchronized with LDAP. By default, the login name of the Primavera® Portfolio Management System Administrator, “admin”, is listed here, to avoid causing this user to become disabled upon running a LDAP synchronization.

4.15

Next to **Ignore ProSight Groups**, enter a list of Primavera® Portfolio Management group names, separated by semicolons, that will not be synchronized with LDAP. By default, the group name “Administrators” is listed here to avoid causing this group to either get deleted or contain the names of (Windows) Administrators as defined in LDAP.

4.16

Next to **License Class**, enter the type of license that should be assigned to new users.

4.17 When all fields have been defined as required, click **OK** to accept the entered values and close the Task Parameters window.

4.18 On the Schedule Tasks window, click **OK** to accept all entered values and schedule the LDAP synchronization task as specified.

4.19 Restart Primavera® Portfolio Management for the changes to take effect.