Oracle
Primavera
Unifier Installation Guide for On-Premises

Version 21
August 2025

Contents

Introduction

The *Unifier Installation Guide* describes how to:

- Set up the Unifier servers and third party services. The requirements include:
  - Oracle WebLogic
  - Oracle Linux
  - Oracle Maps (Optional)
  - Oracle WebCenter Content (Optional)
  - Oracle HTTP Server (OHS)
  - Unifier Application / Web Server
  - AutoVue Server
  - Reports Server (Optional)
  - Windows Server

> **Note**: For the full list of system requirements, applications, and application version levels refer to the *Primavera Unifier Tested Configurations* in the Primavera Unifier Documentation Library.

- Install and configure Unifier components

This guide is intended for IT professionals who are installing and configuring the server environment for Unifier and who are supporting Unifier users.

> **Note**: The uDesigner is a module in Unifier.

In This Section

Unifier Overview

Designing, building, and managing facilities requires extensive collaboration between numerous, often geographically dispersed, disciplines and entities. Throughout the process, from conceptual design to facility operations, access to accurate, up-to-date information is critical to the success of a project and facility.

Primavera Unifier is an integrated platform that optimizes business processes and creates visibility to enable customers to better manage all of the communications and information required to successfully manage a facility throughout the lifecycle.

Unifier is a system for managing the flow of information in projects or shells, providing a seamlessly automated and integrated environment across the lifecycle of your company's facilities, from planning, design, procurement, construction and into operations and maintenance. It provides real-time visibility across multiple projects or shells to help your company make fast, accurate decisions.

Unifier lets you track and manage information such as budgets, project or shell members, specifications, requests for information, and shared documents. You decide who has access to the information, which team members are allowed to approve changes to the information, and how information flows between people.

Primavera Unifier solutions automate manual processes and pull together information from various point systems typically used on a portfolio of projects or shells. Through Unifier, executives and project or shell team members can better manage all data and business processes in one centralized system, while reducing the reliance on older technologies such as email, fax, and desktop applications.

Unifier was designed from the ground up specifically for the facility owner, based upon our industry domain expertise and knowledge of best practices combined with direct customer input gathered over decades of client interaction. The result is a robust set of capabilities with an intuitive, easy-to-use interface. Unifier enables leading owners and operators to increase enterprise efficiencies, reduce project and operating costs, enhance visibility, and improve time-to-market.

Installation Prerequisites

Create an installation account on the server that has full administration privileges. You will need to use this account for maintenance and upgrades.

The following are also prerequisites:

- Installation of the supported versions of WebLogic and JDK.
- Installation of the supported version of Oracle HTTP Server (OHS)
- If you have installed Unifier previously and you have to use the command-line version of the Configurator, make copies of the bluedoor.properties and custom.properties files currently located in <Unifier_Home>/configurator.
- If you have to use the command-line version of the Configurator and you need to encrypt or decrypt a password, update the new or existing bluedoor.properties file with the encrypted information.

Refer to the *Primavera Unifier Tested Configurations* for the supported versions.

In This Section

Installing JDK

For the full list of system requirements, applications, and application version levels, refer to the *Unifier Tested Configurations* document.

As announced in 2020, support for JavaFX on JDK 8 ended in March 2025. Starting with JDK 98 update 451, the JavaFX module, which is used by the Unifier Configurator, is no longer available as a part of the default JDK bundle distribution. Oracle continues to develop and release JavaFX as standalone modules via the OpenJFX project for the latest versions of Java only. Because the Unifier Configurator uses JavaFX, it cannot start when used with JDK 1.8 or later. This change has been addressed for environments that use JDK 11 and later to ensure that on-premises customers who use JDK 11 and later can use the Unifier Configurator.

> **Notes:** For on-premises customers that continue to use JDK 8, Oracle is providing a command-line package and instructions to work around the removal of JavaFX.

Installing WebLogic

You will need to install WebLogic to deploy Primavera Unifier.

> **Note**: For the full list of system requirements, applications, and application version levels refer to the *Primavera Unifier Tested Configurations* in the Primavera Unifier Documentation Library.

Refer to the WebLogic documentation for installation instructions (Oracle Fusion Middleware Documentation: https://docs.oracle.com/en/middleware/middleware.html).

Installing Oracle Fusion Middleware Infrastructure

1) Download Oracle Fusion Infrastructure.

> **Note**: See the *Primavera Unifier Tested Configurations* in the Primavera Unifier for supported versions.

2) Start command prompt as Administrator.
3) Run the following command to install:
   `C:\Oracle\Java\<jdk version>\bin\java -jar fmw_<WebLogic Version>_infrastructure.jar`

   If you have multiple java versions, just add the full path to Java 1.8 JDK to java command above.

> **Note:** Specify the WebLogic home as the Oracle Home for this installation.

Installing Oracle HTTP Server (OHS)

You will need to install the Oracle HTTP server (OHS) for load balancing and redirection of Unifier.

> **Note**: For the full list of system requirements, applications, and application version levels refer to the *Primavera Unifier Tested Configurations* in the Primavera Unifier Documentation Library.

Refer to the Oracle HTTP Server document for installation instructions (Oracle Fusion Middleware Documentation: https://docs.oracle.com/en/middleware/middleware.html).

1) Install Oracle HTTP Server (OHS) on desired server.
2) If OHS is installed on a different server than the Unifier server, then copy the `Unifier_Home` directory and all the files from the Unifier server to the OHS server, using the same path and directory structure on both the servers. For example: `[Unifier_Home]\apps\ROOT`

> **Note**: The `[Unifier home]\apps\ROOT` contents must be kept consistent between the Unifier app server and the OHS server. For example, if a Unifier patch set or interim patch set results in modifying

the contents of the `[Unifier home]\apps\ROOT`, re-copy the revised directory over to the OHS server.

Installing Fonts

Oracle **Outside In** requires access to **True Type** fonts in order to generate thumbnail and page images. As part of install setup, an administrator must ensure that the system has appropriate fonts installed.

The Unifier application searches for the following directory in the application server for the installed fonts, as explained below for:

Note: If none of the options below is available, you will not be able to view your documents by way of Outside In viewer.

Linux

`/usr/share/fonts/liberation`

Microsoft Windows

`C:\Windows\Fonts`

Note: To ensure that your file preview function, in the Document Manager tile view, work properly, go to My Oracle Support (MOS) and follow the instructions stated in the "File Previews Are Not Showing in the Document Manager Tile View (Doc ID 2534540.1)" article.

Installing Unifier on Windows

Complete the procedures in the order listed below to install and configure Unifier for a first time installation. Each step corresponds to a section in this guide.

> **Note**: Before you begin, create an installation account that has full administration privileges for the server. This account is needed for installation, maintenance and upgrades.

1) Download Unifier
2) Configure the database server

   Complete this step before configuring Unifier. This information will be used during database configuration in Unifier Configurator.
3) Configure WebLogic for Unifier
4) Install and configure the Reports Server. (Optional)
5) Install Oracle WebCenter Content. (Optional)
6) Install AutoVue Server
7) Configure Unifier using the Configurator
8) Deploy Unifier in WebLogic
9) Configure the Web Server
10) Launch Unifier
11) Downloading and Installing Unifier applications

In This Section

Downloading and Extracting Unifier

Download Unifier by following these steps:

1) Go to https://edelivery.oracle.com/ (Oracle Software Delivery Cloud) and sign in.
2) Navigate to access the Primavera Unifier page.
3) Download the **Primavera Unifier** ZIP file.

The **Primavera Unifier** ZIP file enables you to download the necessary files for installing only the *platform* version of the product. The platform version of Unifier contains all the Unifier modules and allows the users to create their own designs (Business Processes and Attribute forms). This version of Unifier does not have preconfigured designs.

In addition to the Primavera Unifier ZIP file, you will see the following zip folders:

- The **Primavera Unifier Tools** ZIP file enables you to download the necessary files for installing various Unifier-related products.
- The **Primavera Unifier Documentation** ZIP file enables you to download all the Unifier documents.

4) Extract the files to a **<Unifier_Home>** directory.
5) If you need to use the command-line package to configure Unifier, complete the following:
   a. If you have downloaded and installed Unifier previously, copy the existing **bluedoor.properties** file to **<Unifier_Home>/configurator**.
   b. If you have downloaded and installed Unifier previously and you use custom properties, copy the **custom.properties** file to **<Unifier_Home>/configurator**.
6) If you have access to the**Primavera Unifier Project Controls** and/or **Unifier Facilities and Asset Management** base products (applications/products), download and install them.

   For details, see ***Downloading and Installing Unifier Base Configuration***.

Recommended Setup after Downloading Unifier

Unifier (Platform) will be available in your environments. You need a minimum of two environments:

1) Development
2) Production

> **Note**: Although the BASIC files will be available, since Unifier (Platform) is already loaded, enter only the company details to use the Unifier (Platform).

Configuring the Oracle Database Server

The following is an overview of the steps required to configure the Oracle Database for use with Unifier. For more information and specific instructions, refer to your Oracle documentation.

> **Note**: For the full list of system requirements, applications, and application version levels refer to the Unifier Tested Configurations in the Unifier Documentation Library.

Configure an Oracle Database for Unifier as follows:

1) Create an instance for the database.

> **Note**: You can accept the defaults except for the following: Ensure to set encoding to Unicode (UTF-8).

2) Create a user account on the newly created database.

   For successful Primavera Unifier/uDesigner installation, make sure ample free space of at least 2GB is available for the default tablespace where the new user will be located.

3) Grant the new user with connect, resource, create view, and create table privileges.

> **Note**: This information will be used later for setting database information in the Database tab of the Unifier Configurator.

For example:

```
create user unifier identified by unifier
temporary tablespace temp
default tablespace users;
grant connect, resource, create view, create table to unifier;
```

> **Notes**:
>
> - (Required) Ensure that maximum open cursor in Oracle DB is set to 1000, or above.
> - Ensure that Database user quota is set to unlimited on tablespace users.

Implementing Transparent Data Encryption (Optional)

Transparent Data Encryption (TDE) is an Oracle Advanced Security feature that is used for Oracle Database encryption. TDE provides strong protection from malicious access to database files by encrypting data before it is written to storage, decrypting data when being read from storage, and offering built-in key management.

For more information about TDE, refer to the Oracle Advanced Security: http://www.oracle.com/technetwork/database/options/advanced-security/overview/index.html.

The following is an overview of the steps required to configure the Oracle Database for use with Unifier. For more information and specific instructions, refer to your Oracle documentation.

> **Note**: For the full list of system requirements, applications, and application version levels refer to the Unifier Tested Configurations in the Unifier Documentation Library.

Configure an Oracle Database for Unifier as follows:

1) Create an instance for the database.

> **Note**: You can accept the defaults except for the following: Ensure to set encoding to Unicode (UTF-8).

2) Create a user account on the newly created database.

For successful Primavera Unifier/uDesigner installation, make sure ample free space of at least 2GB is available for the default tablespace where the new user will be located.

3) Grant the new user with connect, resource, create view, and create table privileges.

> **Note**: This information will be used later for setting database information in the Database tab of the Unifier Configurator.

For example:

```
create user unifier identified by unifier
temporary tablespace temp
default tablespace users;
grant connect, resource, create view, create table to unifier;
```

> **Notes**:
>
> - (Required) Ensure that maximum open cursor in Oracle DB is set to 1000, or above.
> - Ensure that Database user quota is set to unlimited on tablespace users.

Implementing Transparent Data Encryption (Optional)

Transparent Data Encryption (TDE) is an Oracle Advanced Security feature that is used for Oracle Database encryption. TDE provides strong protection from malicious access to database files by encrypting data before it is written to storage, decrypting data when being read from storage, and offering built-in key management.

For more information about TDE, refer to the Oracle Advanced Security: http://www.oracle.com/technetwork/database/options/advanced-security/overview/index.html.

Explain Plan

n order to be able to use the Explain Plan option for the Data Views, you must ensure that you the following configurations (permissions) are in place:

- grant select on v_$sql to {{user}}
- grant select on v_$sql_plan to {{user}}

Installing the AutoVue Server

AutoVue installation is mandatory if you plan to use Unifier Markup feature, also referred to as redlining.

When attaching documents to a Business Process (BP) form, you can add markups (text notes or graphical elements) that display directly on the document.

> **Note**: The markups do not alter the document.

This section describes the following procedures:

- Downloading and installing AutoVue

- Configuring AutoVue
- Deploying Custom GUI AutoVue applets

> **Notes**:
>
> - You must have a license to install AutoVue.
> - The AutoVue server is high-intensive with regard to CPU, I/O, memory, and graphics. So, for optimal performance, ensure that the machine running the AutoVue server is not being used for other applications.

For more information, refer to *Oracle AutoVue Client/Server Deployment Installation and Configuration Guide* available on Oracle Documentation website.

To configure Autovue (Apply Autovue Patch, etc.) follow these instructions:

1) Login to Oracle support site https://support.oracle.com and select the **Patches & Updates**.
2) In the **Patches & Updates** section select the **Patch Name or Number**, AutoVue XX.X.X (for the patch number or name refer to the *Primavera Unifier Tested Configurations* in the Primavera Unifier Documentation Library), and perform search.
3) Click on the result set to download the patch set zip file.
4) Follow the instructions below to apply the patch set. (Refer to the Read Me document in the patchset)
   a. Make a backup of the `gluegen-rt.jar, jogl.jar`, `jsonrpc4j.jar`, `jvue.jar`, and `jvueserver.jar` files located in <AutoVue Installation Directory>\bin directory.
   b. Copy the `gluegen-rt.jar`, `jogl.jar`, `jsonrpc4j.jar`, `jvue.jar`, and `jvueserver.jar` files from the patch to <AutoVue Installation Directory>\bin directory.
   c. Restart the AutoVue server.

> **Note**: For the full list of system requirements, applications, and application version levels refer to the *Primavera Unifier Tested Configurations* in the Primavera Unifier Documentation Library.

Downloading and Installing AutoVue

Download and install Autovue. For supported versions, refer to the *Primavera Unifier Tested Configurations* in the Primavera Unifier Documentation Library. Refer to the Oracle AutoVue documentation site for installation instructions.

> **Note**: For the full list of system requirements, applications, and application version levels refer to the *Primavera Unifier Tested Configurations* in the Primavera Unifier Documentation Library.

After the download is completed:

1) Extract the zip file and go to this directory in which you have extracted the zip file.
2) Run the AutoVue installer executable.
3) Go to the directory in which you have extracted the zip file.

4) Locate the **jvueserver.properties** file and open.
5) Add the following line at the end of the `<AutoVue install dir>\bin\jvueserver.properties` file:
   `jvueserver.authentication.enable=false`

Configuring AutoVue

After installing AutoVue, configure AutoVue by entering information in the following tabs of the Unifier Configurator:

- In the **General** Tab, enter the **Server internal URL** field to access AutoVue.
- In the **Markup Server** Tab, complete all fields in this tab.

Deploying Unifier GUI Applets to AutoVue

AutoVue provides the option of customizing third-party graphical user interface (GUI). The following Unifier applet GUI files are provided to integrate with AutoVue:

- `default.gui`
- `defaultcons.gui`
- `defaultNoMarkup.gui`
- `defaultview.gui`

To deploy the Unifier applet GUI files to AutoVue:

1) Download the current version of the **Primavera Unifier Tools** file from the Oracle Software Delivery Cloud (https://edelivery.oracle.com/).
2) Unzip the **AutoVueMenus.zip** file into the location specified in the **jvueserver.users.directory** parameter in the **<AutoVue install dir>\bin\jvueserver.properties** file.
3) Follow the recommendation in the Oracle AutoVue documentation site.

> **Note**: For the full list of system requirements, applications, and application version levels refer to the *Primavera Unifier Tested Configurations* in the Primavera Unifier Documentation Library.

Configuring WebLogic for Unifier on Windows

This section describes how to configure WebLogic for Unifier. It includes:

Creating a WebLogic Domain for Unifier on Windows

Create a WebLogic domain for Unifier as follows:

1) Run the WebLogic **Configuration Wizard**.
2) In the **Welcome** window:
   a. Select **Create a new WebLogic** domain.
   b. Click **Next**.
3) In the **Select Domain Source** window, click **Next** to accept the default selections.
4) In the **Specify Domain Name and Location**:
   a. Enter a domain name for the new domain to be created.
   b. Enter the location of the new domain on the server.
   c. Click **Next**.
5) In the **Configure Administrator User Name and Password** window:
   a. Enter the User Name and Password for the Administrator that will be created. This user name will be used to login to the WebLogic console.
   b. Click **Next**.
6) In the **Configure Server Start Mode and JDK** window:
   a. In the left pane, select **Production Mode**.
   b. In the right pane, select the JDK you installed earlier.
   c. Click **Next**.
7) In the **Select Optional Configuration** window:
   a. Select the **Administration Server** option.
   b. Click **Next**.
8) (Optional) In the **Configure the Administration Server** window:
   a. Select the **SSL Enabled** option and set the SSL listen port if you are enabling Secure Sockets Layer communication.

      See http://download.oracle.com/docs/cd/E12840_01/wls/docs103/secmanage/ssl.html for more details on setting SSL for WebLogic.

      Note: Oracle recommends you always use SSL in a production environment for secure communications.

   b. Click **Next**.
9) In the **Configuration Summary** window, click **Create**.

   If given the option, you can click **Done** now. Otherwise, continue to the next step.
10) In the **Creating Domain** window, select **Start Admin Server**, and then click **Done**.
11) When prompted, enter the **Administrator User Name** and **Password** that you entered above.

Configuring the WebLogic Domain for Unifier (Mobile Device)

Accessing Unifier through mobile devices with browser capabilities

To enable basic authentication for mobile REST API on WebLogic server, you must first disable the basic authentication performed by WebLogic server, which is enforced by default. For details, refer to the WebLogic server documentation:

Understanding BASIC Authentication with Unsecured Resources (http://docs.oracle.com/middleware/1221/wls/SCPRG/thin_client.htm#SCPRG150)

1) Change to the `weblogic_home/user_projects/domains/your_domain` directory
2) Edit `config/config.xml` by adding the following tag within the`<security-configuration>` tag:

   ```
   <enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>
   ```
3) Start or restart all servers in the domain.

Installing and Configuring the Reports Server (Optional)

Consult your Oracle documentation for instructions on installing Oracle Business Intelligence Publisher.

> **Note**: For the full list of system requirements, applications, and application version levels refer to the *Primavera Unifier Tested Configurations* in the Primavera Unifier Documentation Library.

For configuration information for integrating Unifier and BI Publisher, refer to the *Unifier BI Publisher Configuration Guide*.

Starting the WebLogic Admin Server on Windows

To deploy Unifier in WebLogic, start the admin server as follows:

1) From the **Start** menu, navigate to the **Oracle WebLogic** submenu.
2) Choose **User Projects**, **domain**, **Your domain**, **Start Server**. (*user_projects,domain,<your_domain>,Start Server*)
3) If prompted for a user name and password in the WebLogic console window, enter the administrative user name and password that was specified when creating the domain.

> **Note**: If you turned on the WebLogic precompile option, the WebLogic console displays "Server started in RUNNING mode" when precompiling finishes. For detailed information about turning on precompilation, see your WebLogic Server documentation.

Stopping the WebLogic Admin Server on Windows

Stop WebLogic admin server as follows:

1) From the **Start** menu, navigate to the **Oracle WebLogic** submenu.
2) Choose **User Projects**, **domain**, **Your domain**, **Stop Server**. (*user_projects,domain,<your_domain>,Stop Server*)
3) If prompted for a user name and password in the WebLogic console window, enter the administrative user name and password that was specified when creating the domain.

Note: The WebLogic console window will close automatically when it is shutdown.

Configuring WebLogic as a Service on Windows (Optional)

To automatically start WebLogic on a reboot, complete the following steps to start WebLogic admin server as a service on Windows operating system:

1) Set **WL_HOME** as system environment variable or modify it in **<unifier_home>/weblogic/setenv.bat**.

   WL_HOME is the root directory of the WebLogic installation. For detailed instructions, refer to the topic, ***Creating a WebLogic Domain for Unifier on Windows*** (on page 18) to create the Domain Home for weblogic.

   For example: `C:\Oracle\Middleware\Oracle_Home\wlsserver\server`

2) In **setenv.bat**, set the java_home variable to specify the java home used by the Unifier domain. For detailed instructions on setting the environment variables for Unifier, refer to ***Changing Unifier Configurator Settings on Windows*** (on page 22).
3) Log in as a WebLogic Administrator.
4) Access the **<unifier_home>/weblogic** folder and run the following scripts:
   - Run **service.bat install** to install the service for the first time using "beasvc %DOMAIN_NAME%_AdminServer" as the service name.
   - Run **service.bat start** to start the weblogic server with name "beasvc %DOMAIN_NAME%_AdminServer"
   - Run **service.bat stop** to stop the weblogic server with name "beasvc %DOMAIN_NAME%_AdminServer"
   - Run **service.bat uninstall** to remove the service named "beasvc %DOMAIN_NAME%_AdminServer" from the system.

   where %DOMAIN_NAME% is the WebLogic domain name used for deploying Unifier. For example: unifier_domain

Tip: Check if the **beasvc %DOMAIN_NAME%_%SERVER_NAME%** service exists, runs, or stops from the **Control Panel, Administrative Tools, Services** menu option.

Configuring SSL Hostname Verification

Note: This is required for Adobesign, Docusign, and Bluebeam integrations.

If your app server has Hostname verification configuration, this has to be extended to support the above hosts.

This can also be done by either of the below approaches -

Login into Weblogic console -> Environment -> Servers -> Choose and click on the server name where Unifier is deployed -> SSL -> Expand Advanced (at bottom)

Choose the below values for the below attributes.

Hostname Verification: Custom Hostname Verifier

Custom Hostname Verifier: weblogic.security.utils.SSLWLSWildcardHostnameVerifier

Or set the below property in the startup script of your WebLogic App Server

e.g.

SET JAVA_OPTIONS=%JAVA_OPTIONS% -

Dweblogic.security.SSL.hostnameVerifier=weblogic.security.utils.SSLWLSWildcardHostnameVerifier

Installing Oracle WebCenter Content (Optional)

Consult Oracle documentation for instructions on installing the Oracle WebCenter. For configuration information for integrating Unifier and WebCenter content, refer to *Unifier Content Repository Configuration Guide*.

Configuring Unifier Using the Configurator UI

This section describes how to use the standard Unifier Configurator user interface (UI) to configure Unifier. If you are using JDK 8, complete the steps outlined under ***Configuring Unifier Using a Command-Line Interface (CLI)*** (on page 37).

Editing the SetEnv.bat File on Windows

Edit the **setenv.bat** file as follows:

- Set the `domain_home` variable to specify the path of the domain home folder that will be used by Unifier.
- Set the `admin url` variable to specify host name and port number used by the Unifier domain.
- Set the `java_home` variable to the JDK installed directory.
- Set the `USER_MEM_ARGS` variable specify the JVM maximum memory setting.

Changing Unifier Configurator Settings on Windows

The Unifier environment is configured through the Unifier Configurator window. To change settings in Unifier Configurator:

1) Open the **WebLogic** directory in the **Unifier Home** folder.
2) Run **configure.bat**.
3) Configure the settings for each tab.
4) Click **Save** on each tab.
5) Restart Unifier for the changes to be operative.

General Tab

Server Type is the setting that defines the mode Unifier server is running.

- Set **Server Type** to **Production** if this Unifier installation is acting as the Unifier production environment.

  In this environment, you cannot publish configuration packages.

  The uDesigner designs are read-only.
- Set **Server Type** to **Development** if this Unifier installation is acting as the development server for testing of business processes and other Unifier designs and configurations.

  You cannot convert a **Development** environment to a **Production** environment because all the designs, in uDesigner, must be published in the **Production** environment.

  Note: To have one source of published designs, and to prevent designs and data corruption, Oracle recommends that you have one **Development** environment, only.
- Set **Server Type** to **Test** if this Unifier installation is acting as the test server for testing of business processes and other Unifier designs and configurations.

  In this environment, you cannot publish configuration packages.

Temporary Directory: Enter the temporary directory for Unifier server operations. The Temporary Directory must be local to the server. If you do not want to place the Temporary Directory on a local server, then you must select a different value for the shared location.

Background Job Disabled: Select to disable background jobs.

Server Internal URL: Enter the WebLogic Server URL running the Unifier (For example: `http://host1.example.com:7001`)

> **Note**: BI Publisher and Markup servers use this URL to communicate with Unifier.

Login Session Timeout: Login Session Timeout is used to control the amount of time a user can be idle before having to log back into Unifier. The unit is seconds. For security reasons, the recommended timeout setting is between 30 minutes and 4 hours.

Overdue Tasks Check Interval: Interval, in minutes, used by the internal job server for notification tasks. The suggested interval is 15 minutes. A very small interval may degrade performance.

Test Server Label: This field displays only for Test servers. Enter a custom name for the Test server. The name cannot exceed 30 characters and cannot be labeled Development or Production. It can include all special characters except - (dash/hyphen) and _ (underscore).

UPK Help URL: Enter the URL where the User Productivity Kit (UPK) help content is to be hosted (as a generic example, http://servername/contextroot, or as a specific example is http://localhost/unifierupk).

Unifier Help URL: To deploy a local version of the Unifier online help, enter the URL where the help file is to be hosted.

Repository Tab (CMIS)

The following fields display when you select **CMIS** in the **File Repository** field.

CMIS Login Name: Enter the user name for your content repository.

CMIS Password: Password for the CMIS login name.

CMIS Repository Name: The content repository name.

CMIS Documentation Home: The documentation home.

CMIS Web Service URL: The URL for your web services home.

Notes:

- It is important to plan where these directories are located because they are where Unifier data is stored. Any subsequent upgrade installations need to point to these same location in order for Unifier to 'see' data previously entered.
- These repositories, in addition to your database, should be backed up regularly.
- When naming the folders, be sure there are no spaces in the folder names.
- These files must be on a shared drive that is accessible by other server machines that are operating in a clustering environment.

Index Directory: This folder is for index files used in Document Manager search function. This field is not visible when repository is set to CMIS.

Log File Directory: The folder where the log files are stored.

When Unifier is installed on a multibyte server and connecting to SharePoint or CMIS:

1. Add `"-Djavax.xml.parsers.DocumentBuilderFactory=com.sun.org.apache.xerces.internal.jaxp.DocumentBuilderFactoryImpl"` Java option to **setenv.sh/setenv.bat** file.
2. Restart Unifier.

The above settings enable you to view documents in CMIS.

Examples

Setting in **setenv.bat** file: `SET JAVA_OPTIONS=%JAVA_OPTIONS% -Djavax.xml.parsers.DocumentBuilderFactory=com.sun.org.apache.xerces.internal.jaxp.DocumentBuilderFactoryImpl`

Setting in **setenv.sh** file: `export JAVA_OPTIONS="$JAVA_OPTIONS -Djavax.xml.parsers.DocumentBuilderFactory=com.sun.org.apache.xerces.internal.jaxp.DocumentBuilderFactoryImpl"`

Repository Tab (Database)

The following fields display when you select **Database** in the **File Repository** field.

Host Name: Enter the host name of the computer where you installed the database.

Instance ID: The Instance ID field in the Configurator can accept the following values:

- An Oracle SID
- An Oracle service name (Oracle Database)

> **Note**: For the full list of system requirements, applications, and application version levels refer to the Unifier Tested Configurations in the Unifier Documentation Library.

When you enter a service name for an Oracle service name (Oracle Database), you must preface the name with a forward slash (/), for example, `/servicename`.

If you do not preface the name with a forward slash (/), the system presumes that you have:

- Entered an Oracle SID, if you had selected Oracle from the drop-down list.

Port: Enter the Port number to be used by Unifier to communicate with the database (For example: 1521).

User Name: Enter the database login user account name (created in Oracle) to be used by Unifier. The database login user account needs to have sufficient permissions to create tables in order for Unifier to work correctly.

User Password: Enter the database login user account password to be used by Unifier.

The user has to have the following permissions:

- Connect
- Resource
- ctxapp
- Create job
- run, on ctxsys.ctx_ddl
- run, on dbms_scheduler

Log File Directory: The folder where the log files are stored.

Repository Tab (Network File System)

This topic applies when you select **Network File System** for the File Repository field.

There are two data repositories (folders in which Unifier data is stored), which Unifier requires you to configure. There are additional repositories, such as the archive directory for project archiving, that are used with specific features, as described below. These can be located on a local but separate hard drive, or on a mapped drive on your network.

- **File Repository:** In this field, select **Network File System** from the drop-down list.

Notes:

- It is important to plan where these directories are located because they are where Unifier data is stored. Any subsequent upgrade installations need to point to these same two directories in order for Unifier to 'see' data previously entered.
- These repositories, in addition to your database, should be backed up regularly.
- When naming the folders, be sure there are no spaces in the folder names.

File Directory: Enter (or Browse to) the path where uploaded or attached files are stored. This repository is for storing documents within the Document Manager, such as drawings, plans, Word documents, etc. These files will be available for viewing or attaching to business process forms within Unifier. It also stores imported schedule files.

Notes:

- These files must be on a shared drive that is accessible by other server machines that are operating in a clustering environment.
- Ensure that the user who has started the Unifier application is a network user and has access to network file system.
- Ensure that the File directory value is same in all the machines in the cluster. Use the repository machine name or IP address to specify the shared drive location.
- Ensure that enough disk space is available on the network file system.

Index Directory: This is the pathname to the location where the Search Index files are stored.

Log File Directory: The folder where the log files are stored.

Repository Tab (WebCenter Content)

This topic applies when you select WebCenter Content for the File Repository field.

File Repository: Select WebCenter Content.

WebCenter Content Server Host: This is the IP address of the WebCenter Content server.

WebCenter Content Server Port: This is the port of the WebCenter Content server.

WebCenter Content User: This is the user who will add documents through the API. The user should exist in the WebCenter Content server.

WebCenter Content Root Folder: The root folder in WebCenter Content under which all Unifier folders will be created.

Notes:

- It is important to plan where these directories are located because they are where Unifier data is stored. Any subsequent upgrade

installations need to point to these same location in order for Unifier to 'see' data previously entered.

- These repositories, in addition to your database, should be backed up regularly.
- When naming the folders, be sure there are no spaces in the folder names.
- These files must be on a shared drive that is accessible by other server machines that are operating in a clustering environment.

Log File Directory: The folder where the log files are stored.

Test WebCenter: Enables you to validate the configuration settings that you have entered.

Database Tab (Oracle)

The information entered in this tab is based on your earlier database and user account creation.

Database Type: Select **Oracle**.

Host Name: Enter the host name of the computer where you installed the database.

Instance ID: The Instance ID field in the Configurator can accept the following values:

- An Oracle SID
- An Oracle service name (Oracle Database)

> **Note**: For the full list of system requirements, applications, and application version levels refer to the Unifier Tested Configurations in the Unifier Documentation Library.

When you enter a service name for an Oracle service name (Oracle Database), you must preface the name with a forward slash (/), for example, `/servicename`.

If you do not preface the name with a forward slash (/), the system presumes that you have entered an Oracle SID.

Port: Enter the Port number to be used by Unifier to communicate with the database (For example: 1521).

User Name: Enter the database login user account name (created in Oracle) to be used by Unifier. The database login user account needs to have sufficient permissions to create tables in order for Unifier to work correctly.

User Password: Enter the database login user account password to be used by Unifier.

Max. Connections: The setting that defines the maximum connections to the database. The maximum is 400; the recommended maximum is 80 to 100.

Min. Connections: The setting that defines the minimum connections that must be connected to the database.

Test Connection: Click **Test Connection** to verify that the Application server and the database are connected and communicating. A *Test is successful* message will appear if test is successful. Two conditions are tested:

- Ability of Unifier to connect to the database
- Level of permissions granted to the database login user account

Email Tab

Outbound (SMTP) E-mail Server: (*Required*) Enter the IP address or the URL/machine name.

E-mail Sender Prefix: Enter the email prefix that will be used in the Sender's name whenever an email is generated from a user from within Unifier, for example, `Unifier`. Late email notifications show the E-mail Sender Prefix, only.

Support Contact Information: This field contains the message text that is included in all support-related email notifications.

To enable an email address as a hyperlink, use the following format: <a `href="mailto:name@example.com">name@example.com</a>`

Outbound (SMTP) Authentication Required: Select if authentication is required by the outbound SMTP email server.

Outbound (SMTP) E-mail Account: Enter the outbound Email account.

Outbound (SMTP) E-mail Password: Enter the password that corresponds to the outbound Email account.

Outbound (SMTP) E-mail Encryption Type: (*Optional*) To support TLS protocol, select from one of the following options supported by SMTP server (**Outbound (SMTP) E-mail Server**):

- **SSL/TLS**
- **STARTTLS**

Proxy Server URL for APNs Server: URL of the proxy server used to connect to Apple Push Notification Service.

Proxy Server Port for APNs Server: Port of the proxy server used to connect to Apple Push Notification Service.

> **Note**: Unifier supports outbound email without authentication or with authentication using SSL.

System Notification E-mail Address: This field contains the email ID that the system displays as the "Sender's" email address for all emails generated by the Unifier system, for example, `admin@example.com`.

Project Email Patter: This field has the following values: Suffix and Prefix and determines the project email ID supported (`<pid>-<inboundemail>@oracle.com` or `<inboundemail>+<pid>@oracleindustry.com`).

System Error Notification E-mail Address: This field contains the email address where Unifier sends a notification if Unifier loses connection to the database while the system is running. The email addresses can be separated by semicolon.

License Notification E-mail Address: This field contains the email address where Unifier sends licensing notifications, for example, if the number of users exceeds the number of available licenses. If the number of users exceeds the number of available licenses, then the system sends notifications to the following:

- Users specified in the configurator (Unifier Configurator WebLogic).
- Users who have Notify permission in the License Manager, which was set in Access Control.

Inbound E-mail protocol: Select the protocol used by the inbound email server that can receive email. The supported protocols are POP3, IMAP, POP3S, and IMAPS.

Each Unifier environment (Development, Test, and Production) must be configured with its own inbound email account. To prevent undesired results, do not use the same inbound email for all the environments.

Inbound E-mail Server: Enter the server that can receive email, for example, if a user takes action via email on a business process. This can be the server name or IP address.

(Optional) You can specify the port number after the server name of IP address, for example, `example.com:1521`.

Inbound E-mail Account: Enter the email account to receive response email from the user.

To use the project or shell Mailbox, which allows external email messages to be sent to and stored within a central project or shell mailbox, use the following format for the inbound email account. This allows acceptance of inbound emails sent to the system-generated project/shell email addresses: `*-inboundemailname@example.com.` This configuration is needed on the email server, not within the Unifier Configurator.

Inbound E-mail Password: This field contains the password that corresponds to the inbound email account. This password is used when email is retrieved.

Test Inbound Connection: Enables you to test the Inbound E-mail Server, Inbound E-mail Account, and Inbound E-mail Password.

Test Outbound Connection: Enables you to test the outbound E-mail Server, outbound E-mail Account, and outbound E-mail Password.

About Inbound E-mail

If you are using a open-source `hMailServer` to configure Unifier for inbound emails, ensure that you turn off the "auto ban" feature. If you do not turn off the "auto ban" feature, then you will not be able to use Unifier functionalities such as Project Mailbox and Workflow action view E-mail.

The Project Mailbox functionality rely on email address used for BP Action via Email. If the Inbound email address is `unifier_oracle@unifiermail.com`, then the email address of a Project/Shell could be one of the following, depending on the property value in the `skire.project.email.pattern` in `skire.properties` file. This property can have two values: "prefix" or blank and "suffix." This property can be set either manually (in the skire.properties file) or by selecting the appropriate value from Unifier Configurator - Email Tab and saving the changes.

In case the property value is "prefix" or blank

The email address of any Unifier Project/Shell will follow the pattern `<project id>-unifier_oracle@unifiermail.com` used for Project Mail box functionality. For example, if the project id is 1001, then email address for this particular Project/Shell will be `1001-unifier_oracle@unifiermail.com`. For this to function, you have to set up an email forwarding rule on your mail server such that any emails sent to `.*-unifier_oracle@unifiermail.com` will be automatically forwarded to `unifier_oracle@unifiermail.com` Inbox.

In case the property value is "suffix"

The email address of any Unifier Project/Shell will follow the pattern `unifier_oracle+<project id>@unifiermail.com` used for Project Mail box functionality. For example, if the project id is 1001, then email address for this particular Project/Shell will be `unifier_oracle+1001@unifiermail.com`. For this to function, you have to set up an email forwarding rule on your mail server such that any emails sent to `unifier_oracle+.*@unifiermail.com` will be automatically forwarded to `unifier_oracle@unifiermail.com` Inbox.

If you are using an email address on `oracleindustry.com` domain, you must use the "suffix" pattern, and you must, explicitly, set `skire.project.email.pattern=suffix` because this property is not exposed in current Unifier configurator. The email forwarding rule (for suffix pattern) is enabled on this domain by default.

On Unifier configurator, ensure that you include the port number for the current protocol in Inbound E-mail Server field, for example, `unifiermail.com:110` or `oracleindustry.com:993`. The protocol and port mapping are as follows:

- POP3 - port 110
- IMAP - port 143
- IMAPS - port 993
- POP3S - port 995

To prevent the spam emails to go in the Project Mail box, the system accepts emails from email addresses associated with Unifier user account or the email addresses listed in Approved Email List by Company Admin, *only*.

Markup Server Tab

Use Server Internal URL: (Optional) Select this option only if server internal URL address must be used by markup server to communicate with Unifier. If not selected (default), The user's login base URL address is used by markup server to communicate with Unifier.

Markup Server Host Name: Enter the host name of the markup server.

Markup Server Port: Enter the port number of the markup server. The default port number for AutoVue is 5099.

Important information about AutoVue

When Unifier is installed on a multibyte server and connecting to AutoVue, or when you are having issues with viewing documents in AutoVue from Unifier:

1) Add `"-Djavax.xml.parsers.DocumentBuilderFactory=oracle.xml.jaxp.JXDocumentBuilderFactory"` Java option to `setenv.bat` file.
2) Restart Unifier.

The above settings enable you to view documents in AutoVue.

Example

Setting in setenv.bat file:
```
SET JAVA_OPTIONS=%JAVA_OPTIONS% -Djavax.xml.parsers.DocumentBuilderFactory=oracle.xml.jaxp.JXDocumentBuilderFactory
```

Setting in `setenv.sh` file:
```
export JAVA_OPTIONS="$JAVA_OPTIONS -Djavax.xml.parsers.DocumentBuilderFactory=oracle.xml.jaxp.JXDocumentBuilderFactory"
```

Report Tab

BIP Endpoint URL: Enter the BIP Web Services endpoint URL. For example: http://host1.example.com:9502

BIP User Name: Enter the user name created for the BI Publisher server.

BIP Password: Enter the password for the BI Publisher user.

BIP Data Source: Enter the JDBC data source name that was entered when the JDBC Data Source BI Publisher

BIP Report Folder: The folder under the default location in the BI Publisher catalog. Reports reside in this folder based on company registry.

BIP External Report Folder: The folder under the default location in the BI Publisher catalog. External Reports, synchronized in Unifier, reside in this folder.

> **Note**: The values used in the BIP User Name, BIP Password, BIP Data Source, and BIP Report folder fields are the same as those created when using the *Unifier BI Publisher Configuration Guide*.

OBIEE Analytics URL: The URL to OBIEE Analytics service. This URL should be accessible via internet.

Test Report Connection: Enables you to validate the configuration settings that you have entered.

Geo Map Tab

Map Server Url: Enter **https://elocation.oracle.com**. This is the Oracle Map server base URL where the Oracle MapVeiwer application is deployed with the context "mapviewer". This is where the server obtains the map image.

Map Tile: Enter **elocation_mercator.world_map**. This is the name of the map tile layer (the base map used for map rendering) that was pre-defined on the Oracle Map server. This is the map data source.

Map Geocoder Url: Enter **https://elocation.oracle.com**. This is the server URL where the Oracle Geocoder application is deployed with the context "geocoder." This is the location service.

Authentication Tab (Native)

Authentication Type: Native

The Unifier default authentication mechanism is used.

Login URL: Enter the URL to log in to Unifier.

Authentication Tab (OIM/OAM)

Authentication Type: OIM/OAM

The system determines whether integration of Primavera Unifier with Oracle Identity Manager (OIM) and Oracle Access Manager (OAM) is enabled.

SSO Logout: The logout URL for Oracle Access Manager (OAM) or any third-party Single Sign On (SSO) configuration. For more details, refer to Oracle Access Manager documentation.

Login URL: Enter the URL to log in to Unifier.

Authentication Tab (ORACLE IDENTITY CLOUD SERVICE)

Authentication Type: ORACLE IDENTITY CLOUD SERVICE

Login URL: Enter the URL to log in to Unifier.

SSO Header: Header value used while configuring SSO.

SSO Logout: The logout URL for Oracle Identity Cloud Service.

Authentication Tab (WebLogic)

Authentication Type: Weblogic

Form-based authentication is used to integrate with WebLogic authentication methods. After WebLogic authenticates the user, Unifier determines if the user is a valid Unifier user before granting access to the application.

Realm: Weblogic realm that is used for authentication.

Group(s) (comma separated): Weblogic group name, a comma separated list, used for mapping Weblogic groups to "unifieruser" role.

Login URL: Enter the URL to log in to Unifier.

Authentication Tab (LDAP Simple Bind)

The Lightweight Directory Access Protocol (LDAP) is a protocol for querying, and modifying, directory services. The Administrator can configure the server to use either simple-bind or double-bind authentication.

Authentication Type: LDAP Simple Bind

Login URL: Enter the URL to log in to Unifier.

Provider: To connect the LDAP server (URL), for example, `ldap://ldap.zyz.com:636`

SSL: To connect to the Secure Sockets Layer (SSL) enabled port of the LDAP server.

> **Note**: Oracle recommends you always use SSL in a production environment for secure communications.

When Unifier is configured with JDK 8 and integrated with LDAP SSL:

- Add "-Djdk.tls.client.protocols=TLSv1" Java option to **setenv.sh** file.
- Restart Unifier.

The above settings enable you to log in using LDAP SSL.

Example

Setting in **setenv.sh** file: export `JAVA_OPTIONS="$JAVA_OPTIONS -Djdk.tls.clent.protocols=TLSv1"`

Security Principal Template: To authenticate directly, based on the user name and password (Simple Bind). The template is used to construct the user's Distinguished Name (DN), for example, `cn={0},l=amer,dc=oracle,dc=com`

Admin User Bypass: To allow administrators to bypass LDAP login.

Authentication Tab (LDAP Double Bind)

The Lightweight Directory Access Protocol (LDAP) is a protocol for querying, and modifying, directory services. The Administrator can configure the server to use either simple-bind or double-bind authentication.

Authentication Type: LDAP Double Bind

Login URL: Enter the URL to log in to Unifier.

Provider: To connect the LDAP server (URL), for example, `ldap://ldap.zyz.com:636`

SSL: To connect to the Secure Sockets Layer (SSL) enabled port of the LDAP server.

When Unifier is configured with JDK 8 and integrated with LDAP SSL:

- Add "-Djdk.tls.client.protocols=TLSv1" Java option to **setenv.sh** file.
- Restart Unifier.

The above settings enable you to log in using LDAP SSL.

Example

Setting in **setenv.sh** file: export `JAVA_OPTIONS="$JAVA_OPTIONS -Djdk.tls.clent.protocols=TLSv1"`

Provider Base: (Optional) When you select the Double Bind method of authentication, you need to find the user's DN and then authenticate them. Finding the user's DN is used as the base for searching the LDAP tree. If the Provided Base is not set, the root is assumed by the system: `ldap.provider.base`

Authorized User: When using the Double Bind method of authentication, find the user's Distinguished Name (DN) and then authenticate. This is used as the "trusted" or "search" login user's DN (first bind).

Authorized User Password: When using the Double Bind method of authentication, this is the authorized user's login password.

Search Field: The default value is "cn." You need to enter the node field that you want to search.

Admin User Bypass: To allow the administrator bypass the LDAP login.

Test User Name (not Saved): Enter the LDAP user name to test the LDAP server.

Test User Password (not Saved): Enter the LDAP password to test the LDAP server.

Authentication Tab (Generic SSO)

User Authentication Type: Generic SSO

Login URL: Enter the URL to log in to Unifier.

SSO Header: Header value used while configuring SSO.

> **Note**: For OAM SSO, the value is OAM_REMOTE_USER and for Shibboleth, the value is REMOTE_USER.

SSO Logout: The logout URL for Oracle Access Manager (OAM) or any third-party Single Sign On (SSO) configuration. For more details, refer to Oracle Access Manager documentation.

> **Note**: If Unifier is configured with Shibboleth as SP and IDP, add the following option `ProxyPreserveHost On` in the `httpd-ssl.conf` file in the Shibboleth SP.

Advanced Tab

The **Advanced** tab has the following fields:

Enable Password Encryption	When the password encryption is enabled, the system saves the signature in bluedoor properties file, or a secure location.
Server Time Zone	The server time zone.
Background Job Threads	The number of threads for background jobs.
High Priority Job Threads	The number of threads for high priority jobs.
Include Custom Properties	Check this box to use custom.properties file (in /configurator directory) to set additional properties.
Support Session Failover	Check this box to keep session alive when the server goes down.
Secure Key Location	The directory path where the file containing file "`unifier.properties`" will be stored. The "`unifier.properties`" file will contain the "unifier.secure.seed" property. This setting is optional. If not set, the secure key (a random string) will be generated by the Configurator and stored in the "`skire.properties`" file. If a folder location is given as a secure key location, then the key will be stored in an additional property file in the given folder for extra security (assuming that the secure key folder is a folder with very selective access that is not readable by most IT personnel). This location must be accessible from Unifier server.
Partner Login URL	The JVM default time zone. This time zone must match the java startup parameters. For example: Duser.timezone=America/Chicago. If set, Unifier generated email sent to partner user (users that do not belong to the owner company) containing the given login URL. All user emails will have the same login URL defined in the email tab, normally. This login URL is used in Cloud environment where the owner and partner use different SSO solution.

Oracle Map Server: Proxy Server URL	The URL for the proxy server that is used to connect to Oracle Map/Geocoder server. Unifier connect to `elocation.oracle.com` to get location information from the US address. This is the proxy setting required (if necessary) for Unifier server to connect to elocation server.
Oracle map Server: Proxy Server Port	Port for the proxy server that is used to connect to Oracle Map/Geocoder server. Unifier connect to "`elocation.oracle.com`" to get location information from the US address. This is the proxy setting required (if necessary) for Unifier server to connect to "elocation" server.
Is the above integrator key setup for DocuSign production environments?	Check this box only if the integrator key has been promoted to the production account by using the go-live process. ▸ If you select this option, then Unifier will redirect the customer to login to Production DocuSign Account. ▸ If you do not select this option, then Unifier will redirect the customer to Demo DocuSign Account.

Saving the Configuration Settings

You must save your configuration data to a configuration file. In the Unifier Configuration window, click **File, Save**.

> **Note:** Restart Unifier for the changes to be operative.

Changing Configuration Settings on Windows

After initially installing and configuring Unifier, follow this procedure to make any subsequent changes to the configuration settings:

1) ***Stopping Unifier in WebLogic on Windows*** (on page 36)
2) ***Editing Configuration Data on Windows*** (on page 37)
3) ***Starting Unifier in WebLogic on Windows*** (on page 37)

Stopping Unifier in WebLogic on Windows

To stop the Unifier application in WebLogic:

1) Open the **WebLogic** directory within the **Unifier Home** folder.
2) Run the **stop.bat** file.
3) If prompted, enter the WebLogic user name and password.

Editing Configuration Data on Windows

After stopping Unifier in WebLogic, make changes to the Unifier configuration settings as follows:

1) In the **WebLogic** directory within the **Unifier Home** folder, locate the **configure.bat** file.
2) Run **configure.bat**.
3) Make necessary configuration changes and click **Save**.
4) Restart Unifier in WebLogic.

Starting Unifier in WebLogic on Windows

After a new installation, Unifier must be stopped before you can make any changes to the configuration settings. Be sure to restart it afterward.

To start the Unifier application in WebLogic:

1) Open the **WebLogic** directory within the **Unifier Home** folder.
2) Run the **startup.bat** file.
3) If prompted, enter the WebLogic user name and password.

Copying the Configuration Data File

The configuration data for the Configurator is stored automatically under the installation folder in the **/configurator/bluedoor.properties** file. If necessary, you can transfer the configuration settings from one environment to another by copying the configuration data file and editing it with the new configuration settings.

Configuring Unifier Using a Command-Line Interface (CLI)

The following guidelines are for customers who are using JDK 8, which does not include JavaFX.

- If you are setting up a new environment that does not have a **bluedoor.properties** file, you must create it first. For more information, see ***Creating the bluedoor.properties File*** (on page 38).
- If you need to use encryption, complete the steps outlined under ***Using Encryption*** (on page 51).
- If you are performing an upgrade, complete the steps outlined under ***Completing an Update or Upgrade*** (on page 56).

Creating the bluedoor.properties File

You can use the blank_bluedoor.properties file to create and complete the file for a new environment.

1) Go to: `<Unifier_Home>/configurator`
2) Copy the **blank_bluedoor.properties** file to the same location (**<Unifier_Home>/configurator**) but rename the file to **bluedoor.properties**.
3) Use the information provided in the following tables to complete the specified sections.

General

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
Server Type	server.type	production, test, dev		Yes	Select Text	No
Server Internal	server.internal.url			Yes	Text	No
Temporary Directory	file.temppath			Yes	Text	No
UPK Help URL	upk.help.url			No	Url Text	No
Background Job Disabled	job.disabled	true, false		No	Boolean Text	No
Unifier Help URL	help.url			No	Url Text	No
Login Session Timeout	login.timeout			No	Number	No
Overdue Tasks Check Interval	server.scheduler.interval			No	Number	No

Repository

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
File Repository	ucr.repositorytype	CMIS, NETWORK FILE SYSTEM, DATABASE, WEBCENTER CONTENT		Yes	Select Text	No
Log File Directory	log4j.logfile.home			Yes	Text	No
File Directory	server.file.rootpath		ucr.repositorytype=NETWORK FILE SYSTEM	Yes	Text	No
Index Directory	server.file.index.rootpath		ucr.repositorytype=NETWORK FILE SYSTEM	Yes	Text	No
CMIS Document Home	cmis.docHome		ucr.repositorytype=CMIS	Yes	Text	No
CMIS Login Name	cmis.loginName		ucr.repositorytype=CMIS	Yes	Text	No
CMIS Password	cmis.password	example: HpkUIxPWKartDf1W9q/yxw\=\=	ucr.repositorytype=CMIS	Yes	Text	Yes
CMIS Repository Name	cmis.repoName		ucr.repositorytype=CMIS	Yes	Text	No
CMIS Web Service URL	cmis.wsUrl		ucr.repositorytype=CMIS	Yes	Text	No
Host Name	dm.db.host		ucr.repositorytype=DATABASE	Yes	Text	No

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
Port	dm.db.port		ucr.repositorytype=DATABASE	Yes	Number	No
Instance ID	dm.db.sid		ucr.repositorytype=DATABASE	Yes	Text	No
User Name	dm.db.user.name		ucr.repositorytype=DATABASE	Yes	Text	No
User password	dm.db.user.password	example: IZsUrJruGSk+QbmmKpb4ww\=\=	ucr.repositorytype=DATABASE	Yes	Text	Yes
WebCenter Content User password	wcc.password		ucr.repositorytype=WEBCENTER CONTENT	Yes	Text	Yes
WebCenter Content Root Folder	wcc.rootfolder		ucr.repositorytype=WEBCENTER CONTENT	Yes	Text	No
WebCenter Content Server Host	wcc.server.host		ucr.repositorytype=WEBCENTER CONTENT	Yes	Text	No
WebCenter Content Server Port	wcc.server.port		ucr.repositorytype=WEBCENTER CONTENT	Yes	Number	No
WebCenter Content User	wcc.user		ucr.repositorytype=WEBCENTER CONTENT	Yes	Text	No

Database

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
Host Name	database.databaseHost			Yes	Text	No
Instance ID	database.databaseSID			Yes	Text	No
Password	database.password			Yes	Text	Yes
Database Type	database.type	oracle		Yes	Select Text	No
Username	database.username			Yes	Text	No
Max. Connections	database.maxConnections			No	Number	No
Min. Connections	database.minConnections			No	Number	No

Email

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
System Notification E-mail Address	email.from.address			Yes	Email Text	No
Outbound(SMTP) E-mail Server	email.server			Yes	Text	No
E-mail Sender Prefix	email.from.name			Yes	Text	No
Support Contact Information	email.contact.string			No	Text	No

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
Outbound(SMTP) Authentication Required	email.authentication.required	true, false		Yes	Boolean Text	No
Outbound(SMTP) E-mail Account	email.account		email.authentication.required=true	Yes	Text	No
Outbound(SMTP) E-mail Password	email.password=Ht9JolEet+CRAox706qmJw\=\=		email.authentication.required=true	Yes	Text	Yes
Outbound(SMTP) E-mail Encryption Type	email.server.encryption.type	STARTTLS,SSL/TLS	email.authentication.required=true	No	Select Text	No
System Error Notification E-mail Address	license.notify.to			No	Email Text	No
License Notification E-mail Address	email.notify.to			No	Email Text	No
APNs Proxy Server URL	apns.proxy.server			No	Text	No
APNs Proxy Server Port	apns.proxy.port			No	Number	No
Inbound E-mail protocol	action.email.protocol=IMAPS	IMAPS, POP3		No	Text	No

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
Inbound E-mail Server	action.email.server			No	Text	No
Inbound E-mail Account	action.email.account			No	Text	No
	action.email.account.old			No	Text	No
Inbound E-mail Password	action.email.password			No	Text	Yes
Project Email Pattern	project.email.pattern	suffix, prefix		No	Select Text	No
	project.email.pattern.old			No	Select Text	No

Markup Server

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
Use Server Internal URL	server.internal.url.enabled	true, false		No	Boolean Text	No
Markup Server Host Name	server.jvue.host			No	Text	No
Markup Server Port	server.jvue.port			No	Number	No

Report

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
BIP Endpoint URL	server.report.bip.endpoint			No	Text	No
BIP Password	server.report.bip.password			No	Text	Yes
BIP Username	server.report.bip.username			No	Text	No
OBIEE Analytics URL	server.obi.analytics.url			No	Text	No
BIP Report Folder	server.report.bip.folder			No	Text	No
BIP External Report Folder	server.report.bip.extfolder			No	Text	No
BIP Data Source	server.report.bip.datasource			No	Text	No

Geo Map

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
Map Server Url	map.url			No	Select Text	No
Map Tile	map.tile			No	Select Text	No
Map Geocoder Url	map.geocoder.url			No	Select Text	No

Authentication

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
Login URL	email.login.url			Yes	Text	No
Authorization type	authorization.type	NATIVE, OIM/OAM, Oracle Identity Cloud Service, WEBLOGIC, LDAP SIMPLE BIND, LDAP DOUBLE BIND		Yes	Select Text	No
Logoff redirect url	sso.logout		authorization.type=GENERIC SSO	No	Text	No
SSO Header	sso.header		authorization.type=GENERIC SSO	No	Text	No
SSO Provider	sso.provider	sso, oam, idcs, weblogic	authorization.type=GENERIC SSO	No	Text	No
Group(s) (comma separated)	weblogic.groups		authorization.type=WEBLOGIC	Yes	Text	No
Realm	weblogic.realm		authorization.type=WEBLOGIC	Yes	Text	No
Auth Factory	authorization.factory	ldap	authorization.type=LDAP SIMPLE BIND	Yes	Text	No

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
LDAP server (URL)	ldap.provider.url	Example: ldap://ldap.xyz.com:636	authorization.type=LDAP SIMPLE BIND	Yes	Text	No
LDAP template for single bind	ldap.security.principal.template		authorization.type=LDAP SIMPLE BIND	Yes	Text	No
SSL	ldap.security.protocol	true, false	authorization.type=LDAP SIMPLE BIND	No	Text	No
Administrator's login ids	ldap.user.bypass		authorization.type=LDAP SIMPLE BIND	No	Text	No
Trusted login user's DN	ldap.authorized.user		authorization.type=LDAP SIMPLE BIND	Yes	Text	No
Authorized user's LDAP login password	ldap.authorized.user.password		authorization.type=LDAP SIMPLE BIND	No	Text	Yes
Provider base	ldap.provider.base		authorization.type=LDAP SIMPLE BIND	No	Text	No

Advanced

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
Server timezone	server.timezone	See below*		No	Number	No
Number of threads for high priority jobs	job.p1.threadCount	>5		No	Number	No
Support Session Failover	support.session.failover	true, false		No	Boolean Text	No
Proxy Server Port for Oracle Map Server	map.net.proxy.port			No	Number	No
Proxy Server User for Oracle Map Server	map.net.proxy.url			No	Text	No
Proxy Server URL for Oracle Map Server	email.login.url.partner			No	Text	No
Include Custom properties	include.custom	true, false		No	Boolean Text	No

Apryse

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
Webviewer License Key	apryse.webApryseInfo			No	Text	No

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
Webviewer Server URL	apryse.webviewerServerURL			No	Text	No

***** Values for server.timezone: If not specified, will use Unifier server time zone.

Possible Time Zones

Africa/Djibouti

Africa/Harare

Africa/Lagos

Africa/Maputo

Africa/Mogadishu

Africa/Nairobi

Africa/Nouakchott

America/Buenos_Aires

America/Costa_Rica

America/Denver

America/Edmonton

America/El_Salvador

America/Guayaquil

America/Halifax

America/Indiana/Indianapolis

America/Indianapolis

America/Lima

America/Manaus

America/Mazatlan

America/Mexico_City

America/Montreal

America/New_York

America/Panama

America/Phoenix

America/Puerto_Rico

America/Regina

America/Tijuana
America/Toronto
America/Vancouver
Asia/Aden
Asia/Bahrain
Asia/Dhaka
Asia/Ho_Chi_Minh
Asia/Kamchatka
Asia/Katmandu
Asia/Kolkata
Asia/Kuala_Lumpur
Asia/Kuwait
Asia/Muscat
Asia/Qatar
Asia/Riyadh
Asia/Saigon
Asia/Shanghai
Asia/Singapore
Asia/Taipei
Asia/Tashkent
Atlantic/Azores
Atlantic/Bermuda
Atlantic/Reykjavik
Australia/Hobart
Australia/Lord_Howe
Australia/Sydney
Etc/GMT+0
Etc/GMT+1
Etc/GMT+2
Etc/GMT+3
Etc/GMT+4
Etc/GMT+5
Etc/GMT-10

Etc/GMT-3
Etc/GMT-4
Etc/GMT-5
Etc/GMT-6
Etc/GMT-7
Etc/GMT-8
Etc/UTC
Etc/Zulu
Europe/Amsterdam
Europe/Athens
Europe/Belgrade
Europe/Berlin
Europe/Brussels
Europe/Bucharest
Europe/Budapest
Europe/Copenhagen
Europe/Dublin
Europe/Helsinki
Europe/Istanbul
Europe/Kiev
Europe/Lisbon
Europe/London
Europe/Luxembourg
Europe/Madrid
Europe/Oslo
Europe/Paris
Europe/Prague
Europe/Rome
Europe/Sofia
Europe/Stockholm
Europe/Tirane
Europe/Vienna
Europe/Warsaw

Europe/Zurich

Indian/Chagos

Indian/Cocos

Pacific/Auckland

Pacific/Easter

Pacific/Gambier

Pacific/Honolulu

Pacific/Kwajalein

Pacific/Noumea

Pacific/Pago_Pago

Pacific/Pitcairn

UCT

US/Aleutian

US/Hawaii

UTC

Using Encryption

If you need to encrypt or decrypt a password and you are using JDK 8, you must use a CLI.

Location of encryption tool:

- On Windows: <drive>:\Oracle\<Unifier_Home>\bin\encrypt_password.bat
- On Linux: <Unifier_Home>/bin/encrypt_password.sh

Prerequisite: Make sure that environment variable UNIFIER_HOME is properly defined. For example:

- On Windows: SET UNIFIER_HOME= /scratch/gbuora/Unifier_21.12.7
- On Linux: export UNIFIER_HOME= /scratch/gbuora/Unifier_21.12.7

Encryption applies to the following fields in the **bluedoor.properties** file. If you use the listed features, you must encrypt the corresponding fields.

Field	Description
cmis.password	Content Management Interoperability Services (CMIS) password
database.password	Database schema password
dm.db.user.password	Database manager database user's password
email.password	Outbound (SMTP) email password

Field	Description
ldap.authorized.user.password	Authorized user's Lightweight Directory Access Protocol (LDAP) login password
server.report.bip.password	Oracle Analytics Server Web Services password
wcc.password	WebCenter Content user's password

The following sub topics provide the applicable instructions.

Creating an encryption.properties File

To create an encryption.properties file:

1) If you have an existing file and do not want it overwritten, back it up.
2) Enter: `<Unifier_Home>/bin`
3) Enter: `./encrypt_password.sh createfile`

   The system displays information similar to the following:

```
user@host ~/Unifier_21.12.7/bin$ ./encrypt_password.sh createfile
Encryption properties are saved successfully to
<Unifer_Home>/bin/encrytion.properties
```

   The generated encryption.properties file looks similar to the following:

```
#Encryption Properties
#Tue Jul 08 21:35:39 UTC 2025
unifier.secure.seed=78120818-3d45-4dfb-b43b-61a7b6d99b3c
unifier.secure.signature=qlozt8hw2faOKm+M2+sVTXvCdeeOPoKq/Qged05LG+8
\=
```

   You will use this file to encrypt and decrypt a password.

Encrypting a Password

To encrypt a password:

1) Enter: `cd <Unifier_Home>/bin`
2) Enter: `./encrypt_password.sh encrypt <unencrypted_password>`

   For example: `./encrypt_password.sh encrypt sample_1234_1`

The system displays information similar to the following:

```
user@host ~/Unifier_21.12.7/bin$ ./encrypt_password.sh encrypt
sample_1234_1
input unencrypted password = sample_1234_1
2025-07-08T21:38:20.674Z main INFO Starting configuration
org.apache.logging.log4j.core.config.properties.PropertiesConfigurat
ion@3336e6b6...
2025-07-08T21:38:20.678Z main INFO Start watching for changes to
/scratch/gbuora/Source/Unifier_21.12.7/apps/ROOT/WEB-INF/classes/log
4j2.properties every 0 seconds
2025-07-08T21:38:20.678Z main INFO Configuration
org.apache.logging.log4j.core.config.properties.PropertiesConfigurat
ion@3336e6b6 started.
2025-07-08T21:38:20.682Z main INFO Stopping configuration
org.apache.logging.log4j.core.config.DefaultConfiguration@477b4cdf..
.
2025-07-08T21:38:20.683Z main INFO Configuration
org.apache.logging.log4j.core.config.DefaultConfiguration@477b4cdf
stopped.
output encrypted password = dE+rrTaURO3xvKqZCVTGNg==
```

Decrypting a Password

To decrypt a password:

1) Enter: `cd <Unifier_Home>/bin`
2) Enter: `./encrypt_password.sh decrypt <encrypted_password>`

   For example: `./encrypt_password.sh decrypt dE+rrTaURO3xvKqZCVTGNg==`

   The system displays information similar to the following:

```
user@host ~/Unifier_21.12.7/bin$ ./encrypt_password.sh  decrypt
dE+rrTaURO3xvKqZCVTGNg==
input encrypted password = dE+rrTaURO3xvKqZCVTGNg==
2025-07-08T21:39:20.698Z main INFO Starting configuration
org.apache.logging.log4j.core.config.properties.PropertiesConfigurat
ion@3336e6b6...
2025-07-08T21:39:20.703Z main INFO Start watching for changes to
/scratch/gbuora/Source/Unifier_21.12.7/apps/ROOT/WEB-INF/classes/log
4j2.properties every 0 seconds
2025-07-08T21:39:20.703Z main INFO Configuration
org.apache.logging.log4j.core.config.properties.PropertiesConfigurat
ion@3336e6b6 started.
2025-07-08T21:39:20.706Z main INFO Stopping configuration
org.apache.logging.log4j.core.config.DefaultConfiguration@477b4cdf..
.
```

```
2025-07-08T21:39:20.707Z main INFO Configuration
org.apache.logging.log4j.core.config.DefaultConfiguration@477b4cdf
stopped.
output decrypted password = sample_1234_1
```

Updating an Existing Environment While Retaining the Original Encryption Seed and Signature

To retain your original encryption information:

1) Back up your **bluedoor.properties**, **skire.properties**, and **datasource.properties** files to a separate location.

   These files are located in:

   - **<Unifier_Home>/configurator/bluedoor.properties**
   - **<Unifier_Home>/apps/ROOT/WEB-INF/classes/skire.properties**
   - **<Unifier_Home>/apps/ROOT/WEB-INF/classes/datasource.properties**

2) To create an **encryption.properties** file, complete the steps outlined under ***Creating an encryption.properties File*** (on page 52).
3) In **<Unifier_Home>/configurator**, open the **bluedoor.properties** file and locate the lines related to:
   - **unifier.secure.seed=sampleX**
   - **unifier.secure.signature=sampleY**
4) Open the **encryption.properties** file, and replace the values for **unifier.secure.seed** and **unifier.secure.signature** with the values from **bluedoor.properties** file (**sampleX** and **sampleY**).
5) Encrypt the password, as described under ***Encrypting a Password*** (on page 52).
6) To verify that the encryption works correctly, decrypt the password, as described under ***Decrypting a Password*** (on page 53).
7) Copy the encrypted password to the applicable field in the **bluedoor.properties** file.
8) Enter: `cd <Unifier_Home>/weblogic`
9) To transform **<Unifier_Home>/configurator/bluedoor.properties** into **<Unifier_Home>/apps/ROOT/WEB-INF/classes/skire.properties** and **datasource.properties**, enter: `./ configure.sh unifier.weblogic`
10) If you are using Enterprise Archive (EAR) deployment, to generate the EAR file, run: `./configure.sh ear.weblogic`
11) Restart your WebLogic Server, and verify that you can connect to the Unifier database.

Updating an Existing Environment Using a New Encryption Seed and Signature

To use new encryption information:

1) Back up your **bluedoor.properties**, **skire.properties**, and **datasource.properties** files to a separate location.

   These files are located in:

   - **<Unifier_Home>/configurator/bluedoor.properties**

- **<Unifier_Home>/apps/ROOT/WEB-INF/classes/skire.properties**
- **<Unifier_Home>/apps/ROOT/WEB-INF/classes/datasource.properties**

2) To create an **encryption.properties** file, complete the steps outlined under ***Creating an encryption.properties File*** (on page 52).
3) In **<Unifier_Home>/configurator**, open the **bluedoor.properties** file and locate the lines related to:
   - **unifier.secure.seed=sampleX**
   - **unifier.secure.signature=sampleY**
4) Open the **bluedoor.properties** file, and replace the values for **unifier.secure.seed** and **unifier.secure.signature** with the values from **encryption.properties** file (**sampleX** and **sampleY**).
5) Encrypt the password, as described under ***Encrypting a Password*** (on page 52).
6) To verify that the encryption works correctly, decrypt the password, as described under ***Decrypting a Password*** (on page 53).
7) Copy the encrypted password to the applicable field in the **bluedoor.properties** file.
8) Repeat these steps for all secured fields that you use.

   For more information, see the table under ***Using Encryption*** (on page 51).
9) Enter: `cd <Unifier_Home>/weblogic`
10) To transform **<Unifier_Home>/configurator/bluedoor.properties** into **<Unifier_Home>/apps/ROOT/WEB-INF/classes/skire.properties** and **datasource.properties**, enter: `./ configure.sh unifier.weblogic`
11) If you are using Enterprise Archive (EAR) deployment, to generate the EAR file, run: `./configure.sh ear.weblogic`
12) Restart your WebLogic Server, and verify that you can connect to the Unifier database.

Updating a New Environment and Using Encryption

To use new encryption information with a new environment:

1) Enter: `cd <Unifier_Home>/configurator`
2) To create the required **bluedoor.properties** file, complete the steps outlined under ***Creating the bluedoor.properties File*** (on page 38).
3) To create an **encryption.properties** file, complete the steps outlined under ***Creating an encryption.properties File*** (on page 52).
4) In **<Unifier_Home>/configurator**, open the **bluedoor.properties** file and locate the lines related to:
   - **unifier.secure.seed=sampleX**
   - **unifier.secure.signature=sampleY**
5) Open the **bluedoor.properties** file, and replace the values for **unifier.secure.seed** and **unifier.secure.signature** with the values from **encryption.properties** file (**sampleX** and **sampleY**).
6) Encrypt the password, as described under ***Encrypting a Password*** (on page 52).
7) To verify that the encryption works correctly, decrypt the password, as described under ***Decrypting a Password*** (on page 53).

8) Copy the encrypted password to the applicable field in the **bluedoor.properties** file.
9) Repeat these steps for all secured fields that you use.

   For more information, see the table under ***Using Encryption*** (on page 51).
10) Enter: `cd <Unifier_Home>/weblogic`
11) To transform **<Unifier_Home>/configurator/bluedoor.properties** into **<Unifier_Home>/apps/ROOT/WEB-INF/classes/skire.properties** and **datasource.properties**, enter: `./ configure.sh unifier.weblogic`
12) If you are using Enterprise Archive (EAR) deployment, to generate the EAR file, run: `./configure.sh ear.weblogic`
13) Restart your WebLogic Server, and verify that you can connect to the Unifier database.

Completing an Update or Upgrade

Complete the following steps to finish an upgrade, whether you are setting up a new environment or updating an existing one.

1) If you have not already done so, ensure that the **bluedoor.properties** file has been copied to **<Unifier_Home>/configurator**.

   Whether you are setting up a new environment or updating an existing one, the completed file must reside in the correct location.
2) If you have modified any of the configuration properties, run: `./configure.sh unifier.weblogic`

   This command deploys Unifier. It transforms **bluedoor.properties** into **<Unifier_Home>/apps/ROOT/WEB-INF/classes/datasource.properties** and **skire.properties**. If the custom.properties file was included in **<Unifier_Home>/configurator**, it is copied to **<Unifier_Home>/apps/ROOT/WEB-INF/classes**.
3) If you are using Enterprise Archive (EAR) deployment, to generate the EAR file, run: `./configure.sh ear.weblogic`
4) To install OutsideIn, run: `./configure.sh install-oui`

Configuring the OHTTP Server (OHS)

After installing OHTTP Server (Oracle HTTP Server), or OHS, configure as follows:

1) Modify the **$ORACLE_INSTANCE/ config/ OHS/ ohs1/httpd.conf** file as follows:
   a. Change the default listen port from 7777 to 80.

      Note: Before making the above change, disable or turn-off any other application that is using port 80 (such as IIS or Windows).

   b. Add settings after DocumentRoot as follows:

      ```
      DocumentRoot <Unifier_Home>/apps/ROOT
      ```

   c. Add parameters between <Directory ></Directory> so it appears as follows:

      ```
      <Directory "<Unifier_Home>/apps/ROOT">
      ```

```
        Options Includes FollowSymLinks
        AllowOverride None
        Require all granted
        DirectoryIndex index.html
    </Directory>
    <Directory "<Unifier_Home>/apps/ROOT/WEB-INF">
        Require all denied
    </Directory>
```

d.
```
#Support Http method  GET/POST only
RewriteEngine On
RewriteCond %{REQUEST_METHOD} !^(GET|POST)
RewriteRule .* - [F]
```

e.
```
Header set Content-Security-Policy "default-src 'self'; frame-src *;
child-src *; script-src 'self' 'unsafe-inline' 'unsafe-eval'
http://elocation.oracle.com https://elocation.oracle.com
*.oracle.com; style-src 'self' 'unsafe-inline';img-src 'self' data:
http://elocation.oracle.com https://elocation.oracle.com
*.oracle.com"

<Location /bp/sys/dm/jvue/viewer>
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/dm/project_documents>
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/sys/dm/bp/attachment/viewer>
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/dm/unpublished_documents/log>
```

```
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/studio/share/open_attachments>
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/share/editGCWithoutWorkFlow>
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/share/draftGC/new>
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/share/draftGC/edit>
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/share/commentGC/new>
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/share/commentGC/edit>
```

```
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/share/editGC>
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/share/commentGC/copyFrom>
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/share/draftGC/copyFrom>
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/studio/bp/document/copylineitem>
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/studio/bp/document/itemopen>
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>
```

Notes:

- <Unifier_Home> is the unifier installation directory.
- The session about Supporting Http method GET/POST only can be (or may be) added at the end of http.conf file.

2) Add the following to the **$ORACLE_INSTANCE/ config/ OHS/ ohs1/mod_wl_ohs.conf** file:

```
<LocationMatch
/(bp|bluedoor|g|pub|m|portal|unifier|viewbp|ws|VueServlet|VueJNLPSer
vlet|jvueDMS|xdespellchecker)($|/)>
      SetHandler weblogic-handler
      WebLogicHost localhost
      WebLogicPort 7001
</LocationMatch>
<LocationMatch /(dojo|gs|studio|unifier_js|webant|x)($|/)>
     ExpiresActive on
     ExpiresDefault "access plus 6 month"
   Header set X-Content-Type-Options "nosniff"
   Header set X-XSS-Protection "1; mode=block"
</LocationMatch>
LoadModule deflate_module "${ORACLE_HOME}/ohs/modules/mod_deflate.so"
<LocationMatch /(bp|bluedoor|g|pub|portal|unifier|viewbp)($|/)>
       SetOutputFilter DEFLATE
</LocationMatch>
DeflateBufferSize 20000
```

Note: Modify the enteries (#2) under <Location /> as necessary:

- WebLogicHost: Weblogic server hostname or IP address.
- For WebLogicPort: Weblogic server port number.
- The "deflate_module" must be loaded before "<LocationMatch /(bp|bluedoor|g|pub|portal|unifier|viewbp)($|/)>".
- If the browser displays the error message, "...js MIME type ('text/plain') is not executable, and strict MIME type checking is enabled," then add "text/javascript js" to this file: <OHS Installation path>/instances/instance1/config/OHS/ohs1/mime.types

3. Modify the **$ORACLE_INSTANCE/ config/ OHS/ ohs1/ssl.conf** file as follows:

For **OHTTP**, or **OHS**, version:

Note: For the full list of system requirements, applications, and application version levels refer to the *Primavera Unifier Tested Configurations* in the Primavera Unifier Documentation Library.

Replace: `SSLProtocol nzos_Version_1_0 nzos_Version_3_0`

With: `SSLProtocol -all +TLSv1.2`

Replace: `SSLCipherSuite`

`SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SH`

A,SSL_RSA_WITH_DES_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_C BC_SHA

With: `SSLCipherSuite HIGH`

> **Note**: Oracle recommends the SSLv3 protocol for OHS 11g version and the TLSv1.2 for OHS 12c version.

4. On Windows: Run `startNodeManager.cmd` and `startComponent.cmd ohs1`

   On Linux: Run `./startNodeManager.sh` and `./startCOmponent.sh ohs1`

> **Note**: If OAM is used to setup Unifier then login into OAMconsole, navigate to resources tab and add 3 resources in it: /jVue/**, /VueServlet/** and /jvueDMS/**. The Protection level should be excluded for the newly created resources. If any other SSO server is used then perform the similar steps in this server.

Installing SSL Certificate (Optional)

Unifier works in Secure or Non-secure mode. Installing a Secure Socket Layer (SSL) certificate is optional.

Data Backup Recommendations

Oracle Primavera recommends that Primavera Unifier data be incorporated into your company backup procedures. Primavera Unifier data is stored in two places:

- Unifier database
- Files Repository

These repositories need to be backed up regularly.

Deploying Unifier

To deploy Unifier into the WebLogic domain, complete the following procedures:

1) ***Creating an EAR File From the Configurator*** (on page 62)
2) Deploy the generated EAR file using any of the following methods:
   - ***Deploying Unifier From the Unifier_Home Directory on Windows*** (on page 62)
   - ***Deploying Unifier from the WebLogic Administration Console*** (on page 62)

Creating an EAR File From the Configurator

Complete the following steps to create an .EAR file from the configurator:

1) Access the Configurator.
2) In the configurator, select **Create EAR**.
3) By default, the .EAR file is created in the **unifier/weblogic** directory.
4) Save the file as **unifier.ear**.
5) Proceed to deploy unifier.ear in WebLogic using any of the following methods:
   - ***Deploying Unifier From the Unifier_Home Directory on Windows*** (on page 62)
   - ***Deploying Unifier from the WebLogic Administration Console*** (on page 62)

Deploying Unifier From the Unifier_Home Directory on Windows

After creating the .EAR file, deploy Unifier as follows:

1) In the **<unifier_home>\weblogic** directory, create a `setenv.bat` file by copying the `setenv_sample.bat` file.
2) Edit the `setenv.bat` file as follows:
   - Set the `domain_home` variable to specify the path of the domain home folder that will be used by Unifier.
   - Set the `admin url` variable to specify host name and port number used by the Unifier domain.
   - Set the `java_home` variable to the JDK installed directory.
   - Set the `USER_MEM_ARGS` variable specify the JVM maximum memory setting.
3) Save **setEnv.bat**.
4) Run **startup.bat**.
5) Run **deploy.bat.**
6) When prompted, enter the WebLogic user name and password.
   Unifier is deployed in WebLogic using the variables set in **setEnv.bat**.

> **Note**: This process may take several minutes.

Deploying Unifier from the WebLogic Administration Console

After creating the .EAR file in the Configurator, deploy the file from the WebLogic Administration Console as follows:

1) In the **Change Center** pane, select **Lock & Edit**.
2) In the **Domain Structure** pane, select **Deployments**.
3) In the **Summary of Deployments** pane, select **Install**.
4) In the **Install Application Assistant** pane:
   a. Specify the path to the unifier.ear file and click **Next**. For example: c:\<unifier_home>\weblogic\unifier.ear.

b. Select **Install this deployment as an application** and click **Next**.
c. Accept the defaults and click **Next**.
d. Review the configuration settings you have chosen and select **Finish** to complete the installation.

5) In the **Settings for unifier** window, select **Save**.
6) In the **Change Center** pane, select **Activate Changes**.
7) In the **Domain Structure** pane, select **Deployments**.
8) In the **Summary of Deployments** pane:
   a. Select **unifier**.
   b. Select the down arrow to the right of the **Start** button and select **Servicing all requests**.
9) In the **Start Application Assistant** pane, select **Yes**.

> **Note:** The **unifier state** column should be **Active**. If the state is **Start Running**, refresh the screen until the status is changed to **Active**.

Launching Unifier

This section describes how to:

- Start Unifier for the first time
- Install Unifier applications
- Set up your company

Before launching Primavera Unifier, ensure that you have read the Getting Started section of the Unifier Help, which contains important information about configuring your browser for use with Primavera Unifier.

Unifier URL (WebLogic)

In your browser, navigate to the URL that launches the Unifier application locally. For example: `http://unifier.oracle.com:7001`

Starting Unifier for the First Time

In the Sign In window, sign in to Unifier with the default Administrator username (*Administrator*) and password (*Administrator*).

Unifier immediately prompts you to change your password. We recommend you do so immediately for security reasons. Once you change your password, Unifier creates your Administrator account.

The Administrator account is the only account with permissions automatically set for all features. The Administrator cannot be a member of any project, even if created in the Hosting Company.

Deploying Unifier Online Help

By default Unifier online help is deployed from site hosted by Oracle. To deploy Unifier help locally, or from an alternative URL, proceed as follows:

1) Go to the Oracle Primavera Primavera Unifier Documentation Library, on the bookmark pane, click **Using**, click **Downloadable Unifier Help**.
2) The content of Unifier help (**help.zip**), when extracted, has a .war file. Deploy the .war file to an app server and then configure the **Unifier Help URL** field in the **General** tab of the **Configurator** to point to that server.

Installing Unifier on Linux

Complete the following procedures to install and configure Unifier for a first time installation. Each step corresponds to a section in this guide.

> **Note**: Before you begin, create an installation account that has full administration privileges for the server. This account is needed for maintenance and upgrades.

1) Download Unifier.
2) Configure the database server.

   Complete this step before configuring Unifier. This information will be used during database configuration in Unifier Configurator.
3) Configure WebLogic for Unifier.
4) Install and configure the Reports Server. (Optional)
5) Install Oracle WebCenter Content. (Optional)
6) Install AutoVue Server.
7) Configure Unifier using the Configurator.
8) Configure the Web Server.
9) Deploy Unifier in WebLogic.
10) Launch Unifier and install Unifier applications.

In This Section

Downloading and Extracting Unifier

Download Unifier by following these steps:

1) Go to https://edelivery.oracle.com/ (Oracle Software Delivery Cloud) and sign in.
2) Navigate to access the Primavera Unifier page.
3) Download the **Primavera Unifier** ZIP file.

The **Primavera Unifier** ZIP file enables you to download the necessary files for installing only the *platform* version of the product. The platform version of Unifier contains all the Unifier modules and allows the users to create their own designs (Business Processes and Attribute forms). This version of Unifier does not have preconfigured designs.

In addition to the Primavera Unifier ZIP file, you will see the following zip folders:

- The **Primavera Unifier Tools** ZIP file enables you to download the necessary files for installing various Unifier-related products.
- The **Primavera Unifier Documentation** ZIP file enables you to download all the Unifier documents.

4) Extract the files to a **<Unifier_Home>** directory.
5) If you need to use the command-line package to configure Unifier, complete the following:
   a. If you have downloaded and installed Unifier previously, copy the existing **bluedoor.properties** file to **<Unifier_Home>/configurator**.
   b. If you have downloaded and installed Unifier previously and you use custom properties, copy the **custom.properties** file to **<Unifier_Home>/configurator**.
6) If you have access to the**Primavera Unifier Project Controls** and/or **Unifier Facilities and Asset Management** base products (applications/products), download and install them.

   For details, see ***Downloading and Installing Unifier Base Configuration***.

Recommended Setup after Downloading Unifier

Unifier (Platform) will be available in your environments. You need a minimum of two environments:

1) Development
2) Production

> **Note**: Although the BASIC files will be available, since Unifier (Platform) is already loaded, enter only the company details to use the Unifier (Platform).

Configuring the Oracle Database Server

The following is an overview of the steps required to configure the Oracle Database for use with Unifier. For more information and specific instructions, refer to your Oracle documentation.

> **Note**: For the full list of system requirements, applications, and application version levels refer to the Unifier Tested Configurations in the Unifier Documentation Library.

Configure an Oracle Database for Unifier as follows:

1) Create an instance for the database.

> **Note**: You can accept the defaults except for the following: Ensure to set encoding to Unicode (UTF-8).

2) Create a user account on the newly created database.

   For successful Primavera Unifier/uDesigner installation, make sure ample free space of at least 2GB is available for the default tablespace where the new user will be located.

3) Grant the new user with connect, resource, create view, and create table privileges.

> **Note**: This information will be used later for setting database information in the Database tab of the Unifier Configurator.

For example:

```
create user unifier identified by unifier
temporary tablespace temp
default tablespace users;
grant connect, resource, create view, create table to unifier;
```

> **Notes**:
>
> - (Required) Ensure that maximum open cursor in Oracle DB is set to 1000, or above.
> - Ensure that Database user quota is set to unlimited on tablespace users.

Implementing Transparent Data Encryption (Optional)

Transparent Data Encryption (TDE) is an Oracle Advanced Security feature that is used for Oracle Database encryption. TDE provides strong protection from malicious access to database files by encrypting data before it is written to storage, decrypting data when being read from storage, and offering built-in key management.

For more information about TDE, refer to the Oracle Advanced Security: http://www.oracle.com/technetwork/database/options/advanced-security/overview/index.html.

The following is an overview of the steps required to configure the Oracle Database for use with Unifier. For more information and specific instructions, refer to your Oracle documentation.

> **Note**: For the full list of system requirements, applications, and application version levels refer to the Unifier Tested Configurations in the Unifier Documentation Library.

Configure an Oracle Database for Unifier as follows:

1) Create an instance for the database.

> **Note**: You can accept the defaults except for the following: Ensure to set encoding to Unicode (UTF-8).

2) Create a user account on the newly created database.

For successful Primavera Unifier/uDesigner installation, make sure ample free space of at least 2GB is available for the default tablespace where the new user will be located.

3) Grant the new user with connect, resource, create view, and create table privileges.

> **Note**: This information will be used later for setting database information in the Database tab of the Unifier Configurator.

For example:

```
create user unifier identified by unifier
temporary tablespace temp
default tablespace users;
grant connect, resource, create view, create table to unifier;
```

> **Notes**:
>
> - (Required) Ensure that maximum open cursor in Oracle DB is set to 1000, or above.
> - Ensure that Database user quota is set to unlimited on tablespace users.

Implementing Transparent Data Encryption (Optional)

Transparent Data Encryption (TDE) is an Oracle Advanced Security feature that is used for Oracle Database encryption. TDE provides strong protection from malicious access to database files by encrypting data before it is written to storage, decrypting data when being read from storage, and offering built-in key management.

For more information about TDE, refer to the Oracle Advanced Security: http://www.oracle.com/technetwork/database/options/advanced-security/overview/index.html.

Explain Plan

n order to be able to use the Explain Plan option for the Data Views, you must ensure that you the following configurations (permissions) are in place:

- grant select on v_$sql to {{user}}
- grant select on v_$sql_plan to {{user}}

Installing the AutoVue Server

AutoVue installation is mandatory if you plan to use Unifier Markup feature, also referred to as redlining.

When attaching documents to a Business Process (BP) form, you can add markups (text notes or graphical elements) that display directly on the document.

> **Note**: The markups do not alter the document.

This section describes the following procedures:

- Downloading and installing AutoVue

- Configuring AutoVue
- Deploying Custom GUI AutoVue applets

> **Notes**:
>
> - You must have a license to install AutoVue.
> - The AutoVue server is high-intensive with regard to CPU, I/O, memory, and graphics. So, for optimal performance, ensure that the machine running the AutoVue server is not being used for other applications.

For more information, refer to *Oracle AutoVue Client/Server Deployment Installation and Configuration Guide* available on Oracle Documentation website.

To configure Autovue (Apply Autovue Patch, etc.) follow these instructions:

1) Login to Oracle support site https://support.oracle.com and select the **Patches & Updates**.
2) In the **Patches & Updates** section select the **Patch Name or Number**, AutoVue XX.X.X (for the patch number or name refer to the *Primavera Unifier Tested Configurations* in the Primavera Unifier Documentation Library), and perform search.
3) Click on the result set to download the patch set zip file.
4) Follow the instructions below to apply the patch set. (Refer to the Read Me document in the patchset)
   a. Make a backup of the `gluegen-rt.jar, jogl.jar`, `jsonrpc4j.jar`, `jvue.jar`, and `jvueserver.jar` files located in <AutoVue Installation Directory>\bin directory.
   b. Copy the `gluegen-rt.jar`, `jogl.jar`, `jsonrpc4j.jar`, `jvue.jar`, and `jvueserver.jar` files from the patch to <AutoVue Installation Directory>\bin directory.
   c. Restart the AutoVue server.

> **Note**: For the full list of system requirements, applications, and application version levels refer to the *Primavera Unifier Tested Configurations* in the Primavera Unifier Documentation Library.

Downloading and Installing AutoVue

Download and install Autovue. For supported versions, refer to the *Primavera Unifier Tested Configurations* in the Primavera Unifier Documentation Library. Refer to the Oracle AutoVue documentation site for installation instructions.

> **Note**: For the full list of system requirements, applications, and application version levels refer to the *Primavera Unifier Tested Configurations* in the Primavera Unifier Documentation Library.

After the download is completed:

1) Extract the zip file and go to this directory in which you have extracted the zip file.
2) Run the AutoVue installer executable.
3) Go to the directory in which you have extracted the zip file.

4) Locate the **jvueserver.properties** file and open.
5) Add the following line at the end of the `<AutoVue install dir>\bin\jvueserver.properties` file:
   `jvueserver.authentication.enable=false`

Configuring AutoVue

After installing AutoVue, configure AutoVue by entering information in the following tabs of the Unifier Configurator:

- In the **General** Tab, enter the **Server internal URL** field to access AutoVue.
- In the **Markup Server** Tab, complete all fields in this tab.

Deploying Unifier GUI Applets to AutoVue

AutoVue provides the option of customizing third-party graphical user interface (GUI). The following Unifier applet GUI files are provided to integrate with AutoVue:

- `default.gui`
- `defaultcons.gui`
- `defaultNoMarkup.gui`
- `defaultview.gui`

To deploy the Unifier applet GUI files to AutoVue:

1) Download the current version of the **Primavera Unifier Tools** file from the Oracle Software Delivery Cloud (https://edelivery.oracle.com/).
2) Unzip the **AutoVueMenus.zip** file into the location specified in the **jvueserver.users.directory** parameter in the **<AutoVue install dir>\bin\jvueserver.properties** file.
3) Follow the recommendation in the Oracle AutoVue documentation site.

> **Note**: For the full list of system requirements, applications, and application version levels refer to the *Primavera Unifier Tested Configurations* in the Primavera Unifier Documentation Library.

Configuring WebLogic for Unifier on Linux

This section describes how to configure WebLogic for Unifier on a Linux 64-bit operating system. It includes:

Creating a WebLogic Domain for Unifier on Linux

To create a WebLogic domain:

1) Run the WebLogic **Configuration Wizard**.
2) In the **Welcome** window:
   a. Select **Create a new WebLogic** domain.
   b. Click **Next**.
3) In the **Select Domain Source** window, click **Next** to accept the default selections.
4) In the **Specify Domain Name and Location**:
   a. Enter a domain name for the new domain to be created.
   b. Enter the location of the new domain on the server.
   c. Click **Next**.
5) In the **Configure Administrator User Name and Password** window:
   a. Enter the User Name and Password for the Administrator that will be created. This user name will be used to login to the WebLogic console.
   b. Click **Next**.
6) In the **Configure Server Start Mode and JDK** window:
   a. In the left pane, select **Production Mode**.
   b. In the right pane, select the JDK you installed earlier.
   c. Click **Next**.
7) In the **Select Optional Configuration** window:
   a. Select the **Administration Server** option.
   b. Click **Next**.
8) (Optional) In the **Configure the Administration Server** window:
   a. Select the SSL enabled option and set the SSL listen port if you are enabling Secure Sockets Layer communication.

      See http://download.oracle.com/docs/cd/E12840_01/wls/docs103/secmanage/ssl.html for more details on setting SSL for WebLogic.

      Note: Oracle recommends you always use SSL in a production environment for secure communications.

   b. Click **Next**.
9) In the **Configuration Summary** window, click **Create**.
10) Click **Done** after the domain is created.
11) When prompted, enter the **Administrator User Name** and **Password** that you entered above.

Configuring WebLogic Basic Authentication on Linux

Authorization

The system authenticates all Unifier users' requests based on the Authorization header. In a stand-alone Unifier environment, the user name and password is determined based on the Basic Authorization headerEnsure that you disable the Basic Authentication by following these steps:

Understanding BASIC Authentication with Unsecured Resources (http://docs.oracle.com/middleware/1221/wls/SCPRG/thin_client.htm#SCPRG150)

1) Change to the `weblogic_home/user_projects/domains/your_domain` directory
2) Edit `config/config.xml` by adding the following tag within the`<security-configuration>` tag:

   ```
   <enforce-valid-basic-auth-credentials>false</enforce-valid-basic-aut
   h-credentials>
   ```
3) Start or restart all servers in the domain.

Starting the WebLogic Admin Server on Linux

To deploy Unifier in WebLogic, start the Admin server as follows:

1) Change to the *weblogic_home*/user_projects/domains/*your_domain* directory.
2) Run the **startWebLogic.sh** script.
3) If prompted for a user name and password in the WebLogic console window, type in the administrative user name and password you specified when creating the domain.

> **Note**: If you turned on the WebLogic precompile option, the WebLogic console displays "Server started in RUNNING mode" when precompiling finishes. For detailed information about turning on precompilation, see your WebLogic Server documentation.

Stopping the WebLogic Admin Server on Linux

When you are finished working in the WebLogic Administration Console, stop the WebLogic admin server as follows:

1) Change to the `weblogic_home/user_projects/domains/domain_home/bin` directory.
2) Run the **stopWebLogic.sh** script.
3) If prompted for a user name and password in the WebLogic console window, enter the administrative user name and password that was specified when creating the domain.

> **Note**: The WebLogic console window will close automatically at shutdown.

Configuring WebLogic and OHS as a Service on Linux

Complete the following steps to install WebLogic and Oracle HTTPS Server (OHS) as a service on a Linux 64-bit operating system.

1) Set **WL_HOME** as system environment variable or modify it in **<unifier_home>/weblogic/setenv.sh**. WL_HOME is the root directory of the WebLogic installation. For detailed instructions, refer to the topic, ***Creating a WebLogic Domain for Unifier on Windows*** (on page 18) to create the Domain Home for weblogic.

   For example: C:\Oracle\Middleware\wlserver_11\server
2) Set the environment variables for Unifier. For detailed instructions, refer to ***Changing Unifier Configurator Settings on Windows*** (on page 22).
3) For WebLogic installed in production mode, create **boot.properties** at **$DOMAIN_HOME/servers/<server_name>/security**.
4) Ensure all variables are set for a ROOT_USER.
5) Login to Linux as a ROOT_USER.
6) In the **<unifier_home>/weblogic/unifier**, modify values for the following parameters:
   - OHS_INSTANCE_HOME: The home directory of OHS.
   - UNIFIER_HOME: The home directory of Primavera Unifier.
   - OHS_USER: User who can start OHS. Alternatively, locate the user in the **httpd.conf** file.
   - WL_USER: User who can start WebLogic.

   Note: Change the command to start weblogic in accordance to the user privilege on the system.
7) Ensure that when the server is restarted the Xvfb process is also started with the same DISPLAY value as follows for the ROOT_USER:
   a. Install Xvfb

      yum install Xvfb
   b. start Xvfb

      locate Xvfb (where Xvfb is installed)

      /usr/bin/Xvfb :99 -screen 0 1x1x8 &
   c. Edit the unifier file to add: `export DISPLAY=:99`
8) Copy the **unifier** script into the **/etc/rc.d/init.d** folder
9) To make the file executable, run the command: **chmod 755 unifier**
10) To add the service at system reboot, run the command: **chkconfig --add unifier**
11) To start the unifier service from the console, run the command: **service unifier start**

Stopping the Service

To stop the unifier service from the console, run the command: **service unifier stop**

Uninstalling the Service

To remove the service, run the command: **chkconfig --del unifier**

Configuring SSL Hostname Verification

Note: This is required for Adobesign, Docusign, and Bluebeam

integrations.

If your app server has Hostname verification configuration, this has to be extended to support the above hosts.

This can also be done by either of the below approaches -

Login into Weblogic console -> Environment -> Servers -> Choose and click on the server name where Unifier is deployed -> SSL -> Expand Advanced (at bottom)

Choose the below values for the below attributes.

Hostname Verification: Custom Hostname Verifier

Custom Hostname Verifier: weblogic.security.utils.SSLWLSWildcardHostnameVerifier

Or set the below property in the startup script of your WebLogic App Server

e.g.

SET JAVA_OPTIONS=%JAVA_OPTIONS% -

Dweblogic.security.SSL.hostnameVerifier=weblogic.security.utils.SSLWLSWildcardHostnameVerifier

Installing and Configuring the Reports Server (Optional)

Consult your Oracle documentation for instructions on installing Oracle Business Intelligence Publisher.

> **Note**: For the full list of system requirements, applications, and application version levels refer to the *Primavera Unifier Tested Configurations* in the Primavera Unifier Documentation Library.

For configuration information for integrating Unifier and BI Publisher, refer to the *Unifier BI Publisher Configuration Guide*.

Installing Oracle WebCenter Content (Optional)

Consult Oracle documentation for instructions on installing the Oracle WebCenter. For configuration information for integrating Unifier and WebCenter content, refer to *Unifier Content Repository Configuration Guide*.

Configuring Unifier Using the Configurator UI

This section describes how to use the standard Unifier Configurator user interface (UI) to configure Unifier. If you are using JDK 8, complete the steps outlined under ***Configuring Unifier Using a Command-Line Interface (CLI)*** (on page 37).

Editing the SetEnv.sh File on Linux

Ensure that the following variables are saved in the **setenv.sh** file:

- Set the `domain_home` variable to specify the path of the domain home folder that will be used by Unifier.
- Set the `admin url` variable to specify host name and port number used by the Unifier domain.
- Set the `java_home` variable to the JDK installed directory.
- Set the `USER_MEM_ARGS` variable specify the JVM maximum memory setting.

Changing Unifier Configurator Settings on Linux

The Unifier environment is configured through the Unifier Configurator window. To change settings in Unifier Configurator:

1) Open the **WebLogic** directory in the **Unifier Home** folder.
2) Run **configure.sh**.
3) Configure the settings for each tab.
4) Click **Save** on each tab.
5) Restart Unifier for the changes to be operative.

General Tab

Server Type is the setting that defines the mode Unifier server is running.

- Set **Server Type** to **Production** if this Unifier installation is acting as the Unifier production environment.

  In this environment, you cannot publish configuration packages.

  The uDesigner designs are read-only.
- Set **Server Type** to **Development** if this Unifier installation is acting as the development server for testing of business processes and other Unifier designs and configurations.

  You cannot convert a **Development** environment to a **Production** environment because all the designs, in uDesigner, must be published in the **Production** environment.

  Note: To have one source of published designs, and to prevent designs and data corruption, Oracle recommends that you have one **Development** environment, only.
- Set **Server Type** to **Test** if this Unifier installation is acting as the test server for testing of business processes and other Unifier designs and configurations.

  In this environment, you cannot publish configuration packages.

Temporary Directory: Enter the temporary directory for Unifier server operations. The Temporary Directory must be local to the server. If you do not want to place the Temporary Directory on a local server, then you must select a different value for the shared location.

Background Job Disabled: Select to disable background jobs.

Server Internal URL: Enter the WebLogic Server URL running the Unifier (For example: `http://host1.example.com:7001`)

> **Note**: BI Publisher and Markup servers use this URL to communicate with Unifier.

Login Session Timeout: Login Session Timeout is used to control the amount of time a user can be idle before having to log back into Unifier. The unit is seconds. For security reasons, the recommended timeout setting is between 30 minutes and 4 hours.

Overdue Tasks Check Interval: Interval, in minutes, used by the internal job server for notification tasks. The suggested interval is 15 minutes. A very small interval may degrade performance.

Test Server Label: This field displays only for Test servers. Enter a custom name for the Test server. The name cannot exceed 30 characters and cannot be labeled Development or Production. It can include all special characters except - (dash/hyphen) and _ (underscore).

UPK Help URL: Enter the URL where the User Productivity Kit (UPK) help content is to be hosted (as a generic example, http://servername/contextroot, or as a specific example is http://localhost/unifierupk).

Unifier Help URL: To deploy a local version of the Unifier online help, enter the URL where the help file is to be hosted.

Repository Tab (CMIS)

The following fields display when you select **CMIS** in the **File Repository** field.

CMIS Login Name: Enter the user name for your content repository.

CMIS Password: Password for the CMIS login name.

CMIS Repository Name: The content repository name.

CMIS Documentation Home: The documentation home.

CMIS Web Service URL: The URL for your web services home.

> **Notes:**
>
> - It is important to plan where these directories are located because they are where Unifier data is stored. Any subsequent upgrade installations need to point to these same location in order for Unifier to 'see' data previously entered.
> - These repositories, in addition to your database, should be backed up

regularly.

- When naming the folders, be sure there are no spaces in the folder names.
- These files must be on a shared drive that is accessible by other server machines that are operating in a clustering environment.

Index Directory: This folder is for index files used in Document Manager search function. This field is not visible when repository is set to CMIS.

Log File Directory: The folder where the log files are stored.

When Unifier is installed on a multibyte server and connecting to SharePoint or CMIS:

1. Add `"-Djavax.xml.parsers.DocumentBuilderFactory=com.sun.org.apache.xerces.internal.jaxp.DocumentBuilderFactoryImpl"` Java option to **setenv.sh/setenv.bat** file.
2. Restart Unifier.

The above settings enable you to view documents in CMIS.

Examples

Setting in **setenv.bat** file: `SET JAVA_OPTIONS=%JAVA_OPTIONS% -Djavax.xml.parsers.DocumentBuilderFactory=com.sun.org.apache.xerces.internal.jaxp.DocumentBuilderFactoryImpl`

Setting in **setenv.sh** file: `export JAVA_OPTIONS="$JAVA_OPTIONS -Djavax.xml.parsers.DocumentBuilderFactory=com.sun.org.apache.xerces.internal.jaxp.DocumentBuilderFactoryImpl"`

Repository Tab (Database)

The following fields display when you select **Database** in the **File Repository** field.

Host Name: Enter the host name of the computer where you installed the database.

Instance ID: The Instance ID field in the Configurator can accept the following values:

- An Oracle SID
- An Oracle service name (Oracle Database)

> **Note**: For the full list of system requirements, applications, and application version levels refer to the Unifier Tested Configurations in the Unifier Documentation Library.

When you enter a service name for an Oracle service name (Oracle Database), you must preface the name with a forward slash (/), for example, `/servicename`.

If you do not preface the name with a forward slash (/), the system presumes that you have:

- Entered an Oracle SID, if you had selected Oracle from the drop-down list.

Port: Enter the Port number to be used by Unifier to communicate with the database (For example: 1521).

User Name: Enter the database login user account name (created in Oracle) to be used by Unifier. The database login user account needs to have sufficient permissions to create tables in order for Unifier to work correctly.

User Password: Enter the database login user account password to be used by Unifier.

The user has to have the following permissions:

- Connect
- Resource
- ctxapp
- Create job
- run, on ctxsys.ctx_ddl
- run, on dbms_scheduler

Log File Directory: The folder where the log files are stored.

Repository Tab (Network File System)

This topic applies when you select **Network File System** for the File Repository field.

There are two data repositories (folders in which Unifier data is stored), which Unifier requires you to configure. There are additional repositories, such as the archive directory for project archiving, that are used with specific features, as described below. These can be located on a local but separate hard drive, or on a mapped drive on your network.

- **File Repository:** In this field, select **Network File System** from the drop-down list.

Notes:

- It is important to plan where these directories are located because they are where Unifier data is stored. Any subsequent upgrade installations need to point to these same two directories in order for Unifier to 'see' data previously entered.
- These repositories, in addition to your database, should be backed up regularly.
- When naming the folders, be sure there are no spaces in the folder names.

File Directory: Enter (or Browse to) the path where uploaded or attached files are stored. This repository is for storing documents within the Document Manager, such as drawings, plans, Word documents, etc. These files will be available for viewing or attaching to business process forms within Unifier. It also stores imported schedule files.

Notes:

- These files must be on a shared drive that is accessible by other server machines that are operating in a clustering environment.
- Ensure that the user who has started the Unifier application is a network user and has access to network file system.
- Ensure that the File directory value is same in all the machines in the

cluster. Use the repository machine name or IP address to specify the shared drive location.

- Ensure that enough disk space is available on the network file system.

Index Directory: This is the pathname to the location where the Search Index files are stored.

Log File Directory: The folder where the log files are stored.

Repository Tab (WebCenter Content)

This topic applies when you select WebCenter Content for the File Repository field.

File Repository: Select WebCenter Content.

WebCenter Content Server Host: This is the IP address of the WebCenter Content server.

WebCenter Content Server Port: This is the port of the WebCenter Content server.

WebCenter Content User: This is the user who will add documents through the API. The user should exist in the WebCenter Content server.

WebCenter Content Root Folder: The root folder in WebCenter Content under which all Unifier folders will be created.

Notes:

- It is important to plan where these directories are located because they are where Unifier data is stored. Any subsequent upgrade installations need to point to these same location in order for Unifier to 'see' data previously entered.
- These repositories, in addition to your database, should be backed up regularly.
- When naming the folders, be sure there are no spaces in the folder names.
- These files must be on a shared drive that is accessible by other server machines that are operating in a clustering environment.

Log File Directory: The folder where the log files are stored.

Test WebCenter: Enables you to validate the configuration settings that you have entered.

Database Tab (Oracle)

The information entered in this tab is based on your earlier database and user account creation.

Database Type: Select **Oracle**.

Host Name: Enter the host name of the computer where you installed the database.

Instance ID: The Instance ID field in the Configurator can accept the following values:

- An Oracle SID
- An Oracle service name (Oracle Database)

> **Note**: For the full list of system requirements, applications, and application version levels refer to the Unifier Tested Configurations in the Unifier Documentation Library.

When you enter a service name for an Oracle service name (Oracle Database), you must preface the name with a forward slash (/), for example, `/servicename`.

If you do not preface the name with a forward slash (/), the system presumes that you have entered an Oracle SID.

Port: Enter the Port number to be used by Unifier to communicate with the database (For example: 1521).

User Name: Enter the database login user account name (created in Oracle) to be used by Unifier. The database login user account needs to have sufficient permissions to create tables in order for Unifier to work correctly.

User Password: Enter the database login user account password to be used by Unifier.

Max. Connections: The setting that defines the maximum connections to the database. The maximum is 400; the recommended maximum is 80 to 100.

Min. Connections: The setting that defines the minimum connections that must be connected to the database.

Test Connection: Click **Test Connection** to verify that the Application server and the database are connected and communicating. A *Test is successful* message will appear if test is successful. Two conditions are tested:

- Ability of Unifier to connect to the database
- Level of permissions granted to the database login user account

Email Tab

Outbound (SMTP) E-mail Server: (*Required*) Enter the IP address or the URL/machine name.

E-mail Sender Prefix: Enter the email prefix that will be used in the Sender's name whenever an email is generated from a user from within Unifier, for example, `Unifier`. Late email notifications show the E-mail Sender Prefix, only.

Support Contact Information: This field contains the message text that is included in all support-related email notifications.

To enable an email address as a hyperlink, use the following format: <a `href="mailto:name@example.com">name@example.com</a>`

Outbound (SMTP) Authentication Required: Select if authentication is required by the outbound SMTP email server.

Outbound (SMTP) E-mail Account: Enter the outbound Email account.

Outbound (SMTP) E-mail Password: Enter the password that corresponds to the outbound Email account.

Outbound (SMTP) E-mail Encryption Type: (*Optional*) To support TLS protocol, select from one of the following options supported by SMTP server (**Outbound (SMTP) E-mail Server**):

- **SSL/TLS**
- **STARTTLS**

Proxy Server URL for APNs Server: URL of the proxy server used to connect to Apple Push Notification Service.

Proxy Server Port for APNs Server: Port of the proxy server used to connect to Apple Push Notification Service.

> **Note**: Unifier supports outbound email without authentication or with authentication using SSL.

System Notification E-mail Address: This field contains the email ID that the system displays as the "Sender's" email address for all emails generated by the Unifier system, for example, `admin@example.com`.

Project Email Patter: This field has the following values: Suffix and Prefix and determines the project email ID supported (`<pid>-<inboundemail>@oracle.com` or `<inboundemail>+<pid>@oracleindustry.com`).

System Error Notification E-mail Address: This field contains the email address where Unifier sends a notification if Unifier loses connection to the database while the system is running. The email addresses can be separated by semicolon.

License Notification E-mail Address: This field contains the email address where Unifier sends licensing notifications, for example, if the number of users exceeds the number of available licenses. If the number of users exceeds the number of available licenses, then the system sends notifications to the following:

- Users specified in the configurator (Unifier Configurator WebLogic).
- Users who have Notify permission in the License Manager, which was set in Access Control.

Inbound E-mail protocol: Select the protocol used by the inbound email server that can receive email. The supported protocols are POP3, IMAP, POP3S, and IMAPS.

Each Unifier environment (Development, Test, and Production) must be configured with its own inbound email account. To prevent undesired results, do not use the same inbound email for all the environments.

Inbound E-mail Server: Enter the server that can receive email, for example, if a user takes action via email on a business process. This can be the server name or IP address.

(Optional) You can specify the port number after the server name of IP address, for example, `example.com:1521`.

Inbound E-mail Account: Enter the email account to receive response email from the user.

To use the project or shell Mailbox, which allows external email messages to be sent to and stored within a central project or shell mailbox, use the following format for the inbound email account. This allows acceptance of inbound emails sent to the system-generated project/shell email addresses: `*-inboundemailname@example.com.` This configuration is needed on the email server, not within the Unifier Configurator.

Inbound E-mail Password: This field contains the password that corresponds to the inbound email account. This password is used when email is retrieved.

Test Inbound Connection: Enables you to test the Inbound E-mail Server, Inbound E-mail Account, and Inbound E-mail Password.

Test Outbound Connection: Enables you to test the outbound E-mail Server, outbound E-mail Account, and outbound E-mail Password.

About Inbound E-mail

If you are using a open-source `hMailServer` to configure Unifier for inbound emails, ensure that you turn off the "auto ban" feature. If you do not turn off the "auto ban" feature, then you will not be able to use Unifier functionalities such as Project Mailbox and Workflow action view E-mail.

The Project Mailbox functionality rely on email address used for BP Action via Email. If the Inbound email address is `unifier_oracle@unifiermail.com`, then the email address of a Project/Shell could be one of the following, depending on the property value in the `skire.project.email.pattern` in `skire.properties` file. This property can have two values: "prefix" or blank and "suffix." This property can be set either manually (in the skire.properties file) or by selecting the appropriate value from Unifier Configurator - Email Tab and saving the changes.

In case the property value is "prefix" or blank

The email address of any Unifier Project/Shell will follow the pattern `<project id>-unifier_oracle@unifiermail.com` used for Project Mail box functionality. For example, if the project id is 1001, then email address for this particular Project/Shell will be `1001-unifier_oracle@unifiermail.com`. For this to function, you have to set up an email forwarding rule on your mail server such that any emails sent to `.*-unifier_oracle@unifiermail.com` will be automatically forwarded to `unifier_oracle@unifiermail.com` Inbox.

In case the property value is "suffix"

The email address of any Unifier Project/Shell will follow the pattern `unifier_oracle+<project id>@unifiermail.com` used for Project Mail box functionality. For example, if the project id is 1001, then email address for this particular Project/Shell will be `unifier_oracle+1001@unifiermail.com`. For this to function, you have to set up an email forwarding rule on your mail server such that any emails sent to `unifier_oracle+.*@unifiermail.com` will be automatically forwarded to `unifier_oracle@unifiermail.com` Inbox.

If you are using an email address on `oracleindustry.com` domain, you must use the "suffix" pattern, and you must, explicitly, set `skire.project.email.pattern=suffix` because this property is not exposed in current Unifier configurator. The email forwarding rule (for suffix pattern) is enabled on this domain by default.

On Unifier configurator, ensure that you include the port number for the current protocol in Inbound E-mail Server field, for example, `unifiermail.com:110` or `oracleindustry.com:993`. The protocol and port mapping are as follows:

- POP3 - port 110
- IMAP - port 143
- IMAPS - port 993
- POP3S - port 995

To prevent the spam emails to go in the Project Mail box, the system accepts emails from email addresses associated with Unifier user account or the email addresses listed in Approved Email List by Company Admin, *only*.

Markup Server Tab

Use Server Internal URL: (Optional) Select this option only if server internal URL address must be used by markup server to communicate with Unifier. If not selected (default), The user's login base URL address is used by markup server to communicate with Unifier.

Markup Server Host Name: Enter the host name of the markup server.

Markup Server Port: Enter the port number of the markup server. The default port number for AutoVue is 5099.

Important information about AutoVue

When Unifier is installed on a multibyte server and connecting to AutoVue, or when you are having issues with viewing documents in AutoVue from Unifier:

1) Add `"-Djavax.xml.parsers.DocumentBuilderFactory=oracle.xml.jaxp.JXDocumentBuilderFactory"` Java option to `setenv.bat` file.
2) Restart Unifier.

The above settings enable you to view documents in AutoVue.

Example

Setting in setenv.bat file:
```
SET JAVA_OPTIONS=%JAVA_OPTIONS% -Djavax.xml.parsers.DocumentBuilderFactory=oracle.xml.jaxp.JXDocumentBuilderFactory
```

Setting in `setenv.sh` file:
```
export JAVA_OPTIONS="$JAVA_OPTIONS -Djavax.xml.parsers.DocumentBuilderFactory=oracle.xml.jaxp.JXDocumentBuilderFactory"
```

Report Tab

BIP Endpoint URL: Enter the BIP Web Services endpoint URL. For example: http://host1.example.com:9502

BIP User Name: Enter the user name created for the BI Publisher server.

BIP Password: Enter the password for the BI Publisher user.

BIP Data Source: Enter the JDBC data source name that was entered when the JDBC Data Source BI Publisher

BIP Report Folder: The folder under the default location in the BI Publisher catalog. Reports reside in this folder based on company registry.

BIP External Report Folder: The folder under the default location in the BI Publisher catalog. External Reports, synchronized in Unifier, reside in this folder.

> **Note**: The values used in the BIP User Name, BIP Password, BIP Data Source, and BIP Report folder fields are the same as those created when using the *Unifier BI Publisher Configuration Guide*.

OBIEE Analytics URL: The URL to OBIEE Analytics service. This URL should be accessible via internet.

Test Report Connection: Enables you to validate the configuration settings that you have entered.

Geo Map Tab

Map Server Url: Enter **https://elocation.oracle.com**. This is the Oracle Map server base URL where the Oracle MapVeiwer application is deployed with the context "mapviewer". This is where the server obtains the map image.

Map Tile: Enter **elocation_mercator.world_map**. This is the name of the map tile layer (the base map used for map rendering) that was pre-defined on the Oracle Map server. This is the map data source.

Map Geocoder Url: Enter **https://elocation.oracle.com**. This is the server URL where the Oracle Geocoder application is deployed with the context "geocoder." This is the location service.

Authentication Tab (Native)

Authentication Type: Native

The Unifier default authentication mechanism is used.

Login URL: Enter the URL to log in to Unifier.

Authentication Tab (OIM/OAM)

Authentication Type: OIM/OAM

The system determines whether integration of Primavera Unifier with Oracle Identity Manager (OIM) and Oracle Access Manager (OAM) is enabled.

SSO Logout: The logout URL for Oracle Access Manager (OAM) or any third-party Single Sign On (SSO) configuration. For more details, refer to Oracle Access Manager documentation.

Login URL: Enter the URL to log in to Unifier.

Authentication Tab (ORACLE IDENTITY CLOUD SERVICE)

Authentication Type: ORACLE IDENTITY CLOUD SERVICE

Login URL: Enter the URL to log in to Unifier.

SSO Header: Header value used while configuring SSO.

SSO Logout: The logout URL for Oracle Identity Cloud Service.

Authentication Tab (WebLogic)

Authentication Type: Weblogic

Form-based authentication is used to integrate with WebLogic authentication methods. After WebLogic authenticates the user, Unifier determines if the user is a valid Unifier user before granting access to the application.

Realm: Weblogic realm that is used for authentication.

Group(s) (comma separated): Weblogic group name, a comma separated list, used for mapping Weblogic groups to "unifieruser" role.

Login URL: Enter the URL to log in to Unifier.

Authentication Tab (LDAP Simple Bind)

The Lightweight Directory Access Protocol (LDAP) is a protocol for querying, and modifying, directory services. The Administrator can configure the server to use either simple-bind or double-bind authentication.

Authentication Type: LDAP Simple Bind

Login URL: Enter the URL to log in to Unifier.

Provider: To connect the LDAP server (URL), for example, `ldap://ldap.zyz.com:636`

SSL: To connect to the Secure Sockets Layer (SSL) enabled port of the LDAP server.

> **Note**: Oracle recommends you always use SSL in a production environment for secure communications.

When Unifier is configured with JDK 8 and integrated with LDAP SSL:

- Add "-Djdk.tls.client.protocols=TLSv1" Java option to **setenv.sh** file.
- Restart Unifier.

The above settings enable you to log in using LDAP SSL.

Example

Setting in **setenv.sh** file: export `JAVA_OPTIONS="$JAVA_OPTIONS -Djdk.tls.client.protocols=TLSv1"`

Security Principal Template: To authenticate directly, based on the user name and password (Simple Bind). The template is used to construct the user's Distinguished Name (DN), for example, `cn={0},l=amer,dc=oracle,dc=com`

Admin User Bypass: To allow administrators to bypass LDAP login.

Authentication Tab (LDAP Double Bind)

The Lightweight Directory Access Protocol (LDAP) is a protocol for querying, and modifying, directory services. The Administrator can configure the server to use either simple-bind or double-bind authentication.

Authentication Type: LDAP Double Bind

Login URL: Enter the URL to log in to Unifier.

Provider: To connect the LDAP server (URL), for example, `ldap://ldap.zyz.com:636`

SSL: To connect to the Secure Sockets Layer (SSL) enabled port of the LDAP server.

When Unifier is configured with JDK 8 and integrated with LDAP SSL:

- Add "-Djdk.tls.client.protocols=TLSv1" Java option to **setenv.sh** file.
- Restart Unifier.

The above settings enable you to log in using LDAP SSL.

Example

Setting in **setenv.sh** file: export `JAVA_OPTIONS="$JAVA_OPTIONS -Djdk.tls.client.protocols=TLSv1"`

Provider Base: (Optional) When you select the Double Bind method of authentication, you need to find the user's DN and then authenticate them. Finding the user's DN is used as the base for searching the LDAP tree. If the Provided Base is not set, the root is assumed by the system: `ldap.provider.base`

Authorized User: When using the Double Bind method of authentication, find the user's Distinguished Name (DN) and then authenticate. This is used as the "trusted" or "search" login user's DN (first bind).

Authorized User Password: When using the Double Bind method of authentication, this is the authorized user's login password.

Search Field: The default value is "cn." You need to enter the node field that you want to search.

Admin User Bypass: To allow the administrator bypass the LDAP login.

Test User Name (not Saved): Enter the LDAP user name to test the LDAP server.

Test User Password (not Saved): Enter the LDAP password to test the LDAP server.

Authentication Tab (Generic SSO)

User Authentication Type: Generic SSO

Login URL: Enter the URL to log in to Unifier.

SSO Header: Header value used while configuring SSO.

> **Note**: For OAM SSO, the value is OAM_REMOTE_USER and for Shibboleth, the value is REMOTE_USER.

SSO Logout: The logout URL for Oracle Access Manager (OAM) or any third-party Single Sign On (SSO) configuration. For more details, refer to Oracle Access Manager documentation.

> **Note**: If Unifier is configured with Shibboleth as SP and IDP, add the following option `ProxyPreserveHost On` in the `httpd-ssl.conf` file in the Shibboleth SP.

Advanced Tab

The **Advanced** tab has the following fields:

Enable Password Encryption	When the password encryption is enabled, the system saves the signature in bluedoor properties file, or a secure location.
Server Time Zone	The server time zone.
Background Job Threads	The number of threads for background jobs.
High Priority Job Threads	The number of threads for high priority jobs.
Include Custom Properties	Check this box to use custom.properties file (in /configurator directory) to set additional properties.
Support Session Failover	Check this box to keep session alive when the server goes down.

Secure Key Location	The directory path where the file containing file "`unifier.properties`" will be stored. The "`unifier.properties`" file will contain the "unifier.secure.seed" property. This setting is optional. If not set, the secure key (a random string) will be generated by the Configurator and stored in the "`skire.properties`" file. If a folder location is given as a secure key location, then the key will be stored in an additional property file in the given folder for extra security (assuming that the secure key folder is a folder with very selective access that is not readable by most IT personnel). This location must be accessible from Unifier server.
Partner Login URL	The JVM default time zone. This time zone must match the java startup parameters. For example: Duser.timezone=America/Chicago. If set, Unifier generated email sent to partner user (users that do not belong to the owner company) containing the given login URL. All user emails will have the same login URL defined in the email tab, normally. This login URL is used in Cloud environment where the owner and partner use different SSO solution.
Oracle Map Server: Proxy Server URL	The URL for the proxy server that is used to connect to Oracle Map/Geocoder server. Unifier connect to `elocation.oracle.com` to get location information from the US address. This is the proxy setting required (if necessary) for Unifier server to connect to elocation server.
Oracle map Server: Proxy Server Port	Port for the proxy server that is used to connect to Oracle Map/Geocoder server. Unifier connect to "`elocation.oracle.com`" to get location information from the US address. This is the proxy setting required (if necessary) for Unifier server to connect to "elocation" server.

Is the above integrator key setup for DocuSign production environments?	Check this box only if the integrator key has been promoted to the production account by using the go-live process. ▸ If you select this option, then Unifier will redirect the customer to login to Production DocuSign Account. ▸ If you do not select this option, then Unifier will redirect the customer to Demo DocuSign Account.

Changing Configurator Settings on Linux

After initially installing and configuring Unifier, you must follow this procedure to make any subsequent changes to the configuration settings:

1) ***Stopping Unifier in WebLogic on Linux*** (on page 89)
2) ***Editing Configuration Data on Linux*** (on page 89)
3) ***Starting Unifier in WebLogic on Linux*** (on page 89)

Stopping Unifier in WebLogic on Linux

To stop Unifier in WebLogic:

1) Open the **WebLogic** directory within the **Unifier Home** folder.
2) Run the **stop.sh** file.
3) If prompted, enter the WebLogic user name and password.

Editing Configuration Data on Linux

After stopping Unifier, edit the configuration settings as follows:

1) In the **WebLogic** directory within the **Unifier Home** folder, locate the **configure.sh** file.
2) Run **configure.sh**.
3) Make necessary configuration changes, and click **Save**.
4) Start Unifier in WebLogic.

Starting Unifier in WebLogic on Linux

To start Unifier in WebLogic:

1) Open the **WebLogic** directory within the **Unifier Home** folder.
2) Run the **startup.sh** file.
3) If prompted, enter the WebLogic user name and password.

Opening the Configurator

To open the Configurator follow these steps:

1. Install xorg-x11 fonts using following commands:

```
repoquery -q -f */xclock
sudo yum -y install xorg-x11-apps
sudo yum -y install xorg-x11-fonts*
sudo yum groupinstall "Development Tools"
sudo yum install gtk+-devel gtk2-devel
```

2. Go to Unifier/configurator and edit the build.xml file by adding the following lines:

```
<target name="configure-o" if="not.isSolaris">
<echo message="Starting Primavera Unifier Configurator..."/>
<java classname="com.skire.configuratorfx.ConfiguratorFx" fork="yes"
  failonerror="true">
<arg value="${env.JAVA_HOME}"/>
<arg value="${env.UNIFIER_HOME}"/>
<jvmarg value="-Dapplication.home=${env.UNIFIER_HOME}/configurator"/>
<jvmarg value="-Dprism.useFontConfig=false"/>
<jvmarg value="-Dprism.fontdir=$JAVA_HOME/jre/lib/fonts"/>
<!--$JAVA_HOME should be replaced by the server dependent JAVA_HOME
path-->
<jvmarg value="-Dapplication.server=${env.APPSERVER_TYPE}"/>
<classpath refid="config-classpath"/>
</java>
</target>
```

3. Go to JAVA_HOME/jre/lib/fonts and create a file logicalfonts.properties with the following content:

```
sans.regular.0.font=Lucida Sans Regular
sans.regular.0.file=LucidaSansRegular.ttf
sans.bold.0.font=Lucida Sans Bold
sans.bold.0.file=LucidaSansDemiBold.ttf
monospace.regular.0.font=Lucida Typewriter Regular
monospace.regular.0.file=LucidaTypewriterRegular.ttf
monospace.bold.0.font=Lucida Typewriter Bold
monospace.bold.0.file=LucidaTypewriterBold.ttf
serif.regular.0.font=Lucida Bright
serif.regular.0.file=LucidaBrightRegular.ttf
serif.bold.0.font=Lucida Bright Demibold
serif.bold.0.file=LucidaBrightDemiBold.ttf
serif.italic.0.font=Lucida Bright Italic
serif.italic.0.file=LucidaBrightItalic.ttf
serif.bolditalic.0.font=Lucida Bright Demibold Italic
serif.bolditalic.0.file=LucidaBrightDemiItalic.ttf
```

Copying the Configuration Data File

The configuration data for the Configurator is stored automatically under the installation folder in the **/configurator/bluedoor.properties** file. If necessary, you can transfer the configuration settings from one environment to another by copying the configuration data file and editing it with the new configuration settings.

Configuring Unifier Using a Command-Line Interface (CLI)

The following guidelines are for customers who are using JDK 8, which does not include JavaFX.

- If you are setting up a new environment that does not have a **bluedoor.properties** file, you must create it first. For more information, see ***Creating the bluedoor.properties File*** (on page 38).
- If you need to use encryption, complete the steps outlined under ***Using Encryption*** (on page 51).
- If you are performing an upgrade, complete the steps outlined under ***Completing an Update or Upgrade*** (on page 56).

Creating the bluedoor.properties File

You can use the blank_bluedoor.properties file to create and complete the file for a new environment.

1) Go to: `<Unifier_Home>/configurator`
2) Copy the **blank_bluedoor.properties** file to the same location (**<Unifier_Home>/configurator**) but rename the file to **bluedoor.properties**.
3) Use the information provided in the following tables to complete the specified sections.

General

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
Server Type	server.type	production, test, dev		Yes	Select Text	No
Server Internal	server.internal.url			Yes	Text	No
Temporary Directory	file.temppath			Yes	Text	No
UPK Help URL	upk.help.url			No	Url Text	No
Background Job Disabled	job.disabled	true, false		No	Boolean Text	No

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
Unifier Help URL	help.url			No	Url Text	No
Login Session Timeout	login.timeout			No	Number	No
Overdue Tasks Check Interval	server.scheduler.interval			No	Number	No

Repository

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
File Repository	ucr.repositorytype	CMIS, NETWORK FILE SYSTEM, DATABASE, WEBCENTER CONTENT		Yes	Select Text	No
Log File Directory	log4j.logfile.home			Yes	Text	No
File Directory	server.file.rootpath		ucr.repositorytype=NETWORK FILE SYSTEM	Yes	Text	No
Index Directory	server.file.index.rootpath		ucr.repositorytype=NETWORK FILE SYSTEM	Yes	Text	No
CMIS Document Home	cmis.docHome		ucr.repositorytype=CMIS	Yes	Text	No

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
CMIS Login Name	cmis.loginName		ucr.repositorytype=CMIS	Yes	Text	No
CMIS Password	cmis.password	example: HpkUIxPWKartDf1W9q/yxw\=\=	ucr.repositorytype=CMIS	Yes	Text	Yes
CMIS Repository Name	cmis.repoName		ucr.repositorytype=CMIS	Yes	Text	No
CMIS Web Service URL	cmis.wsUrl		ucr.repositorytype=CMIS	Yes	Text	No
Host Name	dm.db.host		ucr.repositorytype=DATABASE	Yes	Text	No
Port	dm.db.port		ucr.repositorytype=DATABASE	Yes	Number	No
Instance ID	dm.db.sid		ucr.repositorytype=DATABASE	Yes	Text	No
User Name	dm.db.user.name		ucr.repositorytype=DATABASE	Yes	Text	No
User password	dm.db.user.password	example: IZsUrJruGSk+QbmmKpb4ww\=\=	ucr.repositorytype=DATABASE	Yes	Text	Yes
WebCenter Content User password	wcc.password		ucr.repositorytype=WEBCENTER CONTENT	Yes	Text	Yes
WebCenter Content Root Folder	wcc.rootfolder		ucr.repositorytype=WEBCENTER CONTENT	Yes	Text	No

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
WebCenter Content Server Host	wcc.server.host		ucr.repositorytype=WEBCENTER CONTENT	Yes	Text	No
WebCenter Content Server Port	wcc.server.port		ucr.repositorytype=WEBCENTER CONTENT	Yes	Number	No
WebCenter Content User	wcc.user		ucr.repositorytype=WEBCENTER CONTENT	Yes	Text	No

Database

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
Host Name	database.databaseHost			Yes	Text	No
Instance ID	database.databaseSID			Yes	Text	No
Password	database.password			Yes	Text	Yes
Database Type	database.type	oracle		Yes	Select Text	No
Username	database.username			Yes	Text	No
Max. Connections	database.maxConnections			No	Number	No
Min. Connections	database.minConnections			No	Number	No

Email

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
System Notification E-mail Address	email.from.address			Yes	Email Text	No
Outbound(SMTP) E-mail Server	email.server			Yes	Text	No
E-mail Sender Prefix	email.from.name			Yes	Text	No
Support Contact Information	email.contact.string			No	Text	No
Outbound(SMTP) Authentication Required	email.authentication.required	true, false		Yes	Boolean Text	No
Outbound(SMTP) E-mail Account	email.account		email.authentication.required=true	Yes	Text	No
Outbound(SMTP) E-mail Password	email.password=Ht9JolEet+CRAox706qmJw\=\=		email.authentication.required=true	Yes	Text	Yes
Outbound(SMTP) E-mail Encryption Type	email.server.encryption.type	STARTTLS,SSL/TLS	email.authentication.required=true	No	Select Text	No
System Error Notification E-mail Address	license.notify.to			No	Email Text	No

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
License Notification E-mail Address	email.notify.to			No	Email Text	No
APNs Proxy Server URL	apns.proxy.server			No	Text	No
APNs Proxy Server Port	apns.proxy.port			No	Number	No
Inbound E-mail protocol	action.email.protocol=IMAPS	IMAPS, POP3		No	Text	No
Inbound E-mail Server	action.email.server			No	Text	No
Inbound E-mail Account	action.email.account			No	Text	No
	action.email.account.old			No	Text	No
Inbound E-mail Password	action.email.password			No	Text	Yes
Project Email Pattern	project.email.pattern	suffix, prefix		No	Select Text	No
	project.email.pattern.old			No	Select Text	No

Markup Server

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
Use Server Internal URL	server.internal.url.enabled	true, false		No	Boolean Text	No
Markup Server Host Name	server.jvue.host			No	Text	No
Markup Server Port	server.jvue.port			No	Number	No

Report

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
BIP Endpoint URL	server.report.bip.endpoint			No	Text	No
BIP Password	server.report.bip.password			No	Text	Yes
BIP Username	server.report.bip.username			No	Text	No
OBIEE Analytics URL	server.obi.analytics.url			No	Text	No
BIP Report Folder	server.report.bip.folder			No	Text	No
BIP External Report Folder	server.report.bip.extfolder			No	Text	No
BIP Data Source	server.report.bip.datasource			No	Text	No

Geo Map

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
Map Server Url	map.url			No	Select Text	No
Map Tile	map.tile			No	Select Text	No
Map Geocoder Url	map.geocoder.url			No	Select Text	No

Authentication

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
Login URL	email.login.url			Yes	Text	No
Authorization type	authorization.type	NATIVE, OIM/OAM, Oracle Identity Cloud Service, WEBLOGIC, LDAP SIMPLE BIND, LDAP DOUBLE BIND		Yes	Select Text	No
Logoff redirect url	sso.logout		authorization.type=GENERIC SSO	No	Text	No
SSO Header	sso.header		authorization.type=GENERIC SSO	No	Text	No
SSO Provider	sso.provider	sso, oam, idcs, weblogic	authorization.type=GENERIC SSO	No	Text	No

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
Group(s) (comma separated)	weblogic.groups		authorization.type=WEBLOGIC	Yes	Text	No
Realm	weblogic.realm		authorization.type=WEBLOGIC	Yes	Text	No
Auth Factory	authorization.factory	ldap	authorization.type=LDAP SIMPLE BIND	Yes	Text	No
LDAP server (URL)	ldap.provider.url	Example: ldap://ldap.xyz.com:636	authorization.type=LDAP SIMPLE BIND	Yes	Text	No
LDAP template for single bind	ldap.security.principal.template		authorization.type=LDAP SIMPLE BIND	Yes	Text	No
SSL	ldap.security.protocol	true, false	authorization.type=LDAP SIMPLE BIND	No	Text	No
Administrator's login ids	ldap.user.bypass		authorization.type=LDAP SIMPLE BIND	No	Text	No
Trusted login user's DN	ldap.authorized.user		authorization.type=LDAP SIMPLE BIND	Yes	Text	No
Authorized user's LDAP login password	ldap.authorized.user.password		authorization.type=LDAP SIMPLE BIND	No	Text	Yes

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
Provider base	ldap.provider.base		authorization.type=LDAP SIMPLE BIND	No	Text	No

Advanced

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
Server timezone	server.timezone	See below*		No	Number	No
Number of threads for high priority jobs	job.p1.threadCount	>5		No	Number	No
Support Session Failover	support.session.failover	true, false		No	Boolean Text	No
Proxy Server Port for Oracle Map Server	map.net.proxy.port			No	Number	No
Proxy Server User for Oracle Map Server	map.net.proxy.url			No	Text	No
Proxy Server URL for Oracle Map Server	email.login.url.partner			No	Text	No

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
Include Custom properties	include.custom	true, false		No	Boolean Text	No

Apryse

Name	Key	Values	Dependent Key	Required	Data Type	Encrypted
Webviewer License Key	apryse.webApryseInfo			No	Text	No
Webviewer Server URL	apryse.webviewerServerURL			No	Text	No

***** Values for server.timezone: If not specified, will use Unifier server time zone.

Possible Time Zones

Africa/Djibouti

Africa/Harare

Africa/Lagos

Africa/Maputo

Africa/Mogadishu

Africa/Nairobi

Africa/Nouakchott

America/Buenos_Aires

America/Costa_Rica

America/Denver

America/Edmonton

America/El_Salvador

America/Guayaquil

America/Halifax

America/Indiana/Indianapolis

America/Indianapolis

America/Lima

America/Manaus
America/Mazatlan
America/Mexico_City
America/Montreal
America/New_York
America/Panama
America/Phoenix
America/Puerto_Rico
America/Regina
America/Tijuana
America/Toronto
America/Vancouver
Asia/Aden
Asia/Bahrain
Asia/Dhaka
Asia/Ho_Chi_Minh
Asia/Kamchatka
Asia/Katmandu
Asia/Kolkata
Asia/Kuala_Lumpur
Asia/Kuwait
Asia/Muscat
Asia/Qatar
Asia/Riyadh
Asia/Saigon
Asia/Shanghai
Asia/Singapore
Asia/Taipei
Asia/Tashkent
Atlantic/Azores
Atlantic/Bermuda
Atlantic/Reykjavik
Australia/Hobart

Australia/Lord_Howe
Australia/Sydney
Etc/GMT+0
Etc/GMT+1
Etc/GMT+2
Etc/GMT+3
Etc/GMT+4
Etc/GMT+5
Etc/GMT-10
Etc/GMT-3
Etc/GMT-4
Etc/GMT-5
Etc/GMT-6
Etc/GMT-7
Etc/GMT-8
Etc/UTC
Etc/Zulu
Europe/Amsterdam
Europe/Athens
Europe/Belgrade
Europe/Berlin
Europe/Brussels
Europe/Bucharest
Europe/Budapest
Europe/Copenhagen
Europe/Dublin
Europe/Helsinki
Europe/Istanbul
Europe/Kiev
Europe/Lisbon
Europe/London
Europe/Luxembourg
Europe/Madrid

Europe/Oslo

Europe/Paris

Europe/Prague

Europe/Rome

Europe/Sofia

Europe/Stockholm

Europe/Tirane

Europe/Vienna

Europe/Warsaw

Europe/Zurich

Indian/Chagos

Indian/Cocos

Pacific/Auckland

Pacific/Easter

Pacific/Gambier

Pacific/Honolulu

Pacific/Kwajalein

Pacific/Noumea

Pacific/Pago_Pago

Pacific/Pitcairn

UCT

US/Aleutian

US/Hawaii

UTC

Using Encryption

If you need to encrypt or decrypt a password and you are using JDK 8, you must use a CLI.

Location of encryption tool:

- On Windows: <drive>:\Oracle\<Unifier_Home>\bin\encrypt_password.bat
- On Linux: <Unifier_Home>/bin/encrypt_password.sh

Prerequisite: Make sure that environment variable UNIFIER_HOME is properly defined. For example:

- On Windows: SET UNIFIER_HOME= /scratch/gbuora/Unifier_21.12.7
- On Linux: export UNIFIER_HOME= /scratch/gbuora/Unifier_21.12.7

Encryption applies to the following fields in the **bluedoor.properties** file. If you use the listed features, you must encrypt the corresponding fields.

Field	Description
cmis.password	Content Management Interoperability Services (CMIS) password
database.password	Database schema password
dm.db.user.password	Database manager database user's password
email.password	Outbound (SMTP) email password
ldap.authorized.user.password	Authorized user's Lightweight Directory Access Protocol (LDAP) login password
server.report.bip.password	Oracle Analytics Server Web Services password
wcc.password	WebCenter Content user's password

The following sub topics provide the applicable instructions.

- ***Creating an encryption.properties File*** (on page 52)
- ***Encrypting a Password*** (on page 52)
- ***Decrypting a Password*** (on page 53)
- ***Updating an Existing Environment While Retaining the Original Encryption Seed and Signature*** (on page 54)
- ***Updating an Existing Environment Using a New Encryption Seed and Signature*** (on page 54)
- ***Updating a New Environment and Using Encryption*** (on page 55)

Creating an encryption.properties File

To create an encryption.properties file:

1) If you have an existing file and do not want it overwritten, back it up.
2) Enter: `<Unifier_Home>/bin`
3) Enter: `./encrypt_password.sh createfile`

   The system displays information similar to the following:

```
user@host ~/Unifier_21.12.7/bin$ ./encrypt_password.sh createfile
Encryption properties are saved successfully to
<Unifer_Home>/bin/encrytion.properties
```

   The generated encryption.properties file looks similar to the following:

```
#Encryption Properties
#Tue Jul 08 21:35:39 UTC 2025
unifier.secure.seed=78120818-3d45-4dfb-b43b-61a7b6d99b3c
```

```
unifier.secure.signature=qlozt8hw2faOKm+M2+sVTXvCdeeOPoKq/Qged05LG+8
\=
```

You will use this file to encrypt and decrypt a password.

Encrypting a Password

To encrypt a password:

1) Enter: `cd <Unifier_Home>/bin`
2) Enter: `./encrypt_password.sh encrypt <unencrypted_password>`

   For example: `./encrypt_password.sh encrypt sample_1234_1`

   The system displays information similar to the following:

```
user@host ~/Unifier_21.12.7/bin$ ./encrypt_password.sh encrypt
sample_1234_1
input unencrypted password = sample_1234_1
2025-07-08T21:38:20.674Z main INFO Starting configuration
org.apache.logging.log4j.core.config.properties.PropertiesConfigurat
ion@3336e6b6...
2025-07-08T21:38:20.678Z main INFO Start watching for changes to
/scratch/gbuora/Source/Unifier_21.12.7/apps/ROOT/WEB-INF/classes/log
4j2.properties every 0 seconds
2025-07-08T21:38:20.678Z main INFO Configuration
org.apache.logging.log4j.core.config.properties.PropertiesConfigurat
ion@3336e6b6 started.
2025-07-08T21:38:20.682Z main INFO Stopping configuration
org.apache.logging.log4j.core.config.DefaultConfiguration@477b4cdf..
.
2025-07-08T21:38:20.683Z main INFO Configuration
org.apache.logging.log4j.core.config.DefaultConfiguration@477b4cdf
stopped.
output encrypted password = dE+rrTaURO3xvKqZCVTGNg==
```

Decrypting a Password

To decrypt a password:

1) Enter: `cd <Unifier_Home>/bin`
2) Enter: `./encrypt_password.sh decrypt <encrypted_password>`

   For example: `./encrypt_password.sh decrypt dE+rrTaURO3xvKqZCVTGNg==`

   The system displays information similar to the following:

```
user@host ~/Unifier_21.12.7/bin$ ./encrypt_password.sh  decrypt
dE+rrTaURO3xvKqZCVTGNg==
input encrypted password = dE+rrTaURO3xvKqZCVTGNg==
2025-07-08T21:39:20.698Z main INFO Starting configuration
org.apache.logging.log4j.core.config.properties.PropertiesConfigurat
ion@3336e6b6...
```

```
2025-07-08T21:39:20.703Z main INFO Start watching for changes to
/scratch/gbuora/Source/Unifier_21.12.7/apps/ROOT/WEB-INF/classes/log
4j2.properties every 0 seconds
2025-07-08T21:39:20.703Z main INFO Configuration
org.apache.logging.log4j.core.config.properties.PropertiesConfigurat
ion@3336e6b6 started.
2025-07-08T21:39:20.706Z main INFO Stopping configuration
org.apache.logging.log4j.core.config.DefaultConfiguration@477b4cdf..
.
2025-07-08T21:39:20.707Z main INFO Configuration
org.apache.logging.log4j.core.config.DefaultConfiguration@477b4cdf
stopped.
output decrypted password = sample_1234_1
```

Updating an Existing Environment While Retaining the Original Encryption Seed and Signature

To retain your original encryption information:

1) Back up your **bluedoor.properties**, **skire.properties**, and **datasource.properties** files to a separate location.

   These files are located in:

   - **<Unifier_Home>/configurator/bluedoor.properties**
   - **<Unifier_Home>/apps/ROOT/WEB-INF/classes/skire.properties**
   - **<Unifier_Home>/apps/ROOT/WEB-INF/classes/datasource.properties**

2) To create an **encryption.properties** file, complete the steps outlined under ***Creating an encryption.properties File*** (on page 52).
3) In **<Unifier_Home>/configurator**, open the **bluedoor.properties** file and locate the lines related to:

   - **unifier.secure.seed=sampleX**
   - **unifier.secure.signature=sampleY**

4) Open the **encryption.properties** file, and replace the values for **unifier.secure.seed** and **unifier.secure.signature** with the values from **bluedoor.properties** file (**sampleX** and **sampleY**).
5) Encrypt the password, as described under ***Encrypting a Password*** (on page 52).
6) To verify that the encryption works correctly, decrypt the password, as described under ***Decrypting a Password*** (on page 53).
7) Copy the encrypted password to the applicable field in the **bluedoor.properties** file.
8) Enter: `cd <Unifier_Home>/weblogic`
9) To transform **<Unifier_Home>/configurator/bluedoor.properties** into **<Unifier_Home>/apps/ROOT/WEB-INF/classes/skire.properties** and **datasource.properties**, enter: `./ configure.sh unifier.weblogic`
10) If you are using Enterprise Archive (EAR) deployment, to generate the EAR file, run: `./configure.sh ear.weblogic`
11) Restart your WebLogic Server, and verify that you can connect to the Unifier database.

Updating an Existing Environment Using a New Encryption Seed and Signature

To use new encryption information:

1) Back up your **bluedoor.properties**, **skire.properties**, and **datasource.properties** files to a separate location.

   These files are located in:

   - **<Unifier_Home>/configurator/bluedoor.properties**
   - **<Unifier_Home>/apps/ROOT/WEB-INF/classes/skire.properties**
   - **<Unifier_Home>/apps/ROOT/WEB-INF/classes/datasource.properties**

2) To create an **encryption.properties** file, complete the steps outlined under ***Creating an encryption.properties File*** (on page 52).
3) In **<Unifier_Home>/configurator**, open the **bluedoor.properties** file and locate the lines related to:

   - **unifier.secure.seed=sampleX**
   - **unifier.secure.signature=sampleY**

4) Open the **bluedoor.properties** file, and replace the values for **unifier.secure.seed** and **unifier.secure.signature** with the values from **encryption.properties** file (**sampleX** and **sampleY**).
5) Encrypt the password, as described under ***Encrypting a Password*** (on page 52).
6) To verify that the encryption works correctly, decrypt the password, as described under ***Decrypting a Password*** (on page 53).
7) Copy the encrypted password to the applicable field in the **bluedoor.properties** file.
8) Repeat these steps for all secured fields that you use.

   For more information, see the table under ***Using Encryption*** (on page 51).
9) Enter: `cd <Unifier_Home>/weblogic`
10) To transform **<Unifier_Home>/configurator/bluedoor.properties** into **<Unifier_Home>/apps/ROOT/WEB-INF/classes/skire.properties** and **datasource.properties**, enter: `./ configure.sh unifier.weblogic`
11) If you are using Enterprise Archive (EAR) deployment, to generate the EAR file, run: `./configure.sh ear.weblogic`
12) Restart your WebLogic Server, and verify that you can connect to the Unifier database.

Updating a New Environment and Using Encryption

To use new encryption information with a new environment:

1) Enter: `cd <Unifier_Home>/configurator`
2) To create the required **bluedoor.properties** file, complete the steps outlined under ***Creating the bluedoor.properties File*** (on page 38).
3) To create an **encryption.properties** file, complete the steps outlined under ***Creating an encryption.properties File*** (on page 52).
4) In **<Unifier_Home>/configurator**, open the **bluedoor.properties** file and locate the lines related to:

- **unifier.secure.seed=sampleX**
- **unifier.secure.signature=sampleY**

5) Open the **bluedoor.properties** file, and replace the values for **unifier.secure.seed** and **unifier.secure.signature** with the values from **encryption.properties** file (**sampleX** and **sampleY**).
6) Encrypt the password, as described under ***Encrypting a Password*** (on page 52).
7) To verify that the encryption works correctly, decrypt the password, as described under ***Decrypting a Password*** (on page 53).
8) Copy the encrypted password to the applicable field in the **bluedoor.properties** file.
9) Repeat these steps for all secured fields that you use.

   For more information, see the table under ***Using Encryption*** (on page 51).
10) Enter: `cd <Unifier_Home>/weblogic`
11) To transform **<Unifier_Home>/configurator/bluedoor.properties** into **<Unifier_Home>/apps/ROOT/WEB-INF/classes/skire.properties** and **datasource.properties**, enter: `./ configure.sh unifier.weblogic`
12) If you are using Enterprise Archive (EAR) deployment, to generate the EAR file, run: `./configure.sh ear.weblogic`
13) Restart your WebLogic Server, and verify that you can connect to the Unifier database.

Completing an Update or Upgrade

Complete the following steps to finish an upgrade, whether you are setting up a new environment or updating an existing one.

1) If you have not already done so, ensure that the **bluedoor.properties** file has been copied to **<Unifier_Home>/configurator**.

   Whether you are setting up a new environment or updating an existing one, the completed file must reside in the correct location.
2) If you have modified any of the configuration properties, run: `./configure.sh unifier.weblogic`

   This command deploys Unifier. It transforms **bluedoor.properties** into **<Unifier_Home>/apps/ROOT/WEB-INF/classes/datasource.properties** and **skire.properties**. If the custom.properties file was included in **<Unifier_Home>/configurator**, it is copied to **<Unifier_Home>/apps/ROOT/WEB-INF/classes**.
3) If you are using Enterprise Archive (EAR) deployment, to generate the EAR file, run: `./configure.sh ear.weblogic`
4) To install OutsideIn, run: `./configure.sh install-oui`

Configuring the OHTTP Server (OHS)

After installing OHTTP Server (Oracle HTTP Server), or OHS, configure as follows:

1) Modify the **$ORACLE_INSTANCE/ config/ OHS/ ohs1/httpd.conf** file as follows:
   a. Change the default listen port from 7777 to 80.

> **Note**: Before making the above change, disable or turn-off any other application that is using port 80 (such as IIS or Windows).

b. Add settings after DocumentRoot as follows:

```
DocumentRoot <Unifier_Home>/apps/ROOT
```

c. Add parameters between <Directory ></Directory> so it appears as follows:

```
<Directory "<Unifier_Home>/apps/ROOT">
      Options Includes FollowSymLinks
      AllowOverride None
      Require all granted
      DirectoryIndex index.html
</Directory>
<Directory "<Unifier_Home>/apps/ROOT/WEB-INF">
      Require all denied
</Directory>
```

d.
```
#Support Http method  GET/POST only
RewriteEngine On
RewriteCond %{REQUEST_METHOD} !^(GET|POST)
RewriteRule .* - [F]
```

e.
```
Header set Content-Security-Policy "default-src 'self'; frame-src *;
child-src *; script-src 'self' 'unsafe-inline' 'unsafe-eval'
http://elocation.oracle.com https://elocation.oracle.com
*.oracle.com; style-src 'self' 'unsafe-inline';img-src 'self' data:
http://elocation.oracle.com https://elocation.oracle.com
*.oracle.com"


<Location /bp/sys/dm/jvue/viewer>
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>


<Location /bp/dm/project_documents>
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>


<Location /bp/sys/dm/bp/attachment/viewer>
```

```
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/dm/unpublished_documents/log>
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/studio/share/open_attachments>
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/share/editGCWithoutWorkFlow>
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/share/draftGC/new>
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/share/draftGC/edit>
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/share/commentGC/new>
```

```
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/share/commentGC/edit>
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/share/editGC>
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/share/commentGC/copyFrom>
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/share/draftGC/copyFrom>
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/studio/bp/document/copylineitem>
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>

<Location /bp/studio/bp/document/itemopen>
```

```
Header set Content-Security-Policy "connect-src 'self'
http://localhost:2345 http://localhost:7575 http://localhost:8888
http://localhost:9999 https://localhost:2345 https://localhost:7575
https://localhost:8888 https://localhost:9999"
</Location>
```

Notes:

- <Unifier_Home> is the unifier installation directory.
- The session about Supporting Http method GET/POST only can be (or may be) added at the end of http.conf file.

2) Add the following to the **$ORACLE_INSTANCE/ config/ OHS/ ohs1/mod_wl_ohs.conf** file:

```
<LocationMatch
/(bp|bluedoor|g|pub|m|portal|unifier|viewbp|ws|VueServlet|VueJNLPSer
vlet|jvueDMS|xdespellchecker)($|/)>
      SetHandler weblogic-handler
      WebLogicHost localhost
      WebLogicPort 7001
</LocationMatch>
<LocationMatch /(dojo|gs|studio|unifier_js|webant|x)($|/)>
     ExpiresActive on
     ExpiresDefault "access plus 6 month"
   Header set X-Content-Type-Options "nosniff"
   Header set X-XSS-Protection "1; mode=block"
</LocationMatch>
LoadModule deflate_module "${ORACLE_HOME}/ohs/modules/mod_deflate.so"
<LocationMatch /(bp|bluedoor|g|pub|portal|unifier|viewbp)($|/)>
       SetOutputFilter DEFLATE
</LocationMatch>
DeflateBufferSize 20000
```

Note: Modify the enteries (#2) under <Location /> as necessary:

- WebLogicHost: Weblogic server hostname or IP address.
- For WebLogicPort: Weblogic server port number.
- The "deflate_module" must be loaded before "<LocationMatch /(bp|bluedoor|g|pub|portal|unifier|viewbp)($|/)>".
- If the browser displays the error message, "...js MIME type ('text/plain') is not executable, and strict MIME type checking is enabled," then add "text/javascript js" to this file: <OHS Installation path>/instances/instance1/config/OHS/ohs1/mime.types

3. Modify the **$ORACLE_INSTANCE/ config/ OHS/ ohs1/ssl.conf** file as follows:

For **OHTTP**, or **OHS**, version:

> **Note**: For the full list of system requirements, applications, and application version levels refer to the *Primavera Unifier Tested Configurations* in the Primavera Unifier Documentation Library.

Replace: `SSLProtocol nzos_Version_1_0 nzos_Version_3_0`

With: `SSLProtocol -all +TLSv1.2`

Replace: `SSLCipherSuite`

`SSL_RSA_WITH_RC4_128_MD5,SSL_RSA_WITH_RC4_128_SHA,SSL_RSA_WITH_3DES_EDE_CBC_SH`

A,SSL_RSA_WITH_DES_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_C BC_SHA

With: `SSLCipherSuite HIGH`

> **Note**: Oracle recommends the SSLv3 protocol for OHS 11g version and the TLSv1.2 for OHS 12c version.

4. On Windows: Run `startNodeManager.cmd` and `startComponent.cmd ohs1`

   On Linux: Run `./startNodeManager.sh` and `./startCOmponent.sh ohs1`

> **Note**: If OAM is used to setup Unifier then login into OAMconsole, navigate to resources tab and add 3 resources in it: /jVue/**, /VueServlet/** and /jvueDMS/**. The Protection level should be excluded for the newly created resources. If any other SSO server is used then perform the similar steps in this server.

Installing SSL Certificate (Optional)

Unifier works in Secure or Non-secure mode. Installing a Secure Socket Layer (SSL) certificate is optional.

Data Backup Recommendations

Oracle Primavera recommends that Primavera Unifier data be incorporated into your company backup procedures. Primavera Unifier data is stored in two places:

- Unifier database
- Files Repository

These repositories need to be backed up regularly.

Deploying Unifier

To deploy Unifier into the WebLogic domain, complete the following procedures:

1) ***Creating an EAR File From the Configurator*** (on page 62)
2) Deploy the generated EAR file using any of the following methods:

- ***Deploying Unifier From the Unifier_Home Directory on Windows*** (on page 62)
- ***Deploying Unifier from the WebLogic Administration Console*** (on page 62)

Creating an EAR File From the Configurator

Complete the following steps to create an .EAR file from the configurator:

1) Access the Configurator.
2) In the configurator, select **Create EAR**.
3) By default, the .EAR file is created in the **unifier/weblogic** directory.
4) Save the file as **unifier.ear**.
5) Proceed to deploy unifier.ear in WebLogic using any of the following methods:
   - ***Deploying Unifier From the Unifier_Home Directory on Windows*** (on page 62)
   - ***Deploying Unifier from the WebLogic Administration Console*** (on page 62)

Deploying Unifier From the Unifier_Home Directory on Linux

After creating the .EAR file, deploy Unifier as follows:

1) In the **<unifier_home>\weblogic** directory, create a `setEnv.sh` file by copying the `setenv_sample.sh` file.
2) Edit the `setenv.sh` file as follows:
   - Set the `domain_home` variable to specify the path of the domain home folder that will be used by Unifier.
   - Set the `admin url` variable to specify host name and port number used by the Unifier domain.
   - Set the `java_home` variable to the JDK installed directory.
   - Set the `USER_MEM_ARGS` variable specify the JVM maximum memory setting.
3) Save **setEnv.sh**.
4) Run **startup.sh**.
5) Run **deploy.sh**.
6) When prompted, enter the WebLogic administrator user name and password.

   The Unifier application will be deployed in WebLogic using the variables set in the **setEnv.sh**.

> **Note:** This process may take several minutes.

Deploying Unifier from the WebLogic Administration Console

After creating the .EAR file in the Configurator, deploy the file from the WebLogic Administration Console as follows:

1) In the **Change Center** pane, select **Lock & Edit**.
2) In the **Domain Structure** pane, select **Deployments**.

3) In the **Summary of Deployments** pane, select **Install**.
4) In the **Install Application Assistant** pane:
   a. Specify the path to the unifier.ear file and click **Next**. For example: c:\<unifier_home>\weblogic\unifier.ear.
   b. Select **Install this deployment as an application** and click **Next**.
   c. Accept the defaults and click **Next**.
   d. Review the configuration settings you have chosen and select **Finish** to complete the installation.
5) In the **Settings for unifier** window, select **Save**.
6) In the **Change Center** pane, select **Activate Changes**.
7) In the **Domain Structure** pane, select **Deployments**.
8) In the **Summary of Deployments** pane:
   a. Select **unifier**.
   b. Select the down arrow to the right of the **Start** button and select **Servicing all requests**.
9) In the **Start Application Assistant** pane, select **Yes**.

> **Note:** The **unifier state** column should be **Active**. If the state is **Start Running**, refresh the screen until the status is changed to **Active**.

Deploying Unifier to a WebLogic Cluster on Linux

There are two types of clustering environments:

1) Individually deployed WebLogic server that points to the same Unifier DB.

2) WebLogic cluster of multiple managed servers, deployed with a single EAR file.

For both clustering environments, files must be placed on a shared drive that is accessible by other server machines that are operating in a clustering environment.

In addition, for the WebLogic cluster, the directory path must be the same for all WebLogic cluster servers because the same EAR file (and configuration setup) is used by all WebLogic cluster servers.

To setup a WebLogic cluster, refer to the WebLogic documentation for detailed instructions. After setting up the cluster, generate the EAR file and deploy Unifier using the EAR file as described in this guide.

Launching Unifier

This section describes how to:

- Start Unifier for the first time
- Install Unifier applications
- Set up your company

Before launching Primavera Unifier, ensure that you have read the Getting Started section of the Unifier Help, which contains important information about configuring your browser for use with Primavera Unifier.

Unifier URL (WebLogic)

In your browser, navigate to the URL that launches the Unifier application locally. For example: `http://unifier.oracle.com:7001`

Starting Unifier for the First Time

In the Sign In window, sign in to Unifier with the default Administrator username (*Administrator*) and password (*Administrator*).

Unifier immediately prompts you to change your password. We recommend you do so immediately for security reasons. Once you change your password, Unifier creates your Administrator account.

The Administrator account is the only account with permissions automatically set for all features. The Administrator cannot be a member of any project, even if created in the Hosting Company.

Deploying Unifier Online Help

By default Unifier online help is deployed from site hosted by Oracle. To deploy Unifier help locally, or from an alternative URL, proceed as follows:

1) Go to the Oracle Primavera Primavera Unifier Documentation Library, on the bookmark pane, click **Using**, click **Downloadable Unifier Help**.
2) The content of Unifier help (**help.zip**), when extracted, has a .war file. Deploy the .war file to an app server and then configure the **Unifier Help URL** field in the **General** tab of the **Configurator** to point to that server.

Downloading and Installing Unifier Base Configuration

Unifier provides preconfigured designs (Configuration Packages) for both **Project Controls** and **Facilities and Asset Management**. These configuration packages include the business processes, attribute forms, reports, setups, templates, and other related files. These are intended as a starting point for your configuration. The three packages are:

- Project Controls and Facilities & Asset Management (Combined Package)
- Project Controls
- Facilities & Asset Management

These packages are typically installed when an environment is provisioned as there is a potential for naming conflicts if a package is added in the future.

> **Note**: Oracle recommends that you install the combined package in your Development environment even if you have purchase license for one base product. This is to prevent any naming conflicts that may occur between your pre-build configuration and new configuration should you decide to purchase another base product. The only disadvantage to installing the combined package is having additional pre-built business processes in your Development environment which will not be published to Production without you electing to do so.

If your licensing agreement includes **Primavera Unifier Project Controls** and/or **Unifier Facilities and Asset Management** base products (applications/products), the Site Administrator can download and install the base configuration by following the instructions below.

> **Note**: Ensure that the **Primavera Unifier** (platform) has been installed before you proceed to download and install the base products (see ***Downloading and Extracting Unifier*** for details).

You will find the configuration packages in **My Oracle Support**:

1) Go to http://support.oracle.com and sign in.
2) Select the **Patches & Updates** tab.
3) In the **Patch Search** block select the **Product or Family (Advanced)** tab, on the left hand side.
4) In the **Product** field enter **Primavera Unifier** .
5) From the **Release** field select the relevant configuration package (Primavera Unifier Configuration Packages x.x) and click **Search**. If the configuration package require a minimum version of Unifier, then it will appear under a general release number, for example, 18.x, 19.x.
6) Under the list that the system returns, select the appropriate configuration package, based on your current version of Unifier.
7) Once you have downloaded the configuration package, you can proceed with importing it to Unifier. Refer to the Unifier Administration Guide for more details on how to import the configuration package.

Recommended Setup after Downloading Base Products

Based on your licensing agreement, you can setup/configure the following three Unifier environments:

> **Note**: The licensing is impacted by the numbers of users.

1) Development
2) Test
3) Production

Unifier (Platform) version will be loaded by default in all the environments.

After the download is complete, the Site Administrator can install the **Primavera Unifier Project Controls** and/or **Primavera Unifier Facilities and Asset Management** base configuration in **Development** and **Test** environments based on your licensing agreement.

> **Note**: In this type of installation, the new designs created in the Development environment are unpublished until the creation of Production configuration package. Unpublished configuration package can be imported to the Test environment for testing. After a Production configuration package is created, all designs that are included in the configuration package will be published.

The following explains the recommended setup (which downloaded folders must be placed in which environment):

Primavera Unifier Project Controls

- Development
  - The main Unifier application files ("unifier_#.zip" (where # represent the Unifier version number) folder)
  - The files in the main zip folder from Primavera Unifier **Project Controls** download
  - Sign in to Unifier to import it. Refer to the Unifier Administration Guide for details on how to import the Configuration Package.
- Test
  - Generate the configuration package and then import the package to the Test environment
- Production
  - The **Project Controls** base product can be transferred from the Development environment by using a published configuration package

Primavera Unifier Facilities and Asset Management

- Development
  - The main Unifier application files ("unifier_#.zip" (where # represent the Unifier version number) folder)
  - The files in the main zip folder from Primavera Unifier **Facilities and Asset Management** download
  - Sign in to Unifier to import it. Refer to the Unifier Administration Guide for details on how to import the Configuration Package.
- Test
  - Generate the configuration package and then import the package to the Test environment
- Production
  - The **Facilities and Asset Management** base product can be transferred from the Development environment by using a published configuration package

> **Note**: Since the content of the material created by the Users (also known as Custom Strings) can be translated into different languages, with the

exception of data or value entered by the user, you (Unifier Administrator) must sign in to **Unifier**, navigate to the **Company**, expand the **Configuration** node, select the **Internationalization** node, click the **Refresh** drop-down list, and select **All Strings** to populate the **Custom String** table. If you do not refresh after the installation, certain Unifier functions will not work properly.

Installing the Base Products

The following explains how to install the base products after downloading the files:

When you sign in as the Site Administrator, Unifier displays the **Companies** log.

- For **single tenant** and **multi tenant** environments, Unifier displays the **Create** option in the **Companies** log.
- For **single tenant** environment, if the company has already been created, then Unifier disables the **Create** option in the **Companies** log.

Click **Create** and enter the required values as explained in the following table.

When finished, click **Create** at the bottom of the window.

Unifier:

- Creates the company.
- Installs the basic configuration installation file.

Note: You can only create one company in a **single tenant** environment.

The user is required to import the Configuration Packages to the destination environments after the installation of Project Controls and Facilities and Asset Management is completed.

Company Details

In this field:	Do this:
Name	Enter the name of the company.
Short Name	Enter a one-word short name, up to 60 characters. The Short Name is a unique, one-word abbreviated form of your company name, and is used throughout Primavera Unifier in place of the company name. (For example, when importing uDesigner-created business processes, and on logs that identify partner companies.)
Currency	Enter the default currency that will be used by the company.
Contact Email	Enter the email address that will be used for all emails sent from the Support link in Unifier.
Licensed Users	Enter the number of users who will be licensed to use the application.

Address Type	Identify the address you are entering, such as Headquarters, Billing Office, or Satellite Office.
Address	Enter the company address.
City	Enter the city for the address.
State/Province	Enter the state or province for the address.
Zip	Enter the zip code for the address.
Country/Region	Enter the country or region for the address.
Admin Login Username	Enter the company administrator's user name. Default is coadmin. This user name will be automatically added to the Company Administrators group. The `coadmin` user, by default, gets all the permissions for the new designs or new modules. Essentially this user that is company administrator will have all the permissions across the company and projects.
Password	Enter the administrator's password.
Confirm Password	Re-enter the password.

Company Administrator

In this field:	Do this:
Admin Login Username	Enter the company administrator's user name. Default is coadmin. This user name will be automatically added to the Company Administrators group. The `coadmin` user, by default, gets all the permissions for the new designs or new modules. Essentially this user that is company administrator will have all the permissions across the company and projects.
Password	Enter the administrator's password.
Confirm Password	Re-enter the password.

Downloading the Unifier Mobile App

Downloading Unifier Mobile App for iOS

Go to App Store on your mobile device and download the Unifier Mobile App iOS.

Configuring Login and Authentication Settings to Use Unifier Mobile App iOS

To start the app:

1) Find the Unifier app on your device () and tap to launch the app.
2) Slide the **Single Sign On** (SSO) switch to either **ON** or **OFF** position.

If you turn **ON** the SSO switch:

1) Tap the URL field and enter the URL to your server (for example, `http://server:port/`).

> **Note**: You will need to specify the server name and port number in the URL.

2) Tap **Authenticate**.
3) Enter your SSO username and password.

If you turn **OFF** the SSO switch:

1) Tap the URL field and enter the URL to your server (for example, `http://server:port/`).
2) Enter your Unifier username and password.
3) Tap **Sign In**.

Disabling Unifier Mobile App Auto-Login

The Unifier Mobile App Auto-login is enabled by default. If you wish to disable the Unifier Mobile App auto-login, then open the "`skire.properties`" file, change the numeric value for the property name "`skire.access.token.timeout.day`" and redeploy the file. The property indicates the validity of access token in terms of days used for auto-login by mobile app.

That is to state, when an access token is generated after user login (with credentials), the Unifier Mobile App will be able to renew the session by using the generated access token for the next "N" number of days indicated in the property value (the numeric value for the property name).

If you do not set a value for the property, then the default property validity value will be set to 14 (fourteen) days. To opt out of this feature, proceed to set this property value to 0 (zero).

Appendix A: Installing a Service Pack (WebLogic)

To obtain the applicable service pack, go to Oracle Support. Use the Readme associated with the service pack for instructions about how to apply the service pack.

Appendix B: Archiving Projects

Archiving allows Site Administrator to archive individual projects.

Configuring Primavera Unifier for Project Archiving

Set up the archive parameters (Archive Directory and Archive Temp Directory). Refer to "Repository Tab."

Archiving Projects

The archiving process captures project data and creates *.csv* files for all records, including business processes, tasks, documents, attachments, users, groups.

> **Note**: In order to archive projects, you must have "Archive" permission as a Hosting Company user. (This permission is found under Projects (Standard) in Access Control or the Permissions tab of the Edit User/Group window; company must be Hosting Company.)

To archive projects:

1) Sign in to Primavera Unifier as Site Administrator.
2) In Administration Mode, navigate to **System, Customer Support, Projects**. The Project log opens.
3) Select the project to archive. If a project has not yet been archived, the **Archive Status** column will display *Not Started*.
4) Click the **Archive Project** button. The Archive Status column will change to **Scheduled**. A background process picks up the request and runs the archive process. Once it is done, the status will change to **Ready**. The location of the zip file that contains the data will be located in the directory you specified during configuration.

Appendix C: WebLogic Clustering for High Availability

About WebLogic Clustering

WebLogic Server clusters provide scalability and reliability for your applications by distributing the work load among multiple instances of WebLogic Server. Incoming requests can be routed to a WebLogic Server instance in the cluster based on the volume of work being processed. In case of hardware or other failures, session state is available to other cluster nodes that can resume the work of the failed node.

A WebLogic server cluster consists of multiple WebLogic server instances running simultaneously to provide increased scalability and reliability. A cluster appears to clients to be a single WebLogic server instance. The server instances that constitute a cluster can run on the same machine, or be located on different machines. You can increase a cluster's capacity by adding additional server instances to the cluster on an existing machine, or you can add machines to the cluster to host the incremental server instances.

> **Note**: Each server instance in a cluster must run the same version of WebLogic.

Relationship between Clusters and Domains

A domain is an interrelated set of WebLogic server resources that are managed as a unit. A domain includes one or more WebLogic server instances, which can be clustered, non-clustered, or a combination of clustered and non-clustered instances. A domain can include multiple clusters. A domain also contains the application components deployed in the domain, and the resources and services required by those application components and the server instances in the domain. Examples of the resources and services used by applications and server instances include machine definitions, optional network channels, connectors, and startup classes.

In each domain, one WebLogic server instance acts as the Administration Server—the server instance that configures, manages, and monitors all other server instances and resources in the domain. Each domain contains one Administration Server only. If a domain contains multiple clusters, each cluster in the domain has the same Administration Server. All server instances in a cluster must reside in the same domain; you cannot split a cluster over multiple domains. Similarly, you cannot share a configured resource or subsystem between domains.

Clustered WebLogic server instances behave similarly to non-clustered instances, except that they provide failover and load balancing. The process and tools used to configure clustered WebLogic server instances are the same as those used to configure non-clustered instances. However, to achieve the load balancing and failover benefits that clustering enables, you must adhere to certain guidelines for cluster configuration.

High Availability with WebLogic Clustering

Unifier can utilize WebLogic clustering to continue processing data when a server instance fails. You cluster Unifier by deploying it on multiple server instances in the cluster. If a server instance on which Unifier is running fails, then another running server instance on which Unifier is deployed can continue to process data.

For a more comprehensive product overview, documentation, and community forums for WebLogic and its clustering functionality, refer to:
http://www.oracle.com/technetwork/middleware/weblogic/overview/index.html

Introduction to High Availability

High availability allows application processing to continue when a server instance fails and provides a reliable environment with minimal or no loss of service. High Availability is often achieved through the use of clusters, units of servers running concurrently to provide application failover and load balancing. Enterprise application deployments can benefit from the additional reliance and flexibility high availability systems provide.

Reasons for Implementing High Availability

Mission critical computer systems need to be available 24 hours a day, 7 days a week, and 365 days a year. However, part or all of the system may be inoperable during planned or unplanned downtime. A system's availability is measured by the amount of time that it provides service over the total time elapsed since the system's initial deployment.

System downtime may be categorized as planned or unplanned. Planned downtime refers to scheduled operations that render the system unavailable. The effect of planned downtime on end users is typically minimized by scheduling downtime when system traffic is slow. Unplanned downtime is any sort of unexpected failure. Unplanned downtime may have a greater effect than planned downtime because it can happen at peak hours, disrupt business operations, or lead to lost productivity or revenue.

When designing your Unifier implementation, it is important to recognize the cost of downtime to understand how your services can benefit from availability improvements.

High Availability Options for Unifier

WebLogic Clustering enables you to provide high availability for Unifier applications, ensuring your services remain scalable and resilient against unexpected failures.

Prerequisites for WebLogic Clustering

This guide assumes that you have already installed and configured Unifier.

> **Note**: The installation wizard deploys Unifier to a single managed server assigned to a cluster within a WebLogic domain.

In addition to the prerequisites to enable WebLogic clustering on your initial Unifier deployment, which are described in either Installation Prerequisites of the Installation and Configuration Guide or Prerequisites in Manual Deployment Guide, you will need to install a supported version of Oracle HTTP Server. For a supported version of Oracle HTTP Server, refer to Tested Configurations.

Deploying Unifier with WebLogic clustering requires you to install WebLogic on each machine that will use the Unifier domain, which was created by the Unifier configuration wizard.

> **Note**: You must install the same version of WebLogic on each machine.

Setting Up WebLogic Clustering for Unifier Applications

After you have installed and configured Unifier, you can add new machines, servers, and clusters using the WebLogic Administration Console. You must then add any new servers to different machines and create a cluster to utilize high availability for your application deployments. After creating a cluster, you must add servers to the cluster. To add new servers to your clusters and establish high availability for your Unifier applications, complete the following topics in the order that they are listed:

- Adding New Machines in WebLogic
- Adding New Servers in WebLogic
- Adding New Clusters in WebLogic
- Assigning Servers to Clusters
- Associating Servers with Machines
- Copying the Unifier Domain to Additional Machines
- Running Node Manager as a Service
- Starting Node Managers and Managed Servers on Additional Machines

After the servers have been added to your cluster, deploy the Unifier WebLogic domain to new machines by creating a zip file of the domain, extracting its contents to the domains folder in Oracle Middleware Home, and then updating nodemanager.properties with the correct ListenAddress hostname. For the procedures to deploy the Unifier domain to new machines, refer to Copying the Unifier Domain to Additional Machines.

When deploying Unifier to managed servers in a cluster running across different physical machines to the domain's administration server, you must modify the Web Service Manager (WSM) Policy Manager on the remote machines so that the additional managed servers can use the WSM Policy Framework. To modify the WSM Policy Manager, refer to Modifying the WSM Policy Manager.

Lastly, configure the WebLogic proxy plugin driver (mod_wl_ohs) of an Oracle HTTP Server (OHS) instance to connect to the Unifier WebLogic cluster using the instructions in Configuring the WebLogic Proxy Plugin Driver of an Oracle HTTP Server and then start your node managers and managed servers using the instructions in Starting the Node Managers and Managed Servers on Additional Machines.

Adding New Machines in WebLogic

To add new machines in WebLogic:

1) Log in to the WebLogic Administration Console with the following URL:
   `http://<host_name>:<port>/console`
2) In the Change Center pane, click Lock & Edit.
3) In the Domain Structure pane, click Environment and then click **Machines**.
4) Click New.
5) On the Create a New Machine page, complete the following:

a. In the Name field, enter a logical name for the machine (for example, Machine 1).
b. In the Machine OS list, select Unix if the machine uses a Unix operating system or select Other if the machine uses a non-Unix operating system, such as Windows.
c. Click Next.

6) On the Create a New Machine page, complete the following:
   a. In the Type list, select the protocol with which the node manager on the machine communicates with its servers. The protocol options are SSL (default option), Plain, RSH, and SSH.
   b. In the Listen Address field, enter the hostname or IP Address of the remote server.
   c. In the Port field, enter the port number for the remote server on which the node manager will run.
   d. Click Finish.
7) Click Activate Changes.

Adding New Servers in WebLogic

To add new servers in WebLogic:

1) Log in to the WebLogic Administration Console with the following URL:
   `http://<host_name>:<port>/console`
2) In the Change Center pane, click Lock & Edit.
3) In the Domain Structure pane, click Environment and then click **Servers**.
4) Click New.
5) On the Create a New Server page, complete the following:
   a. In the Server Name field, enter a name for the managed server.
   b. In the Server Listen Address field, enter the hostname or IP Address of the remote server.
   c. Note: If you plan to add a new managed server on the same physical server as the Administration server, you can leave this field blank. This allows all local listening addresses on the server to be utilized.
   d. In the Server Listen Port field, enter the port number from which you want to access the server instance.
   e. You can more easily manage and maintain the servers in your cluster by using the same port number across all of your managed servers.
   f. Select Yes, make this server a member of an existing cluster.
   g. Select a cluster.
   h. Click Finish.
6) Click Activate Changes.

Adding New Clusters in WebLogic

Adding New Clusters in WebLogic

To add new clusters in WebLogic:

1) Log in to the WebLogic Administration Console with the following URL:
   `http://<host_name>:<port>/console`

2) In the Change Center pane, click Lock & Edit.
3) In the Domain Structure Pane, click Environment, then click Clusters.
4) Click New, then select Cluster.
5) On the Create a New Cluster page, complete the following:
   a. Enter a name for the cluster in the Name field.
   b. Select a messaging mode for the cluster, Unicast or Multicast.
   c. If you selected Unicast, enter a Unicast Broadcast Channel.
   d. If you selected Multicast, enter a Multicast Address and a Multicast Port number.
6) Click Ok.
7) Click Activate Changes.
8) To learn more about WebLogic clusters, cluster configuration, and application deployment, refer to the official WebLogic documentation:
   `http://docs.oracle.com/middleware/12211/wls/CLUST/toc.htm`

Assigning Servers to Clusters

To assign servers to clusters in WebLogic:

1) Log in to the WebLogic Administration Console with the following URL:
   `http://<host_name>:<port>/console`
2) In the Change Center pane, click Lock & Edit.
3) In the Domain Structure Pane, click Environment, then click Clusters.
4) Click the name of the cluster you want to which you want to assign servers.
5) On the Settings for <Cluster_Name> page, click the Servers tab.
6) On the Servers tab, in the Servers table, click Add.
7) Select Select an existing server, and add it as a member of this cluster, to add a preexisting server to the cluster.
8) Select a server in the Select a server list.
9) Click Next.
10) Click Activate Changes.

Associating Servers with Machines

To associate a server with a machine:

1) Log in to the WebLogic Administration Console with the following URL:
   `http://<host_name>:<port>/console`
2) In the Change Center pane, click Lock & Edit.
3) In the Domain Structure pane, click Environment and then click Machines.
4) Click the name of the machine to which you want to add a server.
5) Under the Configuration tab, click Servers.
6) Click Add.
7) On the Add Server to Machine page, complete the following:
   a. Select Select an existing server, and associate it with this machine.

b. In the Select a Server list, select the name of the server that you want to add to the machine.
c. Click Finish.

8) Click Activate Changes.

Copying the Unifier Domain to Additional Machines

After you have added new managed servers to your Unifier cluster and modified the WSM Policy Manager, create a zip file of your initial Unifier domain. After the zip file is created, extract the WebLogic domain and components on the remote machines which contain additional managed servers. After you have successfully extracted the WebLogic domain to additional machines, modify the nodemanager.properties file with information about the hostname on which the administration server runs.

To add the Unifier domain to additional machines:

1) Navigate to the Oracle Middleware Home of the machine on which you created the initial Unifier domain.
2) Create a zip file of the user projects folder of the Unifier domain.
3) Copy the zip file to the machines on which you have created additional servers.
4) Extract the zip file to the Oracle Middleware Home folder on the additional machines.

   Note: When copying the domain, ensure that the directory structure of each additional WebLogic instance is similar to the directory structure of the WebLogic instance where you initially installed the Unifier domain.
5) Navigate to `<Oracle_Middleware_Home>/user_projects/domains/primavera/nodemanager`.
6) Edit `nodemanager.properties`.
7) Modify the `ListenAddress` hostname and `ListenPort` number to match the hostname and port number of your current machine and then save your changes.

Running Node Manager as a Service

To run the node manager as a background process upon system startup, you can run the node manager as a service on Windows or you can configure the node manager as a daemon on Unix.

For *Unix*

To start the node manager upon system startup and to run it in the background:

1) Open a terminal and run the following script: `nohup <Oracle_Middleware_Home>/user_projects/domains/<Primavera_Domain>/bin/startNodeManager.sh > logfilename.log 2>&1 &`
2) Create a shell script using the following sample script:

```
#! /bin/bash
#
# wlsnmd Oracle Weblogic NodeManager service
#
# chkconfig:   345 85 15
```

```
# description: Oracle Weblogic NodeManager service
case "$1" in
   start)
        export WL_HOME=<Oracle_Middleware_Home>/wlserver/

   $WL_HOME/../user_projects/domains/<Primavera_Domain>/bin/startNod
eManager.sh
        ;;
   *)
        echo "Usage: $0 {start}"
        exit 1
esac
exit_status
```

3) Save the script to /etc/init.d/nodemgr.
4) Run the following command with root privileges:

```
# chmod +x /etc/init.d/nodemgr
# chkconfig --add nodemgr
```

For *Windows*

To create and run a node manager as a Windows service:

1) Log in to a machine with administrative privileges.
2) Go to: `<Oracle_Middleware_Home>/wlserver/server/bin.`
   a. Edit `installNodeMgrSvc.cmd`.
   b. Comment out the following lines:
      `set NODEMGR_HOST=<host>`
      `set NODEMGR_PORT=<port>`
   c. Save your changes and then close the file.
3) Go to: `<Oracle_Middleware_Home>/user_projects/domains/<Primavera_Domain>/bi`n.
   a. Edit installNodeMgrSvc.cmd.
   b. Comment out the following lines:
      `set NODEMGR_HOST=<host>`
      `set NODEMGR_PORT=<port>`
   c. Save your changes and then close the file.
4) Open a command prompt and then complete the following:
   a. Change your directory to `<Oracle_Middleware_Home>/user_projects/domains/<Primavera_Domain>/bin`.
   b. Run `installNodeMgrSvc.cmd`.

Note: If the node manager service has already been installed, the following message will display: CreateService failed - The specified service already exists.

c. Close the command prompt.

5) Go to Control Panel\All Control Panel Items\Administrative Tools and then click Services.
6) Right-click Oracle WebLogic <primavera_domain> NodeManager and then click Start.

Starting Node Managers and Managed Servers on Additional Machines

After the Unifier domain has been modified on machines on which they reside, you must start the node manager on each machine to control the managed servers from the WebLogic Administration Console.

To start a managed server:

1) Log in to the Domain's Administration Console.
2) In the left pane of the Administration Console, expand Environment and select Servers.
3) In the right pane, select the Control tab.
4) In the Server Status table, select the check box next to the name of the server you want to start and click Start.
5) Click Yes to confirm.

To start the node manager:

1) Go to `<Oracle_Middleware_Home>/user_projects/domains/<Primavera_Domain>/bin`.
2) Depending on your operating system, complete the following:

   For *Windows*, run:

   ```
   startManagedWeblogic.bat <server_name>
   t3://<administration_server_name>:<port>
   ```

   For *Unix*, run:

   ```
   ./startNodeManager.sh
   ```

Copyright

Oracle Primavera Unifier Installation Guide for On-Premises