

Primavera® P6™ Integration API

Administrator's Guide

Version 6.2.1

Copyright © 2003, 2009, Oracle and/or its affiliates. All rights reserved.

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, JD Edwards, PeopleSoft, and Siebel are registered trademarks 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.

To view the P6 Commercial Notices and Disclosures for Documentation, go to the \Documentation\<language>\Notices and Disclosures folder of the P6 physical media or download. After installing Primavera P6 Integration API, it is also available in the \docs folder of your Primavera P6 Integration API installation folder.

Table of Contents

Preface.....	v
Using this Administrator's Guide	vi
Where to Get Support	vii
Installing the Integration API.....	1
What is the Integration API?.....	2
System Requirements.....	3
Integration API Installation Process	4
Deploying the Integration API for Remote Mode	7
Changing Database Configuration Settings	12
Enabling Access.....	13
Java Security Manager	14
Using the Primavera Administrator Application	15
Starting the Primavera Administrator Application	16
Reviewing and Modifying Integration API Configurations.....	17
Integration API Configuration Settings	21
Configuring Authentication Modes	45
Authentication Modes	46
Implementing Non-Native Authentication.....	47
Choosing an Authentication Scheme	48
Running the Authentication Configuration Wizard	49
Configuring Integration API Authentication	60
Logon/Logout Changes to Support Authentication Modes	61
Index.....	63

Preface

In this preface:

[Using this Administrator's Guide](#)

[Where to Get Support](#)

The Primavera Integration API is a Java-based API and server that enables developers to create client code that can seamlessly access Primavera's project management functionality.

Using this Administrator's Guide

This guide describes the steps required to install the Primavera Integration API and how to configure it to use one of three authentication modes. It is organized as follows:

Installing the Integration API Describes how to install the Primavera P6 Integration API and explains how to use the Primavera Administrator to review, modify, add, and delete Integration API server configurations.

Configuring Authentication Modes Describes the authentication modes available in this release and explains how to configure the Primavera Integration API to operate using one of three authentication modes.

Where to Get Support

If you have a question about using Primavera products that you or your network administrator cannot resolve with information in the documentation or Help, contact Primavera Customer Support at the times and locations listed below.

Please provide your Primavera product serial number when contacting Primavera. Each interaction is logged to help Primavera resolve your questions quickly.

Office	Time Zone	Hours	Telephone	FAX	E-mail Address*
Bala Cynwyd, Pennsylvania, USA	ET	8:00–8:00 (Mon–Fri) 9:00–2:00 (Sat)	+1-610-668-3030	+1-610-667-0652	support@primavera.com
London, England, UK	GMT	8:30–6:30 (Mon–Thur) 8:30–5:30 (Fri)	+44-20-8563-5555	+44-20-8563-5543	support@primavera.com
Hong Kong	GMT +8	8:00–5:00 (Mon–Fri)	+852-2111-8299	+852-2111-9477	support@primavera.com

*Primavera's Web site at <http://www.primavera.com/customer/index.asp> provides support and product information, such as knowledge bases, file downloads, user group and newsgroup information, and a product enhancement request form.



In the United States, Primavera periodically and randomly monitors technical support calls to ensure that you receive the highest quality support.

All Primavera products are backed by comprehensive support and training.

Installing the Integration API

In this chapter:

What is the Integration API?

System Requirements

**Integration API Installation
Process**

**Deploying the Integration API for
Remote Mode**

**Changing Database Configuration
Settings**

Enabling Access

Java Security Manager

**Using the Primavera
Administrator Application**

**Starting the Primavera
Administrator Application**

**Reviewing and Modifying
Integration API Configurations**

**Integration API Configuration
Settings**

This chapter describes how to install the Primavera Integration API. In addition, this chapter explains how to use the Primavera Administrator to review, modify, add, and delete Integration API server configurations.

What is the Integration API?

The Primavera Integration API is a Java-based API and server that enables developers to create client code that can seamlessly access Primavera's project management functionality.

System Requirements

The Primavera Integration API has the following system requirements for both local and remote mode installations:

Java Runtime Environment

- If you write code against the interface, you need to install the Java Development Kit (JDK), version 1.5.x, also known as J2SE 5.0. While the Primavera Integration API is compatible with any 1.5 version, we recommend using Update 13 or later. The Integrated Development Environment (IDE) you use to create code must work with this version.
- If you do not plan on writing code against the interface and will only be running the sample applications, you will need to install only the Java Runtime Environment (JRE), version 1.5.x, also known as J2SE 5.0. While the Primavera Integration API is compatible with any 1.5 version, we recommend using Update 13 or later.

You can download the JRE or Java JDK from the Sun Microsystems Web site. If you are using the Java JDK, ensure that it is installed before running the Integration API setup.

Operating Systems

- The Primavera Integration API is fully supported on Windows, Solaris, and Linux operating systems.



Even though the JRE and JDK are available on other operating systems, they have not been tested by Primavera Systems.

For the full list of supported operating systems and database versions, refer to the `testedcfg.pdf` file, which is provided in the `\Documentation\<language>\Technical Documentation` folder on the P6 physical media or download.

Project Management Database

- A Primavera P6 project management database (Oracle, SQLServer, and SQL Server Express are supported)

Application Servers

Remote mode installations of the Primavera Integration API require one of the following supported application servers:

- JBoss 4.0.5
- BEA WebLogic Server 10
- IBM WebSphere Application Server 6.1

Integration API Installation Process

For information on installing the project management database and the client application, see the *Primavera P6 Administrator's Guide* (adminguide.pdf), which is provided in the \Documentation\<language>\<industry> folder on the P6 physical media or download.

Before installing the Integration API, you need to install the project management database and the P6 Project Management client module. Additionally, you must uninstall any earlier versions of the API before installing the current version.



The Primavera Project Management client module does not have to be installed on the same server as the Primavera Integration API.

The Integration API Installer provides a wizard to guide you through the installation process, which includes

- Choosing the installation mode
- Installing the Integration API client side and server side libraries
- Setting up and configuring the Integration API database



Before you start the installation, make sure you set the JAVA_HOME environment variable.

To install the Integration API

- 1 Go to the root folder of the Integration API Installation CD-ROM:

For the Windows platform, double-click `setup.exe`.

For the Solaris platform, run `setupSolaris.bin`

For the Linux platform, run `setupLinux.bin`



Click Next on each wizard dialog box to advance to the next step.

- 2 On the **Welcome** screen, click **Next**.
- 3 On the **Please select the installation type** screen, specify the installation mode.

Local Mode - Choose this option to use the API in local mode, without Java RMI.

This option installs client-side and server-side Java libraries, database configuration tools, and javadoc.

Client Side Packages Only - Choose this option to use the API in remote mode. This option installs client-side Java libraries and javadoc.



The maximum number of clients that can access a remote server at one time is approximately 50. This number may be less, depending on multiple factors (e.g., system hardware, network configuration, the number of available licenses, etc.).

After installing the client-side packages, to complete a remote mode installation, install the Integration API on a separate machine using the following option.

- Supported J2EE compatible application or Web servers

This option installs the Integration API application file, `PrimaveraAPI.war`, into the `applications` subdirectory of the destination you specify in the wizard.

The `PrimaveraAPI.war` file contains both client-side and server-side libraries, database configuration tools, and the javadoc. You can deploy the Integration API as a Web application into any J2EE-compatible application or Web server that supports JDK/JRE 1.5.x.

- 4 On the **Please specify the location of . . .** dialog box, type or browse to the Integration API installation location and the location of the JRE.

The default location of the Integration API is:

`c:\Program Files\Primavera\IntegrationAPI`

The default location of the JRE is:

`c:\Program Files\Java\jre1.5.x`

The setup wizard should detect and prefill the location of the JDK. Edit the location if desired.

If you setup the `JAVA_HOME` environment variable, the location of the JRE is automatically filled in for you.

- 5 On the **Please select the components . . .** dialog box, select the components to install, then click **Next** to start the installation.
- 6 On the dialog box that lists the components and features to be installed, click **Next** to start the installation.
- 7 On the **Setup and Configuration of the Primavera Database** dialog box, specify the database type.
- 8 On the **Please enter the following information . . .** dialog box, specify the database connection parameters.

You can later change the database type through the Integration API Database Configuration Setup.

For more information about configurations, see [“Using the Primavera Administrator Application”](#) on page 15.

The Integration API requires **pubuser** access (in the User Name field) to the database. The database name, host address, and host port are specific to your Oracle or MS SQL Server installation. Database Host Port displays the default port for the database type you selected. You can edit this port.

- 9 On the **The installer has detected an existing . . .** dialog box, choose the appropriate action.

The configuration stores server-side settings for the server.



If your site includes P6 Web Access, you can share a new Integration API configuration with P6 Web Access. However, an existing configuration for P6 Web Access cannot be shared with the Integration API because it will not provide support for new Integration API configuration settings.

If there is no existing configuration, the **The installer has detected an existing . . .** dialog box does not appear and the installation process automatically creates a default configuration named Primavera Configuration. You can edit the settings for this configuration through the Primavera Administrator Application.



After installation, you can use the Database Configuration Setup wizard to choose or create a different configuration, if necessary.

- 10 When the message displays to confirm that the database configuration has completed successfully, click **OK**. Then, click **Finish** to close the Setup wizard.

You will now have the following shortcuts appended to the Primavera Integration API entry in your Start menu:

- Demo applications
- Documentation (Java API Documentation, License, Programmer’s Reference, Release Notes, and Readme)
- Configuring the database connection
- Running the Administrator application
- Starting and stopping the application server (Remote mode installation only)
- Uninstall Primavera Integration P6 API

Deploying the Integration API for Remote Mode

If you selected **Supported J2EE compatible application or Web servers** when installing the Integration API, you need to then deploy the API into the appropriate application or web server that supports JDK/JRE 1.5.x.



Refer to your application server documentation for detailed deployment instructions.

Deploying into JBoss 4.0.5 on Windows

Do the following to deploy the Integration API into JBoss on Windows:

When deploying into JBoss, note the following:

- 1 Go to the <JBoss INSTALL LOCATION>\server folder.
- 2 Select the folder named 'default' and create a copy of it.
- 3 Rename the copied folder to primaveraAPI.
- 4 Copy the PrimaveraAPI.war file from the Integration API home folder to the following JBoss folder.

<JBoss INSTALL LOCATION>\server\primaveraAPI\deploy\

- 5 For international support, edit the following file:

<JBoss INSTALL LOCATION>\server\primaveraAPI\deploy\jbossweb-tomcat55.sar\server.xml

In the Connector setting, add the parameter
URIEncoding="UTF-8".
For example:

```
<!--A HTTP/1.1 Connector on port 8080-->
<Connector port="8080" URIEncoding="UTF-8"
address="{jboss.bind.address}"
maxThreads="250" strategy="ms" maxHttpHeaderSize="8192"
emptySessionPath="true"
enableLookups="false" redirectPort="8443" acceptCount="100"
connectionTimeout="20000" disableUploadTimeout="true"/>
```



When you are using the SSL-connector, add this parameter to its settings as well.

- 6 In the run.bat file in the bin folder, insert the following line before the :RESTART line:

```
set JAVA_OPTS="-Dprimavera.bootstrap.home=<Integration API home>" %JAVA_OPTS%
```

Change <Integration API home> to the appropriate location/

- 7 Create a bat file named startPrimaveraAPIinJboss.bat that contains the following:

```
@echo off
set JBOSS_HOME=C:\jboss-4.0.5.GA
call %JBOSS_HOME%\bin\run.bat -c primaveraAPI
```

This bat file is necessary for starting the JBoss application server.

Deploying into Weblogic 10



Note: We recommend that the WebLogic application server should be set to run in "non-production" mode (i.e. Development Mode). To run in non-production mode, the WebLogic Startup Parameter "StartMode=" must be left blank. After performing the steps below to complete the Integration API deployment, set the WebLogic Startup Parameter "StartMode=" to true and reboot the WebLogic application server.

However, if you want to keep the WebLogic application server in production mode, you need to manually deploy the `PrimaveraAPI.war` file.

Do the following to deploy the Integration API into Weblogic:

- 1 Run the WebLogic Configuration Wizard to create a server domain for the Integration API application. On the Configure Server Start Mode and JDK window, you **MUST** select Development Mode in the WebLogic Domain Startup Mode left hand pane.
- 2 Copy the PrimaveraAPI.war file from the Integration API home folder to the following WebLogic folder for auto-deployment.

`<bea_home>\user_projects\domains\<integration API domain>\autodeploy`

- 3 Edit the file startweblogic.sh (Unix) or startweblogic.cmd (Windows) in the `<bea_home>\user_projects\domains\<integration API domain>\bin\` folder as follows:

- Add the Integration API bootstrap variable to the Java options. Before editing, make a backup copy of the file in case you need to undo any changes.

Windows example:

```
set JAVA_OPTIONS=-Dprimavera.bootstrap.home="<integration API
home folder>"
```

Unix example:

```
JAVA_OPTIONS="-Dprimavera.bootstrap.home=<Integration API
home>${SAVE_JAVA_OPTIONS}"
```

Deploying into Websphere 6.1

Do the following to deploy the Integration API into Websphere:

- 1 Start the Websphere Application Server.
- 2 Launch the WebSphere Application Server Administrative Console.
- 3 In the left-hand navigation pane, expand Servers and click Application Servers.
- 4 On the Application Servers screen, click the server name link.
- 5 On the Configuration tab, under Server Infrastructure, expand Java and Process Management.
- 6 Click Process Definition.
- 7 Under Additional Properties, click Java Virtual Machine.
- 8 Under Generic JVM arguments, type:
`-Dprimavera.bootstrap.home=c:\apihome`
(where 'c:\apihome' is the installation directory).
- 9 Click OK. Click the Save link that appears within the message reporting changes.
- 10 In the left-hand navigation pane, expand Applications and click Install New Application.
- 11 Specify the path to the war file in the apihome folder. For example:
`c:\apihome\applications\primaveraapi.war`
- 12 For the Context Root, type `apiprimavera`, then click Next.
- 13 In the Step 1 section "Select Installation Options", click Next.
- 14 In the Step 2 section "Map Modules to Servers", mark the Primavera Integration API checkbox, and click Next.
- 15 In the Step 3 section "Map Virtual Host for Web Modules", mark the Primavera Integration API checkbox, and click Next.
- 16 On the Step 4 screen (Summary), click Finish. Note that the application war file is now deploying and this process may take several minutes.
- 17 To save the master Websphere configuration, click Save. This process may also take several minutes.

- 18 On the Administrative Console Main screen, in the left-hand navigation, expand Applications and click Enterprise Applications.
- 19 Locate PrimaveraAPI.war and check its application status. If it is not a green arrow, click the Start button above the Select column.
- 20 If necessary, restart the Websphere application server.

Changing Database Configuration Settings

The Integration API Database Configuration wizard lets you create a new configuration or switch to a different configuration than the one specified during the Integration API installation.

The database you connect to during the installation stores one or more Integration API configurations. Each configuration specifies a set of configurable parameters that determine how the Integration API operates. The first time you install the Integration API, and if no configuration exists in the database, you must create a new configuration. For subsequent installs, you can choose an existing configuration or create a new one. After installation, you can use the Database Configuration wizard to select a different Integration API configuration or create a new one.



After selecting a different Integration API configuration or creating a new configuration, you must stop and restart the server for the changes to take effect.

Starting the Database Configuration wizard

- On Windows, from the Start menu, choose Programs, Primavera Integration API 6.2, Database Configuration.
- On Solaris/Linux, change to the PrimaveraAPI directory under the application server install directory and run the `dbconfig.sh` script.

Enabling Access

Before users can log in to the API, they must be granted access via a named license in the Project Management module (select Admin, Users; click the Licensing tab; mark the box under Named User for Integration API).

Java Security Manager

The Java security manager enables programmers to establish a custom security policy for their Java applications.



The Java security manager is not supported for IBM WebSphere Application Server v 6.1.

Unless it is specifically enabled when the API server is started, the security manager is disabled. To enable/disable the security manager, edit the API server's startup script with a text editor and uncomment/comment the appropriate command (see below).

For Windows platforms, edit `startAppServer.cmd`. For Solaris/Linux, edit `startAppServer.sh`.

WebLogic 10

Windows:

SET ENABLE_JAVA_SECURITY_MANAGER=-Djava.security.manager

Solaris/Linux:

ENABLE_JAVA_SECURITY_MANAGER=-Djava.security.manager



The API server may use different policy files for different application/web servers.

Using the Primavera Administrator Application

As the system administrator, you can use the Primavera Administrator Application to review, modify, add, and delete server configurations. Integration API server configurations are stored in the database specified during installation. These configurations contain all of the settings used to run the Integration API server.



Only experienced administrators should use the Administrator Application to modify configuration settings.

Starting the Primavera Administrator Application

After launching the Administrator Application, you will be prompted for a database level password for the **privuser** account.

Starting the Administrator Application

- On Windows, from the Start menu, choose Programs, Primavera Integration API 6.2, Primavera Administrator.
- On Solaris/Linux, change to the PrimaveraAPI directory under the application server install directory and run the `admin.sh` script.

Reviewing and Modifying Integration API Configurations

The Primavera Administrator Application presents configuration settings in a tabbed dialog box. Tree view and Table view display the current configurations and settings. Log displays a history of configuration changes, additions, or deletions for the current session.



You cannot edit the Factory Default configuration settings. You can only modify custom configurations.

To display brief setting descriptions in Tree or Table view, mark the Show tool tips checkbox. Then, position the mouse over a setting to read the popup description.

Click to display a hierarchical view of the configuration data.

To return a setting to its default value, select it, then right-click and choose Revert to default value. To change a setting value, triple-click on the setting name, then type a new value. On Windows, you can also press F2 to change to Edit mode.

Configuration	Setting Name	Value
Factory Defaults	Database.Instance[1].SessionSetting...	
Factory Defaults	Database.Instance[1].SessionSetting...	
Factory Defaults	Database.Instance[1].URL	jdbc:oracle:thin:@10.12.62.86:1521:athens26
Factory Defaults	Database.Instance[1].UserName	pubuser
Factory Defaults	IntegrationServer.RMI.CompressionS...	<input checked="" type="checkbox"/>
Factory Defaults	IntegrationServer.RMI.CompressionS...	0
Factory Defaults	IntegrationServer.RMI.Enable	<input checked="" type="checkbox"/>
Factory Defaults	IntegrationServer.RMI.HTTPServiceE...	<input type="checkbox"/>
Factory Defaults	IntegrationServer.RMI.HTTPServicePort	0
Factory Defaults	IntegrationServer.RMI.HTTPServiceP...	<input type="checkbox"/>
Factory Defaults	IntegrationServer.RMI.RegistryPort	9099
Factory Defaults	IntegrationServer.RMI.SSLServiceEna...	<input checked="" type="checkbox"/>
Factory Defaults	IntegrationServer.RMI.SSLServicePort	0
Factory Defaults	IntegrationServer.RMI.StandardServi...	<input checked="" type="checkbox"/>
Factory Defaults	IntegrationServer.RMI.StandardServi...	0
Factory Defaults	IntegrationServer.SessionTimeOut	120

Click to display configuration settings in a table format.

To change a setting value, select the setting, click in the Value column, then type a new value.

To sort the table, click a column heading. Sorting can help you distinguish similar settings contained in multiple configurations.

Configuration	Setting Name	Value
Factory Defaults	Database.Instance[1].SessionSetting...	
Factory Defaults	Database.Instance[1].SessionSetting...	
Factory Defaults	Database.Instance[1].URL	jdbc:oracle:thin:@10.12.62.86:1521:athens26
Factory Defaults	Database.Instance[1].UserName	pubuser
Factory Defaults	IntegrationServer.RMI.CompressionS...	<input checked="" type="checkbox"/>
Factory Defaults	IntegrationServer.RMI.CompressionS...	0
Factory Defaults	IntegrationServer.RMI.Enable	<input checked="" type="checkbox"/>
Factory Defaults	IntegrationServer.RMI.HTTPServiceE...	<input type="checkbox"/>
Factory Defaults	IntegrationServer.RMI.HTTPServicePort	0
Factory Defaults	IntegrationServer.RMI.HTTPsServiceE...	<input type="checkbox"/>
Factory Defaults	IntegrationServer.RMI.HTTPsServiceP...	0
Factory Defaults	IntegrationServer.RMI.RegistryPort	9099
Factory Defaults	IntegrationServer.RMI.SSLServiceEna...	<input checked="" type="checkbox"/>
Factory Defaults	IntegrationServer.RMI.SSLServicePort	0
Factory Defaults	IntegrationServer.RMI.StandardServi...	<input checked="" type="checkbox"/>
Factory Defaults	IntegrationServer.RMI.StandardServi...	0
Factory Defaults	IntegrationServer.SessionTimeOut	120

Add Integration API configurations To create a new configuration, you can duplicate an existing configuration.

- To duplicate a configuration, select the configuration name in Tree View, then right-click and choose Duplicate. Enter a name for the configuration, then click OK. Edit the settings as needed.
- To create a new configuration based on factory default settings, right-click on Factory Defaults in Tree View and choose Duplicate.

Add database instances to a configuration The Integration API enables you to access data from different project manager databases. When you configure the Integration API to support multiple database instances, you can choose the instance you want at login.

To add a new database instance to an Integration API configuration, you duplicate an existing instance.

- To duplicate a database instance, select the icon representing the instance, then right-click and choose Duplicate. Enter a unique name for the new instance and edit other settings as needed.

Delete Integration API configurations and database instances

To delete a configuration or database instance, select it, then right-click and choose Delete.

You cannot delete the Factory Defaults configuration. You can delete any custom configuration, but not all of them. There must always be at least one custom configuration.

You can delete any database instance associated with a configuration, but not all of them. Each configuration must have at least one database instance.

For more information, see **Database.Instance.Driver** and **Database.Instance.URL** in the [“Integration API Configuration Settings”](#) on page 21.

Database driver configurations The following table lists the database drivers the Integration API supports for each application server/database configuration. Use the `Database.Instance.Driver` configuration setting to specify the database driver you are using.

Application Server	Database Type	Database Driver	Default
WebLogic	Oracle	Oracle Thin Client	Y
WebLogic	SQL Server, SQL Server Express	SQL Server 2005 JDBC	Y
JBoss	Oracle	Oracle Thin Client	Y
JBoss	SQL Server, SQL Server Express	SQL Server 2005 JDBC	Y
WebSphere	Oracle	Oracle Thin Client	Y
WebSphere	SQL Server, SQL Server Express	SQL Server 2005 JDBC	Y

Configure Integration API Authentication The Integration API uses a single configuration setting to support authentication.

■ `Authentication.Mode`

Because one Integration API server instance may control more than one database, in addition to specifying an authentication mode for a database through the Authentication Configuration wizard, you use the `Authentication.Mode` configuration setting to specify the overall mode you want to use for the Integration API server. For LDAP authentication with secure communication (SSL) between the Integration API server and the LDAP server, two additional configuration settings are required.

For more information about each of these settings, refer to the “[[Authentication Settings](#)]” on page 22.



An Integration API configuration might include database instances that are not set to the same authentication mode as the Integration API server. If a user connects and requests a database that is set to a different authentication mode than the Integration API server, an error message displays. The user must select a database that matches the authentication mode set for the Integration API server.

Integration API Configuration Settings

You can review and modify configuration settings in the Primavera Administrator Application Tree View or Table View. Configuration settings are stored in the Integration API database specified during installation.



Only experienced administrators should use the Primavera Administrator Application to modify configuration settings.



Localization settings are not applicable for the Integration API.

You can specify durations (time-related values) in several ways:

- As a simple number, which is treated as milliseconds.
For example, 240000 would be equivalent to 4 minutes (240000/60000).
- In the form <n>d<n>h<n>m<n>s, where “d” is days, “h” is hours, “m” is minutes, and “s” is seconds. All parts are optional.

For example, you can enter:

1d2h30m20s

4m

1h30s

[Localization Settings]

Setting Name and Description	Default	Valid Ranges/Values
Localization/System Language Language for server string constants	en	—
Localization/System Country Country for server string constants	US	—

[Authentication Settings]

Setting Name and Description	Default	Valid Ranges/Values
Authentication/Mode The method used for client authentication.	NATIVE	Native, LDAP, WebSSO
Authentication/Web Single Sign-On/User Name Header Key The name of the http header you specified in SiteMinder. The value you specify must match the property of a SiteMinder response you have created under the policy domain/realm within which the Web server for P6 Web Access resides. The value of this response should be smuser=uid, where smuser is configurable and uid matches the LDAP server attribute that maps to the Primavera database USER_Name field.	smuser	—
Authentication/Web Single Sign-On/Context Path Override The path used to pass web requests from the SiteMinder Web server to the server of P6 Web Access.	/Primavera	—
Authentication/Web Single Sign-On/Server and Port Override The fully qualified domain name and port for the Web server that SiteMinder is controlling.	http:// servername.domain.co m:82	—
Authentication/LDAP/SSL Certificate Store The full path to the keystore that holds the SSL certificate for the LDAP server.	—	—
Authentication/LDAP/SSL Store Password The password for the keystore that holds the SSL certificate.	—	—

[Database Settings]

Setting Name and Description	Default	Valid Ranges/Values
Database/Instance/Name The name of this database instance.	—	up to 32 characters
Database/Instance/Description A description of this database instance.	—	up to 128 characters
Database/Instance/Schema The schema that will be defined for the database.	PMDB	—
Database/Instance/URL The database URL used to establish a connection to the database. Oracle example: jdbc:oracle:thin:@xx.xxx.xxx.xx:yyyy:zzzz SQL example: jdbc:sqlserver://xxxx:yyyy;database=zzzz; x = IP address or hostname y = database listen port z = database name	—	—
Database/Instance/Public Group ID The public group ID used to establish a connection to the database.	1	—
Database/Instance/User Name The name used to establish a connection to the database.	pubuser	—
Database/Instance/Password The password used to establish a connection to the database.	pubuser	—
Database/Instance/User Security/Log Login Attempts Specifies whether or not login attempts to P6 Web Access are tracked in the Web Access logs.	All	All, None, Failed Attempts, Successful Attempts
Database/Instance/User Security/Login Lockout Count The number of times a user can attempt to login before the account is locked. A setting of “0” allows an unlimited number of attempts. The count resets after each successful login.	0	0-100000

[Database Settings]

Setting Name and Description	Default	Valid Ranges/Values
Database/Instance/User Security/Login Lockout Duration The length of time that a user is blocked from logging into P6 Web Access, starting from the point at which the Logging Lockout Count was exceeded. This setting will be overridden if a user's session is manually reset by an Admin Super user. For more information, see the <i>Primavera P6 Administrator's Guide</i> .	1h	0-24d
Database/Instance/User Security/Allow Multiple User Sessions Specifies whether a single user can be simultaneously logged into Web Access. A setting of "Yes" will allow a single user to login multiple times on any machine. A setting of "No" restricts a user to logging in only once on any machine. A setting of "Single Machine" allows a user to log in multiple times on the same machine, as long as the application server is configured properly to determine the IP address of the machine making the request. For example, if the application server is behind a proxy server, this setting will default to "Yes" instead of "Single Machine."	Yes	Yes, No, Single Machine
Database/Instance/Connection Pool [aaa]/Resize Rate The timeout period after which the system will adjust the number of database connections to be equal to the maximum number of database connections concurrently used during the last period. [PMR] Used for the standard connection pool, which is the most frequently used connection pool in the Business Rule Engine. [PML] Used for the long running connection pool, which is used in the Business Rule Engine when scheduling long running jobs. [PMT] Used for the transactional connection pool, which is used in the Business Rule Engine when a client transaction is requested.	4m	4m - 12h

[Database Settings]

Setting Name and Description	Default	Valid Ranges/Values
Database/Instance/Connection Pool [aaa]/Maintenance Frequency The run frequency of the maintenance that ensures leases have not exceeded the maximum duration. [PMR] Used for the standard connection pool, which is the most frequently used connection pool in the Business Rule Engine. [PML] Used for the long running connection pool, which is used in the Business Rule Engine when scheduling long running jobs. [PMT] Used for the transactional connection pool, which is used in the Business Rule Engine when a client transaction is requested.	1m	10s - 1h
Database/Instance/Connection Pool [aaa]/Lease Request Wait Timeout The amount of time a request for a database connection will wait. [PMR] Used for the standard connection pool, which is the most frequently used connection pool in the Business Rule Engine. [PML] Used for the long running connection pool, which is used in the Business Rule Engine when scheduling long running jobs. [PMT] Used for the transactional connection pool, which is used in the Business Rule Engine when a client transaction is requested.	30s	5s - 2h
Database/Instance/Connection Pool [aaa]/Maximum Connections The maximum number of connections the server will have to the database. [PMR] Used for the standard connection pool, which is the most frequently used connection pool in the Business Rule Engine. [PML] Used for the long running connection pool, which is used in the Business Rule Engine when scheduling long running jobs. [PMT] Used for the transactional connection pool, which is used in the Business Rule Engine when a client transaction is requested.	50	5 - 15000

[Database Settings]

Setting Name and Description	Default	Valid Ranges/Values
Database/Instance/Connection Pool [aaa]/Fetch Size A hint to the database driver for how many rows to fetch at a time. [PMR] Used for the standard connection pool, which is the most frequently used connection pool in the Business Rule Engine. [PML] Used for the long running connection pool, which is used in the Business Rule Engine when scheduling long running jobs. [PMT] Used for the transactional connection pool, which is used in the Business Rule Engine when a client transaction is requested.	120	—
Database/Instance/Connection Pool [aaa]/Trace SQL Trace all SQL sent to the database. [PMR] Used for the standard connection pool, which is the most frequently used connection pool in the Business Rule Engine. [PML] Used for the long running connection pool, which is used in the Business Rule Engine when scheduling long running jobs. [PMT] Used for the transactional connection pool, which is used in the Business Rule Engine when a client transaction is requested.	false	true/false
Database/Instance/Connection Pool [aaa]/Renewable Free Limit The minimum number of connections that should be available for leases to be renewed. [PMR] Used for the standard connection pool, which is the most frequently used connection pool in the Business Rule Engine. [PML] Used for the long running connection pool, which is used in the Business Rule Engine when scheduling long running jobs. [PMT] Used for the transactional connection pool, which is used in the Business Rule Engine when a client transaction is requested.	3	3 - 5

[Database Settings]

Setting Name and Description	Default	Valid Ranges/Values
Database/Instance/Connection Pool [aaa]/Renewable Leases If false, each connection can be leased only for the MaxLeaseDuration period. If true, connection leases are renewed if database statements are completed within the MaxLeaseDuration time period. When true, the code can hold onto the connection as long as it needs, provided SQL statements are completed within the MaxLeaseDuration period. When true, the connection is revoked if no SQL statements are issued within the MaxLeaseDuration period or if one statement takes longer to execute than that period. [PMR] Used for the standard connection pool, which is the most frequently used connection pool in the Business Rule Engine. [PML] Used for the long running connection pool, which is used in the Business Rule Engine when scheduling long running jobs. [PMT] Used for the transactional connection pool, which is used in the Business Rule Engine when a client transaction is requested.	PMR - false PML - false PMT - true	true/false
Database/Instance/Connection Pool [aaa]/Maximum Lease Duration The maximum amount of time a database connection can be leased before it is revoked. [PMR] Used for the standard connection pool, which is the most frequently used connection pool in the Business Rule Engine. [PML] Used for the long running connection pool, which is used in the Business Rule Engine when scheduling long running jobs. [PMT] Used for the transactional connection pool, which is used in the Business Rule Engine when a client transaction is requested.	PMR - 2m PML - 10m PMT - 10m	PMR - 5s - 4h PML - 5s - 6h PMT - 5s - 6h
Database/Instance/Group Server/Protocol Protocol for GroupServer	socket	http, https, socket
Database/Instance/Group Server/Server GroupServer host machine name	servername	—
Database/Instance/Group Server/Port GroupServer host listen port	9002	—

[Database Settings]

Setting Name and Description	Default	Valid Ranges/Values
Database/Instance/Group Server/URL GroupServer servlet URL.	http:// servername	—
Database/Instance/Methodology Management/Name Name of this database instance.	—	—
Database/Instance/Methodology Management/Description Description of this database instance.	—	—
Database/Instance/Methodology Management/URL Database URL used to establish a connection to the database.	—	—
Oracle example: jdbc:oracle:thin:@xx.xxx.xxx.xx:yyyy:zzzz		
SQL example: jdbc:sqlserver://xxxx:yyyy;database=zzzz;		
x = IP address or hostname y = database listen port z = database name		
Database/Instance/Methodology Management/User Name The name used to establish a connection to the database.	—	—
Database/Instance/Methodology Management/Password The password used to establish a connection to the database.	—	—
Database/Instance/Methodology Management/Public Group ID The Group ID used to establish a connection to the database.	1	—
Database/Instance/Methodology Management/Database Alias The DB Alias name used by the Project Architect job service to create a project plan from a methodology.	MMDB	—
Database/Instance/Methodology Management/Connection Pool [MMR]/Resize Rate The timeout period after which the system will adjust the number of database connections to be equal to the maximum number of database connections concurrently used during the last period.	4m	4m - 12h

[Database Settings]

Setting Name and Description	Default	Valid Ranges/Values
Database/Instance/Methodology Management/Connection Pool [MMR]/Maintenance Frequency The run frequency of the maintenance that ensures leases have not exceeded the maximum duration.	1m	10s - 1h
Database/Instance/Methodology Management/Connection Pool [MMR]/Lease Request Wait Timeout The amount of time a request for a database connection will wait.	30s	5s - 2h
Database/Instance/Methodology Management/Connection Pool [MMR]/Maximum Connections The maximum number of connections the server will have to the database.	50	5 - 15000
Database/Instance/Methodology Management/Connection Pool [MMR]/Fetch Size A hint to the database driver for how many rows to fetch at a time.	120	—
Database/Instance/Methodology Management/Connection Pool [MMR]/Trace SQL Trace all SQL sent to the database.	false	true/false
Database/Instance/Methodology Management/Connection Pool [MMR]/Renewable Free Limit The minimum number of connections that should be available for leases to be renewed.	3	3 - 5
Database/Instance/Methodology Management/Connection Pool [MMR]/Renewable Leases If false, each connection can be leased only for the MaxLeaseDuration period. If true, connection leases are renewed if database statements are completed within the MaxLeaseDuration time period. When true, the code can hold onto the connection as long as it needs, provided SQL statements are completed within the MaxLeaseDuration period. When true, the connection is revoked if no SQL statements are issued within the MaxLeaseDuration period or if one statement takes longer to execute than that period.	false	true/false
Database/Instance/Methodology Management/Connection Pool [MMR]/Maximum Lease Duration The maximum amount of time a database connection can be leased before it is revoked.	2m	5s - 4h

[Database Settings]

Setting Name and Description	Default	Valid Ranges/Values
Database/Instance/Content Repository/URL Database URL used to establish a connection to the database. Oracle example: embedded://jdbc:oracle:thin:@xx.xxx.xxx.xx:yyyy:zzzz SQL example: embedded://jdbc:sqlserver://xxxx:yyyy;database=zzzz; x = IP address or hostname y = database listen port z = database name	—	—
Database/Instance/Content Repository/Database User Name The name used to establish a connection to the database. By default, this is admuser for Oracle and sa for SQL.	—	—
Database/Instance/Content Repository/Database Password The password used to establish a connection to the database. By default, this is admuser for Oracle and sa for SQL.	—	—
Database/Instance/Content Repository/Repository Home Location where content repository files will be stored. Specify a location, or type a name and a folder will be created for you in the Bootstrap home directory.	—	—
Database/Instance/Content Repository/Admin User Name Application admin user name for the content repository.	—	—
Database/Instance/Content Repository/Admin Password Application admin password for the content repository.	—	—
Database/Instance/Content Repository/Enable Connection Pooling Provides a pool of shared database connections to the content repository. Utilizes the c3po connection pool.	true	true/false
Database/Instance/Content Repository/Maximum Connections The maximum number of connections that the repository connection pool will have to the database.	25	2-5000

[Database Settings]

Setting Name and Description	Default	Valid Ranges/Values
Database/Instance/Workflow Repository/URL Database URL used to establish a connection to the database. Oracle example: jdbc:oracle:thin:@xx.xxx.xxx.xx:yyyy:zzzz SQL example: jdbc:sqlserver://xxxx:yyyy;database=zzzz; x = IP address or hostname y = database listen port z = database name	—	—
Database/Instance/Workflow Repository/User Name The name used to establish a connection to the database. By default, this is admuser for Oracle and sa for SQL.	—	—
Database/Instance/Workflow Repository/Password The password used to establish a connection to the database. By default, this is admuser for Oracle and sa for SQL.	—	—
Database/Instance/Workflow Repository/Enable Connection Pooling Provides a pool of shared database connections to the workflow system. Utilizes the c3po connection pool.	true	true/false
Database/Instance/Workflow Repository/Maximum Connections The maximum number of connections that the workflow repository connection pool will have to the database.	25	1-5000
Database/Instance/Workflow Repository/Timeout The number of seconds a connection can remain pooled, but unused, before being discarded. If a value of zero is entered, idle connections will never expire.	1m	5s-1h
Database/Instance/Workflow Repository/Connection Test Period The time, in seconds, in which all idle connections will be tested. If a value of zero is entered, no connections will be tested.	5m	5s-1d

[Database Settings]

Setting Name and Description	Default	Valid Ranges/Values
Database/Instance/Session Settings/Setting 1-5 “Alter session” commands used to establish cursor sharing, rule-based mode, SQL trace, and more. Invalid settings in these fields are ignored.	—	alter session set _ = _
Database/Instance/Cost Based Optimization Settings/Enable Enable Cost Based Optimization if true.	false	true/false
Database/Instance/Cost Based Optimization Settings/Dump Matching SQL Set to true to dump the SQL where a match is found in the QUERYLIB table for a given SQL statement. Set to false to dump the SQL where a match is not found in the QUERYLIB table for a given SQL statement.	false	true/false

[Thread Pool Settings]

Setting Name and Description	Default	Valid Ranges/Values
Thread Pool/Number of Threads The number of server threads.	25	2-300
Thread Pool/Maximum Task Duration The maximum duration a thread can be used for one task.	3m	10s - 24d
Thread Pool/Maximum Long Running Task Duration The maximum duration a thread can be used for a long running task.	5m	10s - 24d
Thread Pool/Maintenance Frequency The frequency at which threads are checked for excess time durations.	45s	15s - 24d

[Log Settings]

Setting Name and Description	Default	Valid Ranges/Values
Log/Console Logger/Severity Level Log severity level for the Console Logger.	error	debug, info, warning, error
The ranges are inclusive. For example, choose “debug” to log all messages; choose “warning” to log both warning and error level messages.		
Log/Console Logger/Enabled Enable the Console Logger	false	true/false
Log/File Logger/Archive Size The minimum size (in Kb) a log file must be before it is archived.	1024	1024 - 2073600000
Log/File Logger/Severity Level Log severity level for the HTML Logger.	error	debug, info, warning, error
The ranges are inclusive. For example, choose “debug” to log all messages; choose “warning” to log both warning and error level messages.		
Log/File Logger/Number of Archive Files Maximum number of log files to be used. The default files are named WebAccessLog0.html through WebAccessLog5.html.	6	2 - 2073600000
Log/File Logger/HTML Log as HTML.	true	true/false

[Log Settings]

Setting Name and Description	Default	Valid Ranges/Values
Log/File Logger/Enabled Enable the HTML Logger. Log files are created in a folder named WebAccessLogs, located as follows: JBoss on Windows: <webaccesshome>\WebAccessLogs JBoss on Red Hat Enterprise Linux: /mount_point/<webaccesshome>/AppServer/ WebAccessLogs WebLogic on Windows: <webaccesshome>\WebAccessLogs WebLogic on Solaris: /mount_point/<webaccesshome>/WebAccessLogs WebSphere on Windows: <webaccesshome>\WebAccessLogs WebSphere on Red Hat Enterprise Linux: /mount_point/WebSphere/AppServer/WebAccessLogs	true	true/false
Log/Email Logger/SMTP Host SMTP server that will send the email message.	—	—
Log/Email Logger/From Email Address Set to the email address from which you would like log messages sent.	—	—
Log/Email Logger/To Email Address Set to the email address to which you would like log messages sent.	—	—
Log/Email Logger/Email subject The default Email subject.	P6 Web Access error	—
Log/Email Logger/Enabled Enable the Email logger.	false	true/false
Log/Asynchronous Log messages asynchronously for better performance.	true	true/false

[Application Settings]

Setting Name and Description	Default	Valid Ranges/Values
Application/Prototype User Prototype user login used to create and store default Dashboards and Global Preference settings for new P6 Web Access users.	—	—
Application/Ignore Daylight Savings Time Set to false to account for daylight savings time.	true	true/false
Application/Timesheet URL URL for invoking timesheet program	/action/ launchTimesheetSeemlessly	—
Application/Timesheet Codebase URL for the timesheet application Web site	server/GroupServer	—
Application/Internet Explorer Java Plugin URL URL for Internet Explorer users to download Java Plug-in (JRE).	Defaults to the plug-in version 1.6.0_07 that is installed during setup.	—
Application/FireFox Java Plugin URL URL for Firefox users to download Java Plug-in (JRE).	Defaults to the plug-in version 1.6.0_07 that is installed during setup.	—
Application/Internet Explorer Java Plugin Version JRE version used by applets in Internet Explorer	—	—
Application/FireFox Java Plugin Version JRE version used by applets in Firefox	—	—
Application/Maximum Transactions for Excel Import The maximum number of transactions (activities or resources) that can be imported at once from a .xls or .csv file	2000	100 - 2000
Application/Maximum Excel Import File Size The maximum size of the .xls or .csv file uploaded during an import attempt (KB)	1048	64 - 4096
Application/Allow Auto-Summarize Option Set to true to allow automatic summarization to be available in resource staffing user preferences.	true	true/false
Application/Database Dropdown Key Keyword to use for enabling database selection control in the login page. Pass this as a URL parameter db=keyword. Set this to an empty string if you do not want to require the keyword.	—	—

[Application Settings]

Setting Name and Description	Default	Valid Ranges/Values
Application/Logout URL Directs P6 Web Access to a specific URL when the user exits with the Logout/Close icon in the banner of P6 Web Access. Any valid URL can be used. If no URL is specified, P6 Web Access directs the user to the launch page of P6 Web Access.	—	—
Application/Compress Applet Communication Set to true to compress communication between applets and the server.	true	true/false
Application/Compress HTML Content Set to true to compress HTML-related content generated by P6 Web Access, including .html, .js, and css files, and Ajax content.	true	true/false
Application/Maximum Projects in Portfolio The maximum number of projects returned when creating a portfolio with a filter.	1000	1 - 100000
Application/Maximum Loaded Resource Planning Projects The maximum number of projects that can be open in the Resource Planning spreadsheet.	100	1 - 1000
Application/Maximum Portlets per Dashboard The maximum number of portlets that can be displayed in a dashboard on the Dashboards Home page.	12	1 - 50
Application/Maximum Projects per Portfolio View The maximum number of projects that can be displayed in a portfolio view on the Portfolio Analysis tab and in Portfolio View portlets on dashboards.	5000	1 - 20000
Application/Maximum Activities per Activity View The maximum number of activities that can be displayed in the Activities tab of the Projects section. If greater than 5000, the Maximum memory allocated to Java Applets setting (below) must be 128 or greater.	2000	1 - 15000

If a supported JRE prior to version 1.6.0_10 is being used, the maximum number of activities displayed will be 5000. Also, Primavera recommends that the maximum value be set to 5000 (or lower) if users need to display Earned Value or Baseline-related information. Otherwise, database timeouts may occur.

[Application Settings]

Setting Name and Description	Default	Valid Ranges/Values
Application/Maximum memory allocated to Java Applets The maximum amount of memory, in megabytes, that can be used by Java Applets. If the Maximum Activities per Activity View setting (above) is greater than 5000, the memory allocation must be set to 128 or greater.	64	64-1024
This setting is only valid when using JRE version 1.6.0_10 (or later).		
Application/Maximum MRU List Items The maximum number of items that can be displayed in a Most Recently Used (MRU) list.	5	1 - 10
Application/Maximum Project Activity Codes The maximum number of projects that can be selected and displayed in the Projects tab of the Activity Codes section.	350	1-350
Application/Maximum Activity Code Values The maximum number of activity code values that can be created or selected per Activity Code.	100000	1-1m
Application/Custom Portlet URL Encryption Key Encryption key for custom portlet user password. Assigning a key causes the password that is passed as part of the URL for a custom portlet to be encrypted. If you do not assign a value, the password is not encrypted. The value can be any alphanumeric character or string of characters. This encryption uses the Sun/Blowfish algorithm.	—	—
Application/Transaction Monitor Execution Interval The frequency at which the transaction monitor job runs, which ensures transactions have not been orphaned.	10m	1s - 24d20h31m23s647
Application/Enable Cross Site Scripting Filter Enable or disable the cross site scripting filter. It is not necessary to restart the server after changing the value of this setting.	false	true/false
Application/Notifications/Enable Issue Notifications Enable or disable automated notifications when Issues are added or modified.	false	true/false
Application/Notifications/Enable Invitation Notifications Enable or disable automated notifications when Invitations are added.	false	true/false

[Application Settings]

Setting Name and Description	Default	Valid Ranges/Values
Application/Notifications/Enable Initiation Notifications Enable or disable automated notifications when Invitations are pending.	false	true/false
Application/Notifications/Override Notification Email from User Set to true to always use the system's From email address. Set to false to use the email address of the user who causes notifications to be sent, if their email address is configured.	false	true/false
Application/Notifications/Notification from Email User The email address from which Notifications will be sent when either NotificationsFromEmailOverride is true or the user's email address is not configured	—	—

[Services Settings]

Setting Name and Description	Default	Valid Ranges/Values
Services/License Service/Recalculate Rate The rate at which the database is checked for changes in total license counts.	5m	10s - 10m
Services/License Service/Update Rate The rate at which a Business Rule Engine synchronizes with the database for license counts.	30s	100 - 1m
Services/License Service/Expiration Check Rate The rate at which licenses are checked to see if they should expire.	2m	500 - 15m
Services/Timestamp Service/Refresh Rate The rate at which the database is queried to determine if a table change notification is necessary.	1m	15s - 1h
Services/Registry Service/Refresh Rate The rate at which the database is updated with the status of the Business Rule Engine.	1m30s	15s - 1h
Services/Registry Service/Stale Period The duration of inactivity that indicates an inoperable Business Rule Engine.	4m	1m - 10m

[Services Settings]

Setting Name and Description	Default	Valid Ranges/Values
Services/Registry Service/Port The TCP/IP port on which requests to revive dead Business Rule Engines will be received.	9192	1024 - 65535
Services/Next Key Service/Refresh Rate The rate at which nextkey cache is refreshed.	1m	15s - 1h
Services/Next Key Service/Maximum Cached Keys Maximum nextkeys to cache per table	10	1 - 100
Services/Performance/Use Enterprise Summary Use enterprise level summary data for resources and roles. This setting specifies whether you want to use EPS level records or Project level records to draw Resource Manager histograms. If true, performance is better because only one record (EPS record) is used for the histogram. If false, a much larger number of records (Project records) is used to draw the histogram chart, so performance is slower. However, it is important to note that histogram data is more accurate when the setting is false, using Project records.	false	true/false
Services/Performance/Maximum Summary Node Count The threshold for displaying summarized data in views such as Resource Usage and Resource Analysis. If the number of child elements contained in a node exceeds this number, no data is displayed.	1000	1-50000
Services/Web Scheduler/Enabled If true, scheduling for jobs from P6 Web Access is performed using the Web Scheduler. If false, scheduling is performed using the Job Service Scheduler.	true	true/false
Services/Web Scheduler/Scheduling Interval Amount of time the Web Scheduler will wait before scheduling the next available job.	5m	1s - 24d20h31m23s647
Services/Web Scheduler/Concurrent Schedulers The number of processes (active schedulers) used for scheduling on this server. A value of 0 (zero) indicates that scheduling will not be performed on this server.	2	0-20
Services/Web Scheduler/Active Scheduler Mode If true, jobs are processed continuously until all jobs are scheduled. If false, each job is processed according to the Scheduling Interval.	true	true/false

[Services Settings]

Setting Name and Description	Default	Valid Ranges/Values
Services/Web Scheduler/ASAP Cleanup Rate Amount of time at which completed WebASAP scheduler jobs are removed from the database.	1d	1h - 24d20h31m23s647
Services/Store Period Performance/Enabled Service for storing period performance. If true, ThisPeriod values are stored in the specified financial period.	true	true/false
Services/Store Period Performance/Execution Interval Amount of time the service will wait before checking for any period performance jobs.	5m	1s - 24d20h31m23s647
Services/Store Period Performance/Concurrent Tasks The number of processes used for the PeriodPerformance service on this server. A value of 0 (zero) indicates that the service is not available on this server.	2	0 - 20
Services/Sync Actual This Period/Enabled Service for synchronizing actuals and ActualThisPeriod values. If true, recalculates actual units and costs for ThisPeriod.	true	true/false
Services/Sync Actual This Period/Execution Interval Amount of time the service will wait before checking for any SyncActualThisPeriod jobs.	5m	1s - 24d20h31m23s647
Services/Sync Actual This Period/Concurrent Tasks The number of processes used for the SyncActualThisPeriod service on this server. A value of 0 (zero) indicates that the service is not available on this server.	2	0 - 20

[Services Settings]

Setting Name and Description	Default	Valid Ranges/Values
Services/Project Hierarchy Cache/Cache Policy The cache policy to use. The cache policy determines how much data is in the cache and which data is removed to reclaim memory.	PRR	FIFO, LRU, JVMM, PRR, PRFIFO, PRLRU, PRCC
The allowable values are: FIFO (First In First Out-projects are cleared from the cache in the same order they were added to memory) LRU (Least Recently Used projects are cleared from the cache before more recently used ones) JVMM (Java Virtual Machine Managed-uses soft references to cached elements; memory used by soft references is reclaimed by the JVM as required) PRR (Projects are selected at random to be cleared from cache) PRFIFO (Periodic Refresh First In First Out-same as FIFO, except policy is enforced based on MaintenanceFrequency) PRLRU (Periodic Refresh Least Recently Used-same as LRU, except policy is enforced based on MaintenanceFrequency) PRCC (Periodic Refresh Clear Cache-ignores CacheLimit to flush the entire cache, based on MaintenanceFrequency)		
Services/Project Hierarchy Cache/Cache Limit The maximum number of projects stored in memory.	5000	1000 - 30000
Services/Project Hierarchy Cache/Maintenance Frequency The frequency for applying the specified cache policy. Application of the cache policy might result in memory used by the cache to be reclaimed.	5h	1m - 24d
Services/Collaboration Synchronization Service/Synchronization Interval The interval at which the collaboration synchronization service will run. The synchronization service deletes documents and workflows for projects that have been deleted.	1h	1m - 24d20h31m23s647
Services/Asynchronous Jobs/Purge Interval The frequency at which long running job records will be removed from the database.	1h	0 - 24d20h31m23s647
Services/Asynchronous Jobs/Grace Time The minimum age of long running job records removed during purge.	1d	0 - 24d20h31m23s647

[Services Settings]

Setting Name and Description	Default	Valid Ranges/Values
Services/Mail Service/Email Notification Server Hostname or IP address of the email notification server for Timesheet Approval.	—	—
Services/Mail Service/SMTP Port The tcp/ip port of the outgoing SMTP server.	25	1 - 65535
Services/Mail Service/Send Interval The frequency at which queued mail messages are sent.	1m	0 - 24d20h31m23s647
Services/Mail Service/Maximum Queue Length The maximum size of the mail message queue	250	0 - 2147483647
Services/Mail Service/Authorized User Name The name of the account to use to send mail from this mail server.	—	—
Services/Mail Service/Authorized User Password The password of the account used to send mail from this mail server.	—	—

[Performance Monitor Settings]

Setting Name and Description	Default	Valid Ranges/Values
Performance Monitor/Enabled Performance monitor packets are sent when true.	false	true/false
Performance Monitor/Monitor Host The destination IP or machine name for the performance monitor packets	localhost	—
Performance Monitor/Monitor Port The destination port for the performance monitor packets	6990	1024 - 65535
Performance Monitor/Update Interval The rate at which the performance monitor packets are sent.	1s	250 - 1m

[Tracer Settings]

Setting Name and Description	Default	Valid Ranges/Values
Tracer/Enabled If true, debugging messages are sent to Tracer application.	false	true/false
Tracer/Server Name Hostname or IP address of destination for sending tracer information.	localhost	—
Tracer/Port Port to use for Tracer socket connection	9210	1024-65535
Tracer/Use Background Send Thread If true, use background thread for sending TCP messages to tracer.	true	true/false

[Integration API Server Settings]

Setting Name and Description	Default	Valid Ranges/Values
Integration API server/RMI/Registry Port The port for the RMI Registry. This value is usually set to at least 1024.	9099	1024 - 65535
Integration API server/RMI/Enable The setting that enables the RMI server.	true	true/false
Integration API server/RMI/Enable Compression The setting that enables compression service mode.	true	true/false
Integration API server/RMI/Enable SSL The setting that enables SSL service mode.	true	true/false
Integration API server/RMI/Enable Standard Service The setting that enables Standard service mode.	true	true/false
Integration API server/RMI/Enable HTTP Service The setting that enables HTTP tunneling mode.	false	true/false
Integration API server/RMI/Enable HTTPS Service The setting that enables secure HTTP (SSL) tunneling mode.	false	true/false

[Integration API Server Settings]

Setting Name and Description	Default	Valid Ranges/Values
Integration API server/RMI/Compression Service Port The port to use for Compression service mode. A setting of 0 indicates that any available port will be used. If the server will be accessed across a firewall, you must set this to a specific port.	0	0 - 65535
Integration API Server/RMI/SSL Service Port The port to use for SSL service mode. A setting of 0 indicates that any available port will be used. If the server will be accessed across a firewall, you must set this to a specific port.	0	0 - 65535
Integration API Server/RMI/Standard Service Port The port to use for Standard service mode. A setting of 0 indicates that any available port will be used. If the server will be accessed across a firewall, you must set this to a specific port.	0	0 - 65535
Integration API Server/RMI/HTTP Service Port The port to use for HTTP tunneling mode. A setting of 0 indicates that any available port will be used.	0	0 - 65535
Integration API Server/RMI/HTTPS Service Port The port to use for secure HTTP tunneling mode. A setting of 0 indicates that any available port will be used.	0	0 - 65535
Integration API Server/Session Timeout The amount of time after which an idle client connection will be terminated.	120	1 - 24d

Configuring Authentication Modes

In this chapter:

Authentication Modes

Implementing Non-Native Authentication

Choosing an Authentication Scheme

Running the Authentication Configuration Wizard

Configuring Integration API Authentication

Logon/Logout Changes to Support Authentication Modes

This chapter describes the authentication modes available and explains how to configure the Primavera Integration API to operate using a non-native authentication scheme.

Authentication Modes

The Primavera Integration API provides support for the following authentication modes to validate user logons:

- **Native**
Native mode is the original Primavera authentication scheme and is the default for all applications. When a user attempts to log on to a Primavera application, native mode confirms the user's identity in the project manager or methodology manager database.
- **LDAP (Lightweight Directory Access Protocol)**
LDAP mode is available for the Primavera Project Management client module, P6 Web Access, and the API. In this mode, when a user attempts to log on to a Primavera application, the user's identity is confirmed in a directory server database.

Implementing Non-Native Authentication

By default, all Primavera applications are installed using native authentication. Native authentication is handled directly through the Primavera application with the Primavera database acting as the authority.

To implement non-native authentication for Primavera applications

- uninstall current versions of Primavera applications, if you are upgrading
- install the new version of Primavera client applications and additional components required for your implementation
- run the Authentication Configuration wizard to choose an authentication scheme for the project manager database (PMDb) and, if applicable, methodology manager database (MMDB)
- configure administrative settings for the Integration API

The Borland Database Engine and the database client software must be installed on the machine used to run the LDAP Configuration Utility.

This guide describes the procedures for choosing an authentication scheme and configuring new administrative settings for the Integration API.

For detailed procedures on installing and uninstalling Primavera client applications and server components and upgrading the methodology manager database, refer to the *Primavera P6 Administrator's Guide*.

Choosing an Authentication Scheme

To specify the authentication scheme you want to use for Primavera applications, you use the Primavera Authentication Configuration wizard. Although you specify authentication modes for client/server applications and Web applications separately, you must use a consistent authentication scheme within the Primavera suite. For example, client/server and Web applications must *both* be configured for either LDAP authentication or native authentication. For Custom mode, which is available only for client/server applications, you can choose LDAP for Web applications.

Authentication mode is database-driven, so the configuration utility enables you to first specify a database connection setting, then choose authentication modes for the applications that access that database.

For LDAP authentication, the configuration utility also enables you to specify LDAP servers, map LDAP attributes to Primavera database fields, and provision users.

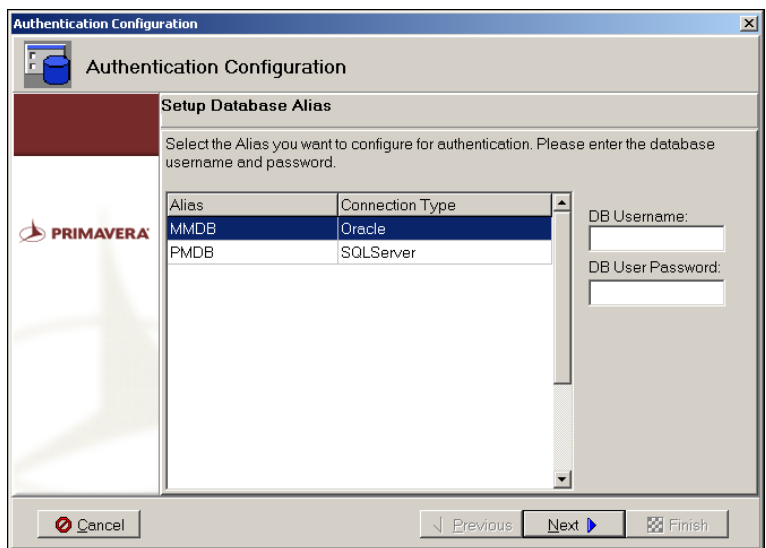
Running the Authentication Configuration Wizard

Use the Authentication Configuration wizard to

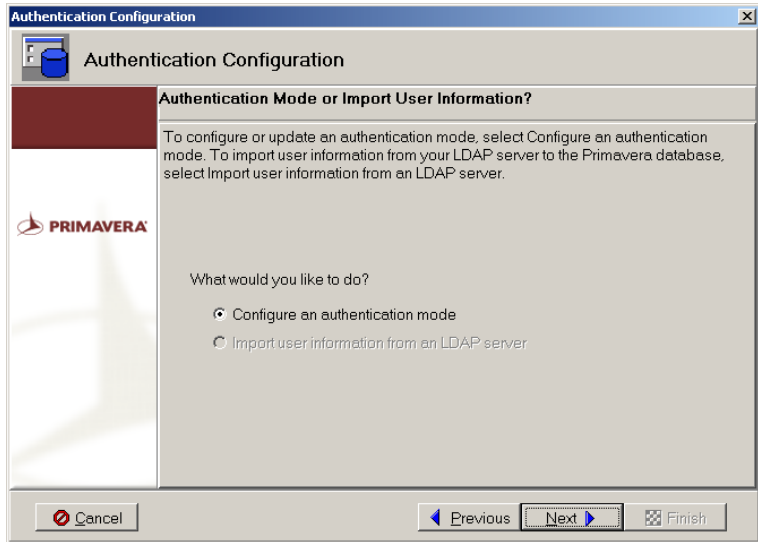
- Select an authentication mode and configure LDAP servers
- Provision LDAP user information to a Primavera database

To select an authentication mode and configure LDAP servers

- 1 From the \Client_Applications\Install\Database\ldap_config folder of the P6 physical media or download, double-click LDAPCfgWiz.exe.
- 2 Select the database alias you want to configure for authentication, then type the database username and password.



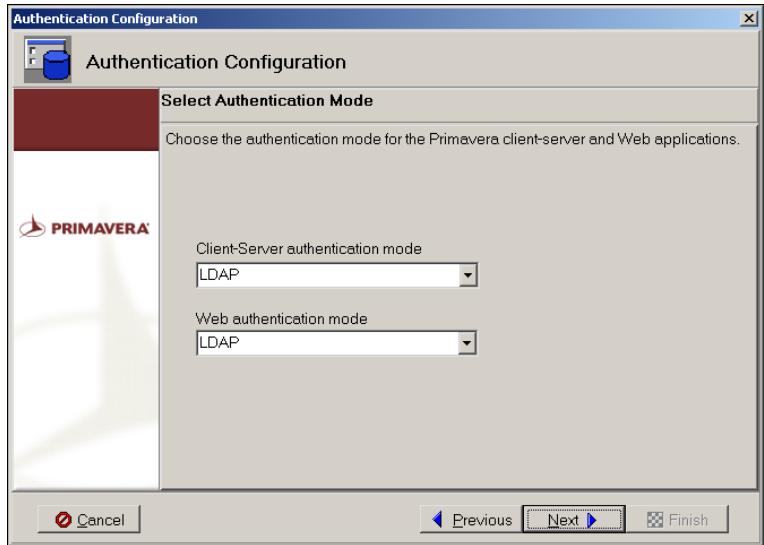
3 Choose to configure an authentication mode.



The Import option is active only if the database has previously been configured for LDAP mode.

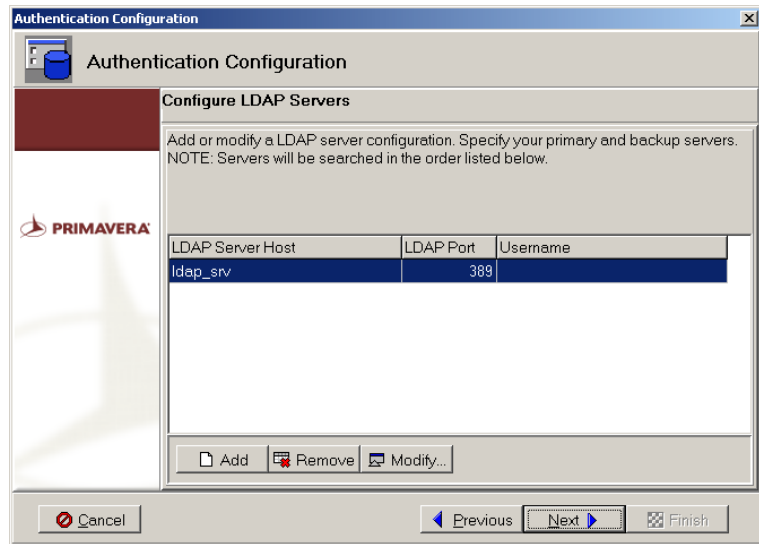
- 4 Choose an authentication mode for the client-server and Web applications.

If you choose Native, the Finish button becomes active so you can exit the wizard. For other modes, continue through the wizard to configure additional information as described in the following steps.



- 5 To add a new LDAP server, click New.

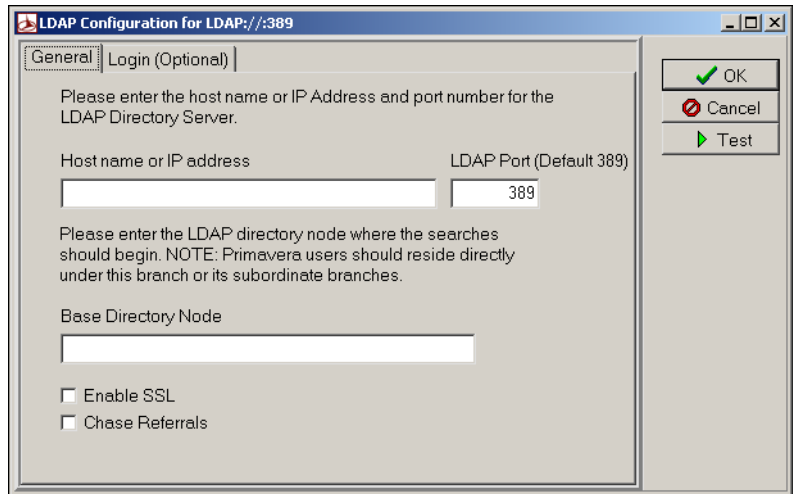
If previously configured LDAP servers are listed, you can modify the information or remove server entries.



- 6 On the General tab, specify the LDAP directory server host name or IP address, listening port, and Base Directory Node.

For Base Directory Node, specify the location in the directory information tree (DIT) that is the location from which to start the search for module users during login. Base Directory Node is also the location where the provisioning function begins the search for directory server users.

To use SSL protocol for communication with the LDAP server, mark the Enable SSL checkbox. To use referrals, mark the Chase Referrals checkbox.

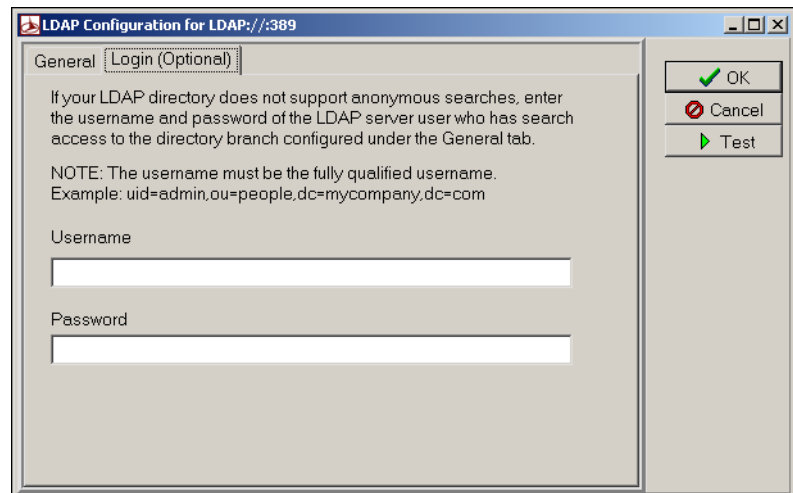


The screenshot shows the 'LDAP Configuration for LDAP://:389' dialog box with the 'General' tab selected. The 'Login (Optional)' tab is also visible. The 'General' tab contains the following fields and options:

- Host name or IP address:** A text input field.
- LDAP Port (Default 389):** A text input field with '389' entered.
- Base Directory Node:** A text input field.
- Enable SSL:** An unchecked checkbox.
- Chase Referrals:** An unchecked checkbox.

On the right side of the dialog, there are three buttons: 'OK' (with a green checkmark icon), 'Cancel' (with a red 'X' icon), and 'Test' (with a green play button icon).

If the LDAP server does not allow anonymous searches, click the Login tab. Type the user name and password of an LDAP server user who has search access for the Base Directory Node you specified on the General tab.



The screenshot shows the 'LDAP Configuration for LDAP://:389' dialog box with the 'Login (Optional)' tab selected. The 'General' tab is also visible. The 'Login (Optional)' tab contains the following fields and options:

- Username:** A text input field.
- Password:** A text input field.

On the right side of the dialog, there are three buttons: 'OK' (with a green checkmark icon), 'Cancel' (with a red 'X' icon), and 'Test' (with a green play button icon).

When you are finished configuring the LDAP server, click OK or, to validate connection with the LDAP server, click Test and click OK after a successful connection message.

USER_NAME is a required field that must be mapped and can not be deleted. Up to four fields can be mapped between the LDAP store and the project management/methodology management database.

- 7 Select an LDAP server. Then, in the LDAP attribute column, specify the term/field in the LDAP store that corresponds to the Primavera project management/methodology management database USER_NAME field.

Optionally, specify the LDAP term/field for e-mail address, actual name, and office phone number. To add fields, click Add. To remove a field, select it and click Remove.



If you are unsure of the correct LDAP terms, check with your LDAP directory server administrator.

Authentication Configuration

Create Mappings

Highlight the appropriate LDAP server.

LDAP Server
LDAP://ldap_srv:389

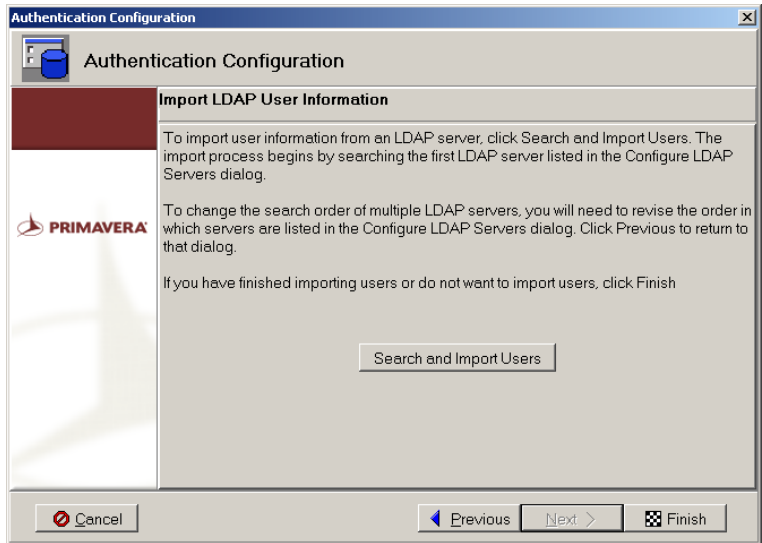
Select a database field from the drop-down list and enter the corresponding LDAP attribute. NOTE: Field mappings for primary and backup servers should be synchronized to avoid data loss.

Database Field Name	LDAP Attribute
EMAIL_ADDR	mail
ACTUAL_NAME	sn
OFFICE_PHONE	phoneNumber

- 8 To provision LDAP user information to the Primavera database, click Next. You can search the LDAP directory server or import an LDIF file to provision users.

To exit the wizard, click Finish.

- 9 Click Search and Import Users.



When you provision users from the LDAP directory, changed records are updated in the Primavera database and new users are added. However, users that have been deleted from the LDAP directory are not automatically removed from the Primavera database. You will need to manually delete these users.

10 To import from an LDIF file, click Load LDIF, then navigate to the file you want to import and click OK.

To import from an LDAP server, you can run an existing search or define a new search.

If one or more previously defined searches exist, the name of the most recently run search is displayed next to the Search Name drop-down list. To initiate the current search, click Run Search. Results display in the Available Users section. To specify a new search, click Define Criteria.

Displays the name of the current search.

Starts the search based on the filter selected in the Search Name drop-down list.

To set the number of search results listed at one time, type a number or click the arrow buttons. To advance through the list, click Go.

Click to save information for the selected users to the Primavera database.

Click to remove the current search results or currently selected users.

After running a search, select the Available users you want to add to the Primavera database, then click the right arrow button. To remove a user from the Selected users list, click the left arrow button. Click the double arrows to add or remove all listed users.

For the selected users, click to compare records between the Primavera db and LDAP store. Status is indicated by background color. White indicates a match, blue indicates that the db record differs from the record in the LDAP store, and red indicates that the user record does not exist in the database.

The screenshot shows the 'Import LDAP Users' dialog box. At the top, it displays 'Current LDAP Server: LDAP://ldap_srv:389'. Below this is the 'LDAP User Search Criteria' section, which includes a 'Define Criteria' button, a 'Run Search' button, a 'Search Name' drop-down menu, and a 'Display next' field with a spinner set to '0' and a 'Go' button. To the right of these buttons are 'Close', 'Import Users', 'View Errors', and 'Load LDIF' buttons. The main area is divided into two tables: 'Available users' and 'Selected users', both with columns for 'User Name', 'Actual Name', and 'E-Mail'. Between these tables are navigation buttons: a 'Clear' button for each table, and a set of four arrow buttons (left, double left, double right, right) to move users between the lists. A 'View Updates' button is located below the arrow buttons. The status of selected users is indicated by the background color of their rows.

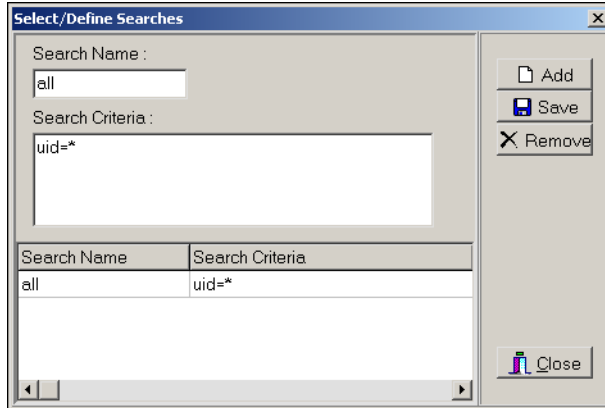
When you click Define Criteria, the Select/Define Searches dialog box displays so you can add, modify, and delete searches.

- To add a search, click Add. Type a unique name for the search. In the Search criteria field, specify the LDAP search filter you want to use. When finished specifying criteria, click Save and Close.



Search filter syntax should adhere to the rules outlined in RFC 2254.

- To modify a search name or criteria, edit the existing information, then click Save and Close.
- To delete a search, select it. Click Remove, then Close.



After provisioning users, you will need to set up Primavera user accounts for the imported users by assigning security profiles and licenses through the Primavera Project Management Module.

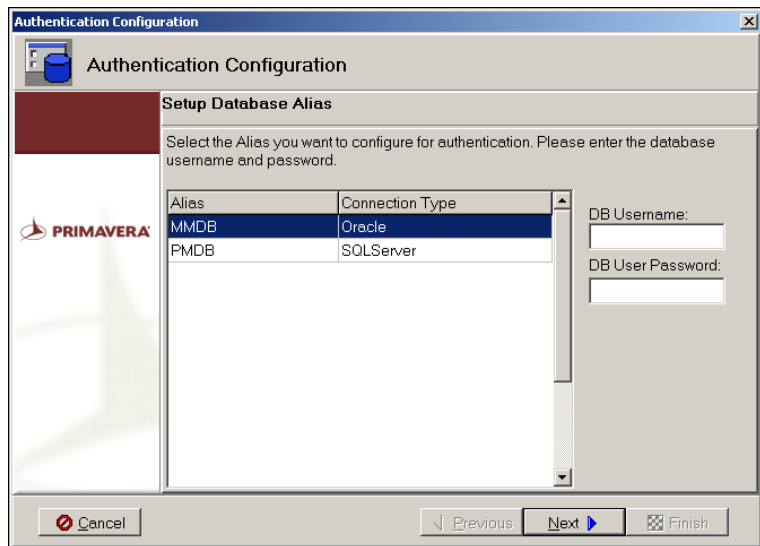
- 11 When finished importing user information, in the Import LDAP Users dialog box, click Close. To exit the Authentication Configuration wizard, click Finish.

Provisioning LDAP user information to the Primavera database



When you provision users, changed records are updated in the Primavera database and new users are added. However, users that have been deleted from the LDAP directory or LDIF file are not automatically removed from the Primavera database. You will need to manually delete these users.

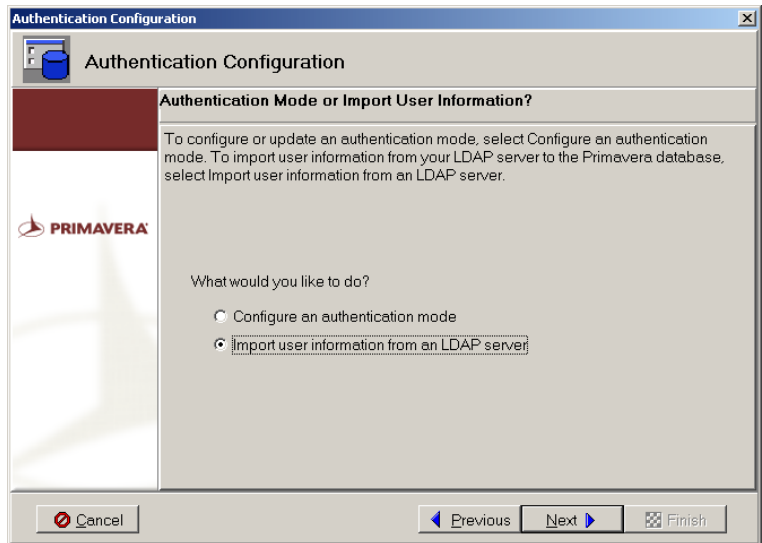
- 1 From the \Client_Applications\Install\Database\ldap_config folder of the P6 physical media or download, double-click on the file LDAPCfWiz.exe.
- 2 Select the database alias you want to provision LDAP information for, then type the database user name and password.



The image shows a screenshot of the 'Authentication Configuration' dialog box. The title bar reads 'Authentication Configuration'. The main window has a header 'Authentication Configuration' with a database icon. Below this is a section titled 'Setup Database Alias'. The instructions state: 'Select the Alias you want to configure for authentication. Please enter the database username and password.' There is a table with two columns: 'Alias' and 'Connection Type'. The table contains two rows: 'MMDB' with 'Oracle' and 'PMDB' with 'SQLServer'. To the right of the table are two text input fields: 'DB Username:' and 'DB User Password:'. At the bottom of the dialog are four buttons: 'Cancel', 'Previous', 'Next', and 'Finish'.

Alias	Connection Type
MMDB	Oracle
PMDB	SQLServer

- 3 Choose to import user information.



The Import option is active only if the database has previously been configured for either LDAP.

- 4 Follow steps 9 - 11 (beginning on [page 54](#)), which describe how to provision users.

Configuring Integration API Authentication

Because one Integration API server instance may control more than one database, in addition to specifying an authentication mode for a database through the Authentication Configuration wizard, you use an administrative configuration setting to specify the overall mode you want to use for the Integration API server. The Primavera Integration API uses a single Primavera configuration setting, `Authentication.Mode`, to support authentication selection. For LDAP authentication with secure communication (SSL) between the Integration API server and the LDAP server, two additional configuration settings are required.

Use the Primavera Administration Application to specify these configuration settings. For more information about the Administrator Application and these configuration settings, see [“Using the Primavera Administrator Application”](#) on page 15.



An Integration API configuration might include database instances that are not set to the same authentication mode as the Integration API server. If a user connects and requests a database that is set to a different authentication mode than the Integration API server, an error message displays. The user must select a database that matches the authentication mode set for the Integration API server.

Logon/Logout Changes to Support Authentication Modes

In Native mode

- Primavera modules present a login dialog that prompts for a user name and password. In Native mode, the use of passwords may be optional, depending on the password policy chosen in Administrative Preferences in the Project Management module.

In LDAP mode

- All Primavera applications require a logon password.
Additionally, because passwords are stored and authenticated against an LDAP directory, changing a user's password within a Primavera application has no effect (i.e., the password is ignored).

In Custom mode

- Client/server applications require a logon password. Custom mode is not supported by the Primavera Integration API.

Index

A

- administrator application [15](#)
 - adding Integration API configurations [18](#)
 - reviewing and modifying configurations [17](#)
- application servers supported [3](#)
- authentication
 - login/logout changes [61](#)
 - custom mode [61](#)
 - LDAP mode [61](#)
 - native mode [61](#)
- Authentication modes
 - select using LDAP Configuration utility [49](#)
- authentication modes [46](#)
 - configuring [45](#)
- authentication scheme
 - choosing [48](#)

C

- configuration settings [21](#)
- Customer support [vii](#)

D

- database
 - managing access to multiple instances [19](#)
- Database Configuration wizard
 - starting [12](#)
- database requirements [3](#)

F

- Factory Default configuration [17](#)

I

- installation [1](#)
- Integration API
 - authentication [20, 60](#)

- deploying [7](#)
 - installing [1, 4–6](#)
 - overview [2](#)

- Integration API configurations
 - add database instances [18](#)
 - adding [18](#)
 - database driver configurations [19](#)
 - deleting [19](#)
 - duplicate [18](#)

J

- Java JDK [3](#)
- Java Runtime Environment [3](#)
- Java security manager [14](#)

L

- LDAP [49](#)
 - provisioning [58](#)
- LDAP authentication
 - configure servers [49](#)
 - provision user information [54, 58](#)
 - running LDAP utility [49](#)

N

- non-native authentication [47](#)

O

- operating systems supported [3](#)

P

- Project Manager database [3](#)
- Provision LDAP user information [54, 58](#)

R

Running Authentication Configuration Wizard [49](#)

S

system requirements [3](#)

T

Technical support [vii](#)