Oracle® Communications Convergence

Installation and Configuration Guide

Release 3.0.3

F99827-01

August 2024

Oracle Communications Convergence Installation and Configuration Guide, Release 3.0.3

F99827-01

Contents

Preface

This guide explains how to install Oracle Communications Convergence and configure its components.

Audience

This document is intended for Convergence installers and system and network administrators. This guide assumes that you have a working knowledge of the following concepts:

- Oracle Communications software products used to deliver Convergence services
- Oracle WebLogic Server
- Directory server management
- Structure and use of a lightweight directory access protocol (LDAP)
- System administration and networking
- General deployment architecture

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

1

Convergence Installation Overview

This chapter provides an overview of the Oracle Communications Convergence installation process.

Overview of Convergence Installed Components

During the installation process, you install and configure the following components:

- Java
- Oracle WebLogic server
- Other Oracle Unified Communications products, such as:
  - Oracle Communications Messaging Server
  - Oracle Communications Calendar Server
  - Oracle Communications Contacts Server
- Convergence

Overview of the Convergence Installation Procedure

The installation procedure follows these steps:

1. Plan your installation, including:
   - Determine the scale of your implementation. For example, is it a small development system, a test system, or a large production system.
   - Determine how many physical systems you need and which software components to install on each system.
   - Plan the system topology. For example, determine how the system components connect to each other over the network.
2. Review and gather the system and information requirements. See "Convergence System Requirements " for more information.
3. Install and configure the software on which Convergence depends, including:
   - Oracle WebLogic Server
   - Java
   - Oracle Unified Directory
4. Install and configure the Oracle Communications software required to deliver your planned services, such as one or more of the following:
   - Messaging Server: used by Convergence to provide mail and SMS services.
   - Calendar Server: used by Convergence to provide calendar services.
   - Contacts Server: used by Convergence to provide address book services. Convergence can also provide its own address book services.

5. Install and configure Convergence.
6. Perform post-installation and configuration tasks.
7. Verify the installation.

Convergence Installation Options

You install Convergence by running an installer in either interactive or silent mode. Silent mode is a non-interactive installation. You launch the installer by running the **commpkg install** command.

You can use silent mode to install multiple instances of the same software component and configuration without having to manually run an interactive installation for each instance.

The silent installer requires a state file to run. You must use the interactive installer to create a state file before you can run the installer in silent mode. The installer automatically creates a state file after each complete installation.

Ensuring a Successful Convergence Installation

Only qualified personnel should install Convergence. You must be familiar with the UNIX operating system and Oracle WebLogic server. You should be experienced with installing Java-related packages. Oracle recommends that only an experienced database administrator install and configure database software.

Follow these guidelines:

- As you install each component (for example, Oracle WebLogic server), verify that the component installed successfully before continuing the installation process.
- Pay close attention to the system requirements. Before you begin installing the software, make sure your system has the required base software. In addition, ensure that you know all of the required configuration values, such as host names and port numbers.
- As you create new configuration values, write them down. In some cases, you might need to reenter configuration values later.

Directory Placeholders Used in This Guide

Table 1-1 lists the directory placeholders used in this guide.

Table 1-1 Convergence Directory Placeholders

Placeholder	Description
Convergence_Home	Specifies the installation location for the Convergence software. The default is **/opt/sun/comms/iwc**.
UCS_Home	Specifies the installation location for the Unified Communications Suite software. The default is **/opt/sun/comms/**.
WebLogic_Home	Specifies the installation location for Oracle WebLogic Server. For example, WLS_HOME.

Table 1-1   (Cont.) Convergence Directory Placeholders

Placeholder	Description
Convergence_Domain	Specifies the application server directory containing the configuration files for the domain in which Convergence is deployed. *Convergence_Domain* is created in *WLS_HOME***/***Oracle_Home***/***user_projects***/domains**. *Convergence_Domain* for Oracle WebLogic Server Deployment is: • *WLS_HOME***/***Oracle_Home***/***user_projects***/domains/base_domain**

2 Planning Your Convergence Installation

This chapter provides information about planning your Oracle Communications Convergence installation.

Planning Considerations

Planning your Convergence installation involves:

- Planning your system deployment. See the discussion about the Convergence deployment architecture in *Convergence System Administrator's Guide* for more information.
- Determining the services you plan to deliver in Convergence.

  For each service, review the planning guidelines for the corresponding application. For example, if you plan to deploy Convergence with the mail, calendar, and address book services, review the planning guidelines for Oracle Communications Messaging Server, Oracle Communications Calendar Server, and Oracle Communications Contacts Server.
- Determining the scale of your implementation. To determine the scale, consider the number of users you intend to serve and the number of services you intend to deliver.
- Designing your network around the services you plan to deliver.

Some Convergence features are limited by third-party applications. Consider the following limitations when planning your Convergence installation, and determine how to inform your users.

- HTML5 support:

  Some Convergence features are delivered over HTML5. Most browsers support HTML5 by default, but some browsers need to be configured to support HTML5.
- Tablet support:

  Convergence can be accessed on an Apple iPad (Safari browser) or a Samsung Galaxy Tab (Chrome browser). When Convergence is accessed from a supported tablet, the following subset of Convergence services is available: messaging, calendar, and address book.

Deployment Recommendations

Oracle recommends that you place the Messaging Server Webmail Server on the same host as Convergence, which allows easy horizontal scalability and easy service growth. Other components such as the message store and message transfer agent (MTA), Calendar Server can be located on other hosts.

Default Paths and File Names

Table 2-1 lists the directories that are created when you install Convergence. The same directories are created for the Solaris and Linux operating systems.

Table 2-1   Platform Convergence Directories

Directory Type	Directory Path and Name
Installation directory	**/opt/sun/comms/iwc**
Data directory	**/var/opt/sun/comms/iwc**
Binary directory	**/opt/sun/comms/iwc/sbin**

3

Convergence System Requirements

This chapter describes the hardware, operating system, software, and server requirements for Oracle Communications Convergence.

System Requirements

This section explains the system requirements for Convergence.

Supported Operating Systems

Table 3-1 lists server-side operating systems that support Convergence.

Table 3-1 Supported Server-Side Operating Systems

Product	Version
Oracle Solaris on SPARC	11
Oracle Solaris on x64	11
Oracle Linux on x64 (64-bit)	8

Software Requirements

Table 3-2 lists the various software requirements for Convergence.

Table 3-2 Convergence Software Requirements

Software	Version	Required or Optional
Directory Server	Oracle Unified Directory 12.2.1.4.0	Required, server-side
Directory Server Schema	6.4.0.30 or later	Required, on directory server
Application Server	Oracle WebLogic Server 12.2.1.4	Required, server-side
Java Runtime Environment (JRE)	Latest certified JDK version - JDK8u411	Required, server-side and client-side
Desktop web browser	Google Chrome 121.0.6167.161 Mozilla Firefox 67 Mozilla Firefox ESR 52 (for SMIME) Microsoft Internet Explorer 11 Microsoft Edge 40 Apple Safari 11.0.2	Required, client-side For more information, see the note below this table.
Tablet web browser	Apple iPad: Safari Android: Google Chrome	Required, client-side See note below table.
Oracle Communications Messaging Server	8.1.x	Required, server-side

Table 3-2 (Cont.) Convergence Software Requirements

Software	Version	Required or Optional
Oracle Communications Calendar Server	8.0.x	Required, server-side
Oracle Communications Contacts Server	8.0.x	Optional, server-side
Oracle Access Manager	12.2.1.4	Optional, server-side
Oracle Outside In Transformation Server	8.5.1	Optional, server-side

> **Note:**
>
> - Some web browsers are updated frequently. Later versions than those listed above should work with Convergence.
> - Some Convergence features and services behave or work differently depending on the browser being used. See "Planning Considerations" for more information. Also, see *Convergence Release Notes* for information about known issues.
> - Convergence is supported on the latest patch updates of the Unified Communication Suite (UCS) component versions mentioned in the Table 3-2.

Hardware Requirements

Table 3-3 lists the minimum hardware requirements for the machine onto which you install Convergence.

Table 3-3 Convergence Minimum Hardware Requirements

Component	Requirement
Disk Space	Minimum 100 MB
RAM	Minimum 1 GB

Information Requirements

During Convergence installation, you must enter values for configuration items such as host names and port numbers. The following tables describe the information that you must provide during the installation process:

- Table 3-4 Convergence Information
- Table 3-5 Oracle WebLogic Server Information
- Table 3-6 Directory Server Information
- Table 3-7 Software Information

Table 3-4 lists the Convergence information that you provide during the initial configuration.

Table 3-4   Convergence Information

Information Type	Description
Convergence Configuration Directory	The directory in which Convergence configuration and data files are saved during initial configuration. Default: **/var/opt/sun/comms/iwc**
Convergence server host name	Host name of the system where the Convergence software is installed.
DNS domain name	The DNS domain for the host system where Convergence is installed.
Convergence administrator user name and password	The Convergence administrator user name and password.

Table 3-5 lists Oracle WebLogic Server information that you provide during initial configuration.

Table 3-5   Oracle WebLogic Server Information

Information Type	Description
Oracle WebLogic Server installation directory	Directory in which Webogic Server is installed. Default is: **WLS_HOME/Oracle_Home**
Oracle WebLogic Server domain directory	The directory in which domain directories are created. Default is: **WLS_HOME/Oracle_Home/ user_projects/domains/ base_domain**
Oracle WebLogic Server document root directory	The Webogic Server document root directory. For Convergence configuration, the default is **/var/opt/sun/comms/iwc/web-src/client**
Oracle Webogic Server target instance name	The name of the server target name. Default: server
Webogic Server virtual server	The virtual server identifier. Default: server
Webogic Server Instance port	The HTTP port number for the server instance. Default: 8181 (HTTPS)
Webogic Server administration server port	The HTTP port number for the target server instance. Default: 4848
Is administration server port secure	Whether Oracle WebLogic Server administration server port is running over SSL. Default: Enabled
Webogic Server administrator user name and password	The user name and password for the Webogic Server administration server.

Table 3-6 lists the directory server information that you provide during the initial configuration.

Table 3-6   Directory Server Information

Information Type	Description
User/Group LDAP URL	The directory server host and port where the User/Group is located. Syntax: **ldaps://***Host_FQDN***:***port*

Table 3-6   (Cont.) Directory Server Information

Information Type	Description
Bind domain name	The directory server domain name used to bind the directory server managing the User/Group data. Syntax: **cn=***Directory_Manager*
Bind password	The password for the Bind domain name.

Table 3-7 lists the information required for other software that you provide during the initial configuration.

Table 3-7   Software Information

Information Type	Description
Default domain name	The domain name for your deployment. For example: *MyDomain***.com**
Webmail host name	The Messaging Server host name. Syntax: **ms.***Default_Domain* For example: **ms.***MyDomain***.com**
Webmail port number	The Messaging Server HTTP port number. Default: 8991 (HTTPS)
Access (Messaging Server) in SSL mode	Whether the Messaging Server port is running over SSL. Default: Enabled
Webmail administrator user name and password	The administration user name and password for Messaging Server.
Calendar Server version	The version of your Calendar Server. Default: 8.0.x
Calendar Server host name	The Calendar Server host name. Syntax: **cs.***Default_Domain* For example: **cs.***MyDomain***.com**
Calendar Server port number	The Calendar Server HTTP port number. Default: 8181 (HTTPS)
Access (Calendar Server) in SSL mode	Whether the Calendar Server port is running over SSL. Default: Enabled
Calendar Server URI	The Calendar Server URI. Default: **/davserver/wcap**
Calendar Server administrator user name and password	The administration user name and password for Calendar Server.
Convergence address book service	How the address book service is provided. You can select either Convergence or Contacts Server. Default: Convergence Address Book
Contacts Server host name	The Contacts Server host name. Syntax: **cos.***Default_Domain* For example: **cos.***MyDomain***.com**
Contacts Server port number	The Contacts Server HTTP port number. Default: 8181 (HTTPS)

Table 3-7 (Cont.) Software Information

Information Type	Description
Access (Contacts Server) in SSL mode	Whether the Contacts Server port is running over SSL. Default: Enabled
Contacts Server URI	The Contacts Server URI. Default: /
Contacts Server administrator user name and password	The administration user name and password for Contacts Server.

4

Convergence Pre-Installation Tasks

This chapter describes the pre-installation steps you must complete before installing and configuring Oracle Communications Convergence.

Installing Java

The application server (Oracle WebLogic Server) is a Java application and needs a Java environment to run.

Install the 32-bit Java JDK if you run a 32-bit OS. Install the 64-bit Java JDK if you run a 64-bit OS.

Download the Java software from the Oracle web site:

`http://www.oracle.com/technetwork/java/javase/downloads/index.html`

Satisfying Unified Communications Suite Software Dependencies

For each optional or required software application you plan to install to deliver Convergence services, you must satisfy its software requirements and pre-installation tasks. For example, if you plan to integrate Convergence with Oracle Communications Messaging Server, Oracle Communications Calendar Server, and Oracle Communications Contacts Server, you must satisfy the software requirements for each of these applications and complete all their pre-installation tasks.

Preparing the Directory Server

You prepare your directory server by running the directory server setup script (rundssetup) against it. You can run the script in either interactive or silent mode.

You must ensure that the directory server is running the correct version of the directory server setup script. See "System Requirements" for more information about the required script version.

To configure Oracle Unified Directory (OUD), use the rundssetup script.

Before running DS Setup, ensure that a Directory Server instance is already created, and install the following:

- OUD 12.2.1.4
- Python 2.7 and above

> **Note:**
>
> To install Oracle Unified Directory, refer to the Installing the Oracle Unified Directory Software in *Oracle Fusion Middleware Installing Oracle Unified Directory*.

To prepare the directory server:

1. Download the DS Setup from:

   https://support.oracle.com

   The rundssetup script is available in the same software package as the Convergence software.
2. Copy the directory server ZIP file to a temporary directory on your directory server hosts and extract the files.
3. Log on to the directory server host machine as the superuser (**root**).
4. Start the directory server, if necessary.
5. Change to the directory where you extracted the rundssetup script.
6. Install the rundssetup script.

   ```
   ./commpkg install
   ```

   Select **Comms DSsetup** from the list of applications to install and proceed with the installation.

   See "commpkg Reference" for more information about the **commpkg** command.
7. rundssetup script can be executed in interactive mode or silent mode.

   ```
   python rundssetup --dsType OUD
   ```

   Answer the command-line prompts.

   > **Note:**
   >
   > You can use either LDAP Schema 2 or Schema 1.

To execute rundssetup script in silent mode, refer "Running rundssetup in silent mode".

If the directory server is already installed at your site, users have already been provisioned. If you have just installed the directory server at your site, then you need to provision users. For information about provisioning users and schema, see *Communications Suite Schema Reference*.

Running rundssetup in silent mode

Following are the options supported for running in silent mode:

```
rundssetup [-h] [--version] [--debug] [--verbose] [-D BINDDN]

    [-j PASSWDFILE] [-i {yes,no}] [-R {yes,no}] [-d INSTLOC]

    [-r DCTREE] [-u UGSUFFIX] [-s {yes,no}] [-t {1,1.5,2}]

    [-m {yes,no}] [-f {yes,no}] [--silent SILENTFILE]

    [--dsType {OUD,DSEE}] [--createSuffixes {yes,no}]

    [--createSuffixDN {yes,no}] [--createMLusersSuffix {yes,no}]

    [--createPiServerDbSuffix {yes,no}]
```

For example,

schema 2:

```
rundssetup -D "cn=Directory Manager" -j /tmp/ds_pass -i yes -R yes -d /oracle/Oracle/
Middleware/asinst_1 -u o=usergroup -s yes -t 2 -m yes -f yes --silent=NONE --dsType=OUD
--createSuffixes yes --createSuffixDN no --createMLusersSuffix yes --
createPiServerDbSuffix yes
```

schema 1:

```
rundssetup -D "cn=Directory Manager" -j /tmp/ds_pass -i yes -R yes -d /oracle/Oracle/
Middleware/asinst_1 --schemaType 1 -r "o=internet" -u "o=usergroup" -s yes -t 1 -m yes -
f yes --silent=NONE --dsType=OUD --createSuffixes yes --createSuffixDN no --
createMLusersSuffix yes --createPiServerDbSuffix yes
```

For more information, run:

```
rundssetup --help
```

Installing and Configuring Unified Communications Suite Software

Install and configure the Oracle Communications software required to deliver your planned Convergence services.

Refer to the documentation for each Oracle Communications application for pre-installation, installation, configuration, and post-installation details.

Enabling MSHTTP in Messaging Server

You must enable HTTP service in Messaging Server by setting the related configuration parameters.

To enable MSHTTP, do one of the following and restart Messaging Server:

- If Messaging Server is deployed with a legacy configuration, set **service.http.enable** parameter to **1**.
- If Messaging Server is deployed with a Unified Configuration, set the **http.enable** parameter to **1**.

See the Messaging Server wiki for more information about http parameters:

http://msg.wikidoc.info/index.php?title=MSHTTP_options

Enabling Message Body Filtering in Messaging Server

You must enable email message body filtering in Messaging Server. Message body filtering allows users to create mail filter rules on the content of email messages.

To enable email message body filtering, do one of the following:

- If Messaging Server is deployed with a legacy configuration, edit **option.dat**, locate the **ENABLE_SIEVE_BODY** parameter, and set it to **1**.
- If Messaging Server is deployed with a Unified Configuration, set the **mta.enable_sieve_body** parameter to **1**.

See the Messaging Server wiki for more information about the **enable_sieve_body** parameter:

http://msg.wikidoc.info/index.php/Enable_sieve_body_MTA_option

5 Installing Convergence

This chapter describes how to install and configure Oracle Communications Convergence.

Installation Assumptions

The instructions in this chapter assume the following:

- That you have installed and configured Oracle WebLogic Server.
- That you have installed and configured all required and optional Unified Communications Suite software needed to deliver your Convergence services.

Downloading the Convergence Software

1. Download the Convergence software for your operating system from the Oracle software delivery web site:

   https://support.oracle.com

   The Convergence software is included in the Oracle Communications Messaging Server and Oracle Communications Calendar Server software package.

2. Extract the Convergence software to a temporary directory (*dir*).

Installing Convergence

You can install Convergence in either interactive mode or in silent mode. See one of the following topics for more information:

- Installing Convergence in Interactive Mode
- Installing Convergence in Silent Mode

Installing Convergence in Interactive Mode

To install Convergence in interactive mode:

1. From *dir*, run the installer:

   ```
   ./commpkg install
   ```

   > **Note:**
   >
   > In case of any failure or no action when the above command is executed, run the installer as:
   >
   > ```
   > ./commpkg -OSversionOverride install
   > ```

See "commpkg Reference" for more information about the **commpkg** command.

2. From the list of available Unified Communications Suite software products for installation, select Convergence and proceed with the installation.

Installing Convergence in Silent Mode

You can use silent mode to install multiple instances of the same software component and configuration without having to manually run an interactive installation for each instance.

To run a silent installation:

1. Obtain a silent installation state file using one of the following means:
    - Use a state file from a previous installation. The installer creates a state file in the **/var/opt/CommsInstaller/logs/** directory each time it installs software. The state file name resembles **silent_CommsInstaller_20070501135358**.
    - Create a state file by running the installer in interactive mode with the **--dry-run** option. This option runs the installer, but does not actually install the software. For example:

      ```
      commpkg install --dry-run
      ```

2. Copy the state file to each host and modify the file as needed.

   The state file is formatted like a property file: blank lines are ignored, comment lines begin with a number sign (#), and properties are key/value pairs separated by an equals (=) sign. Table 5-1 lists the state file options.

Table 5-1 State File Options

Option	Description	Example
VERB	Specifies which function to perform. For a silent install, **VERB** is set to **install**.	**VERB=install**
ALTDISTROPATH	Specifies an alternate distro path.	**ALTDISTROPATH=SunOS5.10_i86pc_DBG.OBJ/release**
PKGOVERWRITE	Specifies a boolean indicating whether to overwrite the existing installation packages.	**PKGOVERWRITE=YES**
INSTALLROOT	Specifies the installation root.	**INSTALLROOT=/opt/sun/comms**
ALTROOT	Specifies a boolean indicating whether to use an alternate root install.	**ALTROOT=yes**
EXCLUDEOS	Specifies to not upgrade operating system patches.	**EXCLUDEOS=YES**
EXCLUDESC	Specifies to exclude shared component patches.	**EXCLUDESC=no**
COMPONENTS	A space separated list of mnemonics of the components to be installed. You can precede the mnemonic with a ~ to indicate that only the shared components for that product be installed.	To specify Convergence: **COMPONENTS=IWS** To view a list of mnemonic product names, run the **commpkg info --listPackages** command.
ACCEPTLICENSE	This option is no longer used.	NA
UPGRADESC	Specifies whether to upgrade all shared components without prompting.	**UPGRADESC=no**
INSTALLNAME	The friendly name for the **INSTALLROOT**.	**INSTALLNAME=**
COMPONENT_VERSIONS	This option is unused.	NA

3. Run the installer in silent mode on each host:

   ```
   commpkg install --silent input_file
   ```

   where *input_file* is the path and name of the state file. For example: **/var/opt/CommsInstaller/logs/silent_CommsInstaller_20070501135358**.

   See "install Verb Syntax" for more information about the **--silent** option.

About Upgrading Shared Components in Silent Mode

By default, the option to upgrade shared components in the state file is automatically disabled (the **UPGRADESC** option is set to **No**.) This is true even if you explicitly asked to upgrade shared components when you ran the interactive installation that generated the state file. That is, you ran either **commpkg install --upgradeSC y** or you answered **yes** when prompted for each shared component that needed upgrading.

Disabling upgrading shared components in the silent state file is done because the other hosts on which you are propagating the installation might have different shared components installed, or different versions of the shared components. Therefore, it is safer to not upgrade the shared components by default.

If you want to upgrade shared components when you run a silent installation, do one of the following:

- Use the **--upgradeSC y** option when you run the silent installation. (The command-line argument overrides the argument in the state file.)
- Edit the value of the UPGRADESC option in the silent installation state file: **UPGRADESC=Yes**.

Configuring Convergence

This section explains how to complete the initial configuration for Convergence, and how to configure Convergence to integrate with other Unified Communications Suite software applications.

The Convergence initial configuration program automatically creates a silent configuration file when the program completes successfully. You can use the silent configuration file to automate future configurations. See "Running the Convergence Initial Configuration Script in Silent Mode" for more information.

Installing and Configuring Oracle WebLogic Server for Convergence

Before you install and configure Oracle WebLogic Server for Convergence, prepare the System user and groups for the installation:

- Create a system user and group for Oracle WebLogic Server setup.

> **Note:**
>
> You must install Oracle WebLogic Server by using a non-root user. For example, to install Oracle WebLogic Server, you can use a Unix non-root user as **uadmin** and a Unix group user as **staff**. You can install Convergence by using a root user or any other user who is added to the **staff** group and possess the same permissions or access as **uadmin**.

- Create an Oracle WebLogic Server home directory for installation and ensure that the permissions for the required setup directories are set as shown in the following example:
  - mkdir *WL_Home*
  - chmod 755 *WL_Home*
  - chown -R uadmin *WL_Home*
  - chgrp -R staff *WL_Home*
- Install JDK 1.8.0 update version on the platform. Ensure **JAVA_HOME** and PATH environment variables are set in the user environment

To install and configure Oracle WebLogic Server for Convergence:

1. Download and unzip the ZIP file that you have obtained for the **Generic** package. See "Oracle WebLogic Server 12.2.1.4 documentation" for information on Oracle WebLogic Server download location.
2. Create a Domain, Administration Server, and Managed Server. See "Starting the Installation Program" for more information.

   See the following Oracle WebLogic Server resources for more information:
   - "Oracle WebLogic Server 12.2.1.4 documentation"
   - "Starting the Installation Program"
   - "Oracle Universal Installer Installation steps"
3. Navigate to the WebLogic Domain directory that you have created. For example, *WL_Home*/**user_projects**/**base_domain**/**bin**.
4. Modify **setDomainEnv.sh** to add the following applicable settings.
   - The following modification is only for the Solaris 11.4 version:
     - JAVA_OPTIONS="${JAVA_OPTIONS} -Dsun.security.pkcs11.enable-solaris=false"
     - export JAVA_OPTIONS
   - (Optional) If you get a Random number related error when you restart the server, ensure to add the following:
     - JAVA_OPTIONS="${JAVA_OPTIONS} -Djava.security.egd=file:/dev/./urandom"
     - export JAVA_OPTIONS
   - To disable DERBY, add the following settings at the end of the file:
     - DERBY_FLAG=**false**
     - export DERBY_FLAG
5. Ensure to set the environment in the terminal that is used to start the servers by sourcing the **setDomainEnv.sh** file as shown below:
   - **cd** *WL_Home*/**user_projects/base_domain/bin**
   - **source** ./**setDomainEnv.sh** or . ./**setDomainEnv.sh**
6. Start the Administration Server.
7. Configure the Managed Server for default HTTP and HTTPS ports and start the Managed Server.
8. Configure Oracle WebLogic Server in a secure mode using the following details if you want to configure Convergence in a secure mode:

   To enable SSL and configure keystores in Oracle WebLogic Server:

- For more information about setting up keystores, see Configuring SSL in Oracle Fusion Middleware in Oracle WebLogic Server documentation.
- Oracle WebLogic Server offers four keystore options in its configuration. However, only the following two keysotore options are recommended for Convergence:
  - CustomIdentityandCustomTrust
  - CustomIdentityandJavaStandardTrust

> **Note:**
>
> You must always set the keystore type to **JKS**.

- The keystore configuration must be same for an Administration Server and Managed Servers. It means, you should configure the same options or certificates for hosting Convergence.
- You must set keystore passwords identical to the Oracle WebLogic Server Administration Server password.

> **Note:**
>
> Convergence is deployed on Oracle WebLogic Server securely only if the keystore passwords and Oracle WebLogic Server passwords match.

9. Ensure that the Administration Server and Managed Server are started successfully.

Validating and Storing Oracle WebLogic Server SSL Details

When you configure Convergence for the first time with Oracle WebLogic Server in a secure mode, run the **extractSSLArgs.sh** script. This script validates the SSL configuration details in Oracle WebLogic Server and stores the valid details in a format that is required by Convergence for all future deployments and processing.

To validate and store Oracle WebLogic Server SSL details for Convergence in a secure mode:

1. Open a new terminal and prepare the terminal by sourcing the **setDomainEnv.sh** script of the Oracle WebLogic Server domain:

   ```
   cd WL_Home/user_projects/base_domain/bin

   source ./setDomainEnv.sh   OR  . ./setDomainEnv.sh
   ```

2. Set the **WLST_PROPERTIES** environment variable depending on the selected Oracle WebLogic Server keystore configuration.

   - If the **CustomIdentityandCustomTrust** keystore option is configured as the Oracle WebLogic Server keystore configuration, set the **WLST_PROPERTIES** variable to:

     ```
     export WLST_PROPERTIES="-Dweblogic.security.TrustKeyStore=CustomTrust , -
     Dweblogic.security.CustomTrustKeyStoreFileName=/WLHOME/user_projects/domains/
     base_domain/mytrust.jks"
     ```

     Where *WLHOME/user_projects/domains/base_domain/mytrust.jks* is the location of truststore file location.

- If the **CustomIdentityandJavaStandardTrust** keystore option is configured as the Oracle WebLogic Server keystore configuration, set the **WLST_PROPERTIES** variable to:

  ```
  export WLST_PROPERTIES="-Dweblogic.security.TrustKeyStore=JavaStandardTrust"
  ```

3. Run the **extractSSLArgs.sh** bash shell script **extractSSLArgs.sh** which is available under the Convergence installed location: *Convergence_Server_Installedlocation*/**sbin**:

   ```
   sh ./extractSSLArgs.sh -u weblogic_admin_user -p weblogic_admin_user_password -l
   t3s://weblogic_server_host:SSL_port
   ```

   If the execution of the script is successful, it creates **.wls_sslargs** under the configuration directory of your Oracle WebLogic Server domain. You can verify the creation of **.wls_sslargs** by navigating to *WLS_DOMAIN_DIRECTORY*/**config**

Running the Convergence Initial Configuration Script for Oracle WebLogic Server

The Convergence initial configuration script launches a program that gathers the required information from you to configure Convergence. See "Information Requirements" for details about the information required to configure Convergence.

- Create a symbolic link between **/usr/jdk/latest** and the desired installed JDK in the **/usr/jdk** directory.
- For example:

  ```
  ln -s /usr/jdk/jdk1.8.0_x /usr/jdk/latest
  ```

- Make sure JAVA_HOME and PATH variables are set in the current shell

To configure Convergence using the initial configuration script:

1. Verify that Oracle WebLogic Server is running.
2. Verify that the directory server is running.
3. Verify that all the Unified Communications Suite software applications with which you intend to integrate Convergence are running.
4. Run the Convergence initial configuration script:

   ```
   ./Convergence_Home/sbin/init-config
   ```

   See "Convergence Configuration Scripts" for more information.

   ```
   ./Convergence_Home/sbin/init-config
   ```

   The Convergence configuration Welcome message appears followed by Convergence Settings section.

   > **Note:**
   >
   > To run the configuration program in silent mode, see Running the Convergence Initial Configuration Script in Silent Mode.

5. Enter the following in Convergence Settings section when prompted:
   - Directory to Store Configuration and Data Files.

    – Do not enter Convergence_Home as the location directory.

- Select the services to configure with Convergence.

    a. Mail Service

    b. Calendar Service

    c. Contacts Service

    If you do not select Contacts Service, Convergence Address Book service will be configured. You can enter multiple items using commas to separate them. For example: 1,2.

    By default only mail service is selected.

- Enter the host name of the system on which Convergence is being configured.
- Enter the DNS domain name of the Convergence host system.

6. Enter the following in Application Server Settings section when prompted:
    - Oracle WebLogic Server Domain directory
    - Oracle WebLogic Server Virtual directory or Document root directory
    - Oracle WebLogic Server target instance name
    - Oracle WebLogic Server Virtual server identifier
    - Oracle WebLogic Server instance port
    - Oracle WebLogic Server Administration server port
    - Is Administration Server port secure
    - Oracle WebLogic Server Administration user ID
    - Oracle WebLogic Server Administration password
    - Oracle WebLogic Server installation user ID
    - Oracle WebLogic Server installation Group ID
    - URI path to where you want to deploy Convergence.

        For example: **/iwc**

    The program tests the connection to Oracle WebLogic administration server. If there is an error while connecting to Application Server, error message will be displayed and user has to enter the correct values to proceed. After validations, Directory Server Settings section appears.

7. Enter the following in Directory Server Settings section when prompted.
    - Specify Whether You Want Hosted Domain Support
    - User/Group LDAP URL: URL for the User/Group LDAP used by Messaging Server and Calendar Server.

        For example: ldaps://MyDomain.com:port

    - Bind DN: Enter the LDAP distinguished name (DN) of the administrator used to bind to the directory server.

        For example: cn=Directory Manager

    - Bind Password: The Bind DN password.
    - Base DN of the DC Tree Suffix.

The configuration program retrieves the base DN from the directory server. You can accept the retrieved value or change it.

This base DN is used to perform domain lookups. If the back-end servers are using Schema 1, this configuration setting specifies the DN of the DC Tree suffix. If the back-end servers are using Schema 2, this setting specifies the DN of the root suffix under which the User/Group tree is located. You must enter (confirm) a value for this item whether you are using Schema 1 or Schema 2.

In a Schema 1 directory layout, Convergence uses the DC Tree suffix to search for domain information. In a Schema 2 directory layout, there is only one root suffix; both domain and user/group data are located under this one suffix.

- Enter the default domain name.

  The default domain name is used during login when the user does not provide the domain as part of their user name.

  For example, if a user attempts to login as John.Smith, the user name qualifies as John.Smith@*DefaultDomain*.com

8. If you chose to configure the mail service, Mail Service Configuration Details section appears.

   Specify the following:

   - Webmail host name
   - Webmail server port number

     The SSL port is provided by default.
   - Access in SSL mode
   - Webmail server administration user ID
   - Webmail server administration password

   The program tests the connection to the Messaging server.

9. If you chose to configure the calendar service, the Calendar Service Configuration Details section appears.

   Specify the following:

   - Calendar server host name
   - Calendar server port number

     The SSL port is provided by default.
   - Access in SSL mode
   - Service URI
   - Calendar server admin user ID
   - Calendar server admin password

   The program tests the connection to the Calendar server.

10. If you chose to provide the address book service with Contacts Server, the Contacts Server Configuration Details screen appears.

    Specify the following:

    - Contacts server host name
    - Contacts server port number

      The SSL port is provided by default.

- Access in SSL mode
- Service URI
- Contacts server admin user ID
- Contacts server admin password

The program tests the connection to the Contacts server.

11. Enter the following in Convergence Administration section when prompted:

    - Provide the Convergence administrator user name.
    - Provide the Convergence administrator password.

      The Administrator user name and password are used for Convergence administration. The user details for the Convergence administrator are stored in the Convergence configuration files, not in the directory server. This administrator user is not tied to any back-end server administrator accounts.

    The confirmation message to Configure Convergence appears with Y/N options. Choose Y to configure. Choosing N stops the configuration process. The Task Sequence section displays the configuration tasks being performed.

    After successful configuration, the screen displays the message Oracle Communications Convergence is configured successfully.

When you complete the configuration process, the initial configuration program creates a configuration file that you can use to automate future configurations. See "Running the Convergence Initial Configuration Script in Silent Mode" for more information.

Running the Convergence Initial Configuration Script in Silent Mode

The Convergence initial configuration program automatically creates a silent configuration file when the program completes successfully. You can use the silent configuration file to automate future configurations.

The silent configuration file is called **saveState** and is created in the *Convergence_Home***/data/setup/lwc-config-***YYYYMMDDHHMMSS* directory, where *YYYYMMDDHHMMSS* represents the date and time of the **saveState** file.

To configure Convergence using the initial configuration script in silent mode:

1. Verify that Oracle WebLogic Server is running.
2. Verify that the directory server is running.
3. Verify that Oracle Communications Messaging Server, Oracle Communications Calendar Server, and any other Unified Communications Suite software applications with which you intend to integrate with Convergence are running.
4. As the root user or super user, run the Convergence initial configuration script:

   ```
   ./Convergence_Home/sbin/init-config -nodisplay -state path/saveState
   ```

   Where *path* is the directory in which the **saveState** file is located.

6
Convergence Post-Installation Tasks

This chapter provides post-installation tasks and instructions for Oracle Communications Convergence.

Verifying the Convergence Installation

Verify the Convergence installation and configuration to ensure it completed successfully.

To verify the Convergence installation, log in to Convergence.

Access Convergence in a supported browser at the following URL:

```
http://hostname.domain:port/URI
```

If Convergence is configured with SSL, use the following URL instead:

```
https://hostname.domain:port/URI
```

For example, if during the Convergence configuration program, you supplied the following values:

- For **Convergence server host name**, you entered **Convergence**.
- For **DNS domain name**, you entered **MyDomain.com**.
- For **Specify the URI path**, you accepted the default **/iwc**.

The Convergence URL would be:

```
http://Convergence.MyDomain.com:8080/iwc
```

or

```
https://Convergence.MyDomain.com:8181/iwc
```

Configuring Convergence Security

See *Convergence Security Guide* for information about security concepts and features, and see *Convergence System Administrator's Guide* for information about enabling security features in your Convergence deployment, such as secure sockets layer (SSL), single sign-on (SSO), mail encryption, digital signatures, and certificate-based authentication.

Customizing Convergence

Convergence is highly customizable. See *Convergence Customization Guide* for more information.

Configuring Add-On Services

Convergence supports add-on services, including:

- One-way short message service (SMS)

- Advertising

See the discussion about add-on services in *Convergence System Administrator's Guide* for more information.

Configuring Convergence for Attachment Previewing

By default, Convergence can preview JPG, GIF, and TXT email attachments. Some web browsers or browser plug-ins enable Convergence to preview PDF email attachments.

You can integrate Convergence with Oracle Outside In Transformation Server to enable it to render and preview many different file types in the browser, including DOC and XLS files.

See the discussion about managing attachment previewing in *Convergence System Administrator's Guide* for more information.

Installing Oracle Outside In Transformation Server

Install Oracle Outside In Transformation Server according to its documentation. When the installation is complete, do the following:

1. Go to the Outside In Transformation Server home directory.
2. Edit **agent_option_sets.xml**. Locate the <OptionSets> element and add to it the code in bold from the following example:

```
<OptionSets xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/" xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:ts="http://
www.outsideinsdk.com/transformation_server/transform/1/0/" xmlns:tss="http://
www.outsideinsdk.com/transformation_server/startup/1/0/"
xsi:type="tss:OptionSetList">
  <OptionSet xsi:type="tss:OptionSet">
    <Name xsi:type="xsd:string">comm_suite_options</Name>
    <Options xsi:type="tss:OptionList">
      <Option xsi:type="ts:Option">
        <name xsi:type="xsd:string">preferOITRendering</name>
        <value xsi:type="xsd:boolean">true</value>
      </Option>
    </Options>
  </OptionSet>
</OptionSets>
```

   The OptionSet <Name> element must have the value **comm_suite_options**.

7

Upgrading Convergence

This chapter describes how to upgrade Oracle Communications Convergence.

This chapter does not explain how to install patches on Convergence.

About Upgrading Convergence

In this chapter, the release from which you are upgrading is called the *old* release, and the release to which you are upgrading is called the *new* release.

Upgrading to a new release of Convergence consists of the following tasks:

- Planning the upgrade
- Reviewing the upgrade impacts
- Performing the pre-upgrade tasks
- Upgrading Convergence
- Performing the post-upgrade tasks

Before upgrading a production environment, you should first test the upgrade in a test environment. See "Testing the Upgrade in a Test Environment" for more information.

Supported Upgrade Paths

You can upgrade to the new version of Convergence from 3.0.2.x version.

See "Upgrading from 3.0.2.x to 3.0.3" for more information.

> **Note:**
>
> - Convergence deployments can be upgraded from 3.0.2.x.0 to 3.0.3.0.0 using **./commpkg upgrade**.
> - In case of any issue ,use this command **./commpkg --OSversionOverride upgrade**.
>
> If you are using a Glassfish deployment, Oracle recommends you to migrate to Weblogic, using the steps provided in "Migrating Convergence Deployment from GlassFish Server to Oracle WebLogic Server".

Planning Your Convergence Upgrade

Depending on the components affected by the upgrade, your upgrade team may include the following:

- A system administrator, to manage any changes to Oracle WebLogic server and to upgrade other Oracle Communications software.

- A UNIX administrator, to manage accounts, network setup, and IP configurations.

Identify who might be affected by the upgrade. For example:

- You might need to give your system administrators and users notice of downtime.
- Tell your system administrator in advance about any changes to the system architecture.
- Train your administrators, users, and developers on new functionality introduced by the upgrade that has an impact on their role.

You might need to make changes to your system after the upgrade is complete to accommodate new or modified features or functionality. For example, if the new release provides new security functionality, additional system configuration steps may be required. See "Upgrade Impacts" for more information.

The best way to estimate the duration of an upgrade is to perform it on a test system with a copy of the production data. See "Testing the Upgrade in a Test Environment" for more information.

Oracle recommends scheduling your upgrade during non-peak hours to minimize the disruption to your operations.

Testing the Upgrade in a Test Environment

Oracle recommends running the upgrade procedure on a test system that models your production environment. Test the upgrade by doing the following:

- Successfully completing all the pre-upgrade, upgrade, and post-upgrade tasks.
- Comparing the default behavior between the old and the new releases.
- Test that your customizations are preserved. Recreate any custom configurations and customizations that could not be upgraded.
- Confirming that all new behavior and functionality works.
- Restarting the Convergence server.
- Log into Convergence and verify its version number

Upgrade Impacts

This section explains any important system changes introduced in the new release of Convergence.

This section does not describe new features or functionality. See *Convergence Release Notes* for information about new features.

Upgrade Impacts from Version 3.0.2.x to 3.0.3.0.0

Upgrading to the new version of Convergence includes the following system changes:

- Java Development Kit Changes
- Directory Server Schema Changes
- Unified Communications Suite Software Compatibility Changes

Java Development Kit Changes

The new version of Convergence requires an updated version of the Java Development Kit (JDK) on the Convergence server. See "System Requirements" for more information. Upgrade Java before upgrading Convergence.

Directory Server Schema Changes

The new version of Convergence requires an updated version of the directory server schema.

Unified Communications Suite Software Compatibility Changes

The new version of Convergence may be compatible with a few older versions of other Unified Communications Suite software. However, it is recommended to upgrade the other Unified Communications Suite software to the latest version to use with this release of Convergence. See "Software Requirements" for more information.

Upgrading from 3.0.2.x to 3.0.3

To upgrade to the new release of Convergence, complete the following:

- Pre-Upgrade Tasks (3.0.2.x to 3.0.3)
- Upgrading Convergence (3.0.2.1.0 to 3.0.3.x)
- Post-Upgrade Tasks (3.0.2.x to 3.0.3)

Pre-Upgrade Tasks (3.0.2.x to 3.0.3)

Before upgrading Convergence, do the following:

1. Install or upgrade the following software:
   - Upgrade the JDK
   - (Optional) Install Oracle Access Manager
   - Install OpenLDAP client or Install Directory Server based LDAP client, if your operating system does not provide it by default
2. Determine whether you need to update the directory server schema version.

   See "Preparing the Directory Server" for more information.
3. Upgrade or install all required and optional Unified Communications Suite software needed to deliver your existing and planned Convergence services. For example, if you are integrating Convergence with Contacts Server to deliver the address book service, install Contacts Server. If you decide to upgrade to a new version of Oracle Communications Messaging Server, upgrade Messaging Server.

   Refer to your application installation documentation for upgrade and installation instructions.
4. Create a directory (*dir*) on each Convergence host system.
5. Download the Convergence software for your operating system from the Oracle software delivery web site:

   `https://edelivery.oracle.com/`

The Convergence software is included in the Oracle Communications Messaging Server and Oracle Communications Calendar Server software package.

6. Extract the Convergence software to *dir*.

Upgrading Convergence (3.0.2.1.0 to 3.0.3.x)

You use the **commpkg upgrade** command to upgrade to the new version of Convergence. The **commpkg upgrade** command upgrades Convergence with an in-place package replacement that cannot be reversed.

To upgrade Convergence on each Convergence host system:

1. Verify that the Application Server is running.
2. Verify that the directory server is running.
3. Verify that all the Unified Communications Suite software with which you intend to integrate Convergence is running.
4. Make sure that the **JAVA_HOME** variable is set to JDK_location in the current shell or in GlassFish Server user profile.
5. From *dir*, run the upgrade installer:

   ```
   ./commpkg upgrade
   ```

   See "commpkg Reference" for more information about the **commpkg** command.
6. From the list of available Communications Products for upgrade, select Convergence and proceed with the upgrade.
7. When the installer has completed the upgrade, restart the weblogic Admin Server and Weblogic Managed Server domain on which Convergence is deployed.

Post-Upgrade Tasks (3.0.2.x to 3.0.3)

After the Convergence upgrade has completed successfully, do the following that apply to you:

- Configure Convergence to work with newly installed Unified Communications Suite software. For example, if as part of this upgrade, you are integrating Convergence with Contacts Server for the first time, you need to configure Convergence to communicate with Contacts Server.

  See "Configuring Convergence" for more information.

Migrating Convergence Deployment from GlassFish Server to Oracle WebLogic Server

Prerequisites for migrating Convergence from GlassFish Server to Oracle WebLogic Server are:

- A previous version of Convergence is installed on GlassfFish 3 or GlassFish 5.
- You must have installed Oracle WebLogic Server 12.2.1.4.

To migrate Convergence deployment from GlassFish Server to Oracle WebLogic Server:

1. Back up the configuration c11n folder and output of **iwcadmin -1** command.

2. Backup the latest savestate file from **Convergence_Home/data/setup/Iwc-config-YYYYMMDDHHMMSS** directory.
3. Install the latest version of Convergence using commpkg tool.
4. Start Oracle WebLogic Admin Server and Managed Server.
5. Make sure all the backend servers are up and running.
6. Configure Convergence using Webogic as application server. Refer to the SaveState file from step 2, for backend and other details.
7. Make sure Convergence configuration is successful.
8. Copy the backed up c11n folder to the configured Document Root Directory, **data_directory/web-src/client/iwc_static**.
9. Update the missing required configurations on Oracle WebLogic Deployment by comparing the output of **iwcadmin -l** command in GlassFish and Oracle WebLogic deployments.
10. Copy the required configuration files from the backed up configuration folder to the new configuration folder. For example, advertising.json.
11. Restart the Managed Server and Login to Convergence to verify that everything is working as expected. For example,you can login to Convergence and access the configured services.

8 Uninstalling Convergence

This chapter describes how to uninstall Oracle Communications Convergence.

Uninstalling Convergence

Use the **commpkg uninstall** command to uninstall the binary files for any Communications Suite applications and shared components.

The **commpkg uninstall** command does not remove OS patches or shared components installed by the **commpkg install** command.

To uninstall Convergence:

1. Undeploy Convergence from Oracle WebLogic server domain.
   - You can use the **java weblogic.Deployer** command or Oracle WebLogic Administration Console to undeploy Convergence. See Oracle WebLogic Server documentation for more information.
2. Change to the *UCS_Home***/CommInstaller/bin** directory.

   Where *UCS_Home* is the installation location for the Unified Communications Suite software. By default, *UCS_Home* is **/opt/sun/comms**.
3. Run the uninstall command:

   ```
   ./commpkg uninstall
   ```

   > **Note:**
   >
   > In case of any failure or no action when the above command is executed, run the installer as
   >
   > ```
   > ./commpkg -OSversionOverride uninstall
   > ```
4. Choose Convergence from the list of installed Unified Communications Suite components and click **Yes**.
5. Follow the on-screen prompts.

A

commpkg Reference

This appendix provides information about the **commpkg** command.

Overview of the commpkg Command

The **commpkg** command, also referred to as the Installer, comprises several commands (verbs) that enable you to install, uninstall, and upgrade Oracle Communications Convergence software and its shared components. The **commpkg** command is installed in the directory in which you unzip the software.

Syntax

```
commpkg [general_options] verb [verb_options]
```

where:

- *general_option*s is one or more of the general option described in Table A-1.
- *verb* is a command verb described in Table A-2.
- *verb_option*s is one or more options that affects the command verb.

Table A-1 describes the **commpkg** command general options.

Table A-1 commpkg Command General Options

commpkg General Options	Description
-? or **--help**	Displays help for the **commpkg** command.
-V or **--version**	Displays the Installer version.
--OSversionOverride	Overrides the operating-system version check.
--fixEntsys [**y**|**n**]	Fixes an invalid Sun Java Enterprise System (Java ES) **entsys symlink**, making the link point to the latest Java version upgraded by **commpkg**. The Java ES symlink is located in **/usr/jdk/entsys-j2se**. Choose **--fixEntsys y** to fix the Java ES symlink to the Java files. If you do not specify this switch, **commpkg** prompts you if the symlink is invalid. However, in silent mode, the default is not to fix the symlink (the equivalent of using a value of n). To fix the symlink in silent mode, type **commpkg install --fixEntsys y --silent** *INPUTFILE* on the command-line.

Table A-2 describes the **commpkg** command verbs.

Table A-2 commpkg Command Verbs

commpkg Command Verbs	Description
install	Performs software installation.

Table A-2 (Cont.) commpkg Command Verbs

commpkg Command Verbs	Description
uninstall	Uninstalls software but does not remove OS patches or shared components installed by **commpkg install**.
info	Displays product information on the paths (also known as *installroots*) where Convergence is installed, and the products that are installed in those paths.
upgrade	Performs software upgrade.
verify	Verifies installed product.

install Verb Syntax

```
commpkg install [verb_options] [ALTROOT|name]
```

Table A-3 describes the **commpkg install** verb options.

Table A-3 commpkg install Options

commpkg install Options	Description
-? or **--help**	Displays help for the install verb.
-V or **--version**	Displays the Installer version.
--excludeOS	Does not apply operating system patches during product installation.
--excludeSC	Does not install, upgrade, or patch any shared components.
ALTROOT|name	This option is available on Solaris only. Specifies an alternate root directory for a multi-instance installation. The *InstallRoot* (the top-level installation directory for all products and shared components) is the alternate root. Use this option to install multiple instances of the product on the same host or Oracle Solaris zone. You can also use this option to perform a side-by-side upgrade of the product. You can give the alternate path a *name*, which is registered in the software list. If you enter *name* as part of the option and it exists in the software list, the corresponding *ALTROOT* is used. If you also specify the **--installroot** option, it must correspond to the entry in the software list. If you specify name and it does not exist in the software list, it is added to the software list. Specifying any *name* other than “” implies an **ALTROOT**. A value for *name* of “” is reserved for the default root.
--installroot	Specify location of INSTALLROOT, the top level installation directory for all products and shared components. The top-level installation directory for individual products are subdirectories under INSTALLROOT. Default is **/opt/sun/comms**.
--distro *path*	Specifies the *path* to packages or patches for the products. Default: Location of **commpkg** script

Table A-3 (Cont.) commpkg install Options

commpkg install Options	Description
--silent *INPUTFILE*	Runs a silent installation, taking the inputs from the *INPUTFILE* and the command-line arguments. The command-line arguments override entries in the *INPUTFILE*. Installation proceeds without interactive prompts. Use **--dry-run** to test a silent installation without actually installing the software. Specify **NONE** for *INPUTFILE* if you want to run in silent mode without using an input file. When you specify **NONE**, the installation uses default values.
--dry-run or **-n**	Does not install software. Performs checks.
--upgradeSC [**y**|**n**]	Upgrades or does not upgrade shared components as required. If this option is not specified, you are prompted for each shared component that needs to be upgraded by using package removal and installation. Default: **n** **Caution:** Upgrading shared components by using package removal and installation is irreversible. However, if you do not upgrade required shared components, products might not work as designed. The **--excludeSC** flag has precedence over this flag.
--auditDistro	Audits the installation distribution to verify that the patches and packages matches the versions in the product files internal to the installer.
--pkgOverwrite	Overwrites the existing installation package. You might use this option when you are installing a shared component in a global zone where either the shared component does not exist in a global zone, or the shared component exists in the whole root zone. The default is not to override the existing package. In general, shared components should be managed in the global zone.
--components *comp1 comp2...*	A space delimited set of component products. Each product has mnemonic associated with it. Use **commpkg info --listPackages** to see the mnemonic for a product. In most shells you need to escape the space between each mnemonic, that is, by adding double quotes around all the components.
--skipOSLevelCheck	(Solaris only) The Installer always checks that the operating system is at a certain minimum patch level. Using this option skips the check.

uninstall Verb Syntax

```
commpkg uninstall [verb_options] [ALTROOT|name]
```

Table A-4 describes the **commpkg uninstall** verb options.

Table A-4 commpkg uninstall Options

commpkg uninstall Options	Description
-? or **--help**	Displays help for the uninstall verb.
-V or **--version**	Displays the Installer version.

Table A-4 (Cont.) commpkg uninstall Options

commpkg uninstall Options	Description
--silent *INPUTFILE*	Runs a silent uninstall, taking the inputs from the *INPUTFILE* and the command-line arguments. The command-line arguments override entries in the *INPUTFILE*. Uninstall proceeds without interactive prompts. Use **--dry-run** to test a silent installation without actually installing the software.
--dry-run or **-n**	Does not install software. Performs checks.
ALTROOT|name	This option is available on Solaris only. Use this option to uninstall multiple instances of the product on the same host or Oracle Solaris zone. You can also use this option to perform a side-by-side upgrade of the product. Either specify the *ALTROOT* path or the name that is registered in the software list.

upgrade Verb Syntax

```
commpkg upgrade [verb_options] [ALTROOT|name]
```

Table A-5 describes the **commpkg upgrade** verb options.

Table A-5 commpkg upgrade Options

commpkg upgrade Options	Description
-? or **--help**	Displays help for the upgrade verb.
-V or **--version**	Displays the Installer version.
--excludeOS	Does not apply operating system patches during product upgrade.
--excludeSC	Does not install, upgrade, or patch any shared components.
ALTROOT|name	This option is available on Solaris only. Use this option to upgrade multiple instances of the product on the same host or Oracle Solaris zone. Either specify the *ALTROOT* path or the name that is registered in the software list.
--distro *path*	Specifies the *path* to packages and patches for the products.Default path: Location of the **commpkg** command.
--silent *INPUTFILE*	Runs a silent upgrade, taking the inputs from the *INPUTFILE* and the command-line arguments. The command-line arguments override entries in the *INPUTFILE*. Upgrade proceeds without interactive prompts. Use **--dry-run** to test a silent upgrade without actually installing the software. Specify **NONE** for *INPUTFILE* if you want to run in silent mode without using an input file. When you specify **NONE**, the upgrade uses default values.
--dry-run or **-n**	Does not upgrade software but performs checks. This option creates a silent upgrade file in the **/tmp** directory.

Table A-5 (Cont.) commpkg upgrade Options

commpkg upgrade Options	Description
--upgradeSC [**y**|**n**]	Indicates whether or not to upgrade shared components as required. If this option is not specified, you are prompted for each shared component that needs to be upgraded by the package uninstall/install. Default: **n** **Caution:** Upgrading shared components is irreversible. However, if you do not upgrade required shared components, products might not work as designed. The **--excludeSC** flag has precedence over this flag.
--pkgOverwrite	This option is only for Solaris systems. Overwrites the existing installation package. You might use this option when you are installing a shared component in a global zone where either the shared component does not exist in a global zone, or the shared component exists in the whole root zone. The default is not to override the existing package. In general, shared components should be managed in the global zone.
--components *comp1 comp2...*	Specifies products to be upgraded. Separate each component product with a space. (Thus, the list is a space-delimited set.) To specify each component product, use the mnemonic associated with that product. To display a list of the mnemonics for all the component products, use the **commpkg info --listpackages** command.
--usePkgUpgrade	If the upgrade can be performed by using a patch or an in-place package upgrade, this option uses the in-place package upgrade. The default is to use a patch to upgrade, if possible. **Note:** Patches are used only on Solaris.

verify Verb Syntax

```
commpkg verify [verb_options] [ALTROOT|name]
```

> **Tip:**
>
> When verifying the package installation in an alternate root, be aware that Convergence uses the operating system components installed in the default root. Some products might also use shared components in the default root. Thus, verify the package installation in the default root as well.

Table A-6 describes the **commpkg verify** verb options.

Table A-6 commpkg verify Options

commpkg verify Options	Description
-? or **--help**	Displays help for the verify verb.
-V or **--version**	Displays the Installer version.
--excludeOS	Do not verify operating system components.
--excludeSC	Do not verify shared components.

Table A-6 (Cont.) commpkg verify Options

commpkg verify Options	Description
--components *comp1 comp2...*	A space delimited set of component products. Each product has mnemonic associated with it. Use **commpkg info --listPackages** to see the mnemonic for a product. In most shells you need to escape the space between each mnemonic, that is, by adding double quotes around all the components.
ALTROOT|name	This option is available on Solaris only. Use this option to verify multiple instances of the product on the same host or Solaris zone. Either specify the *ALTROOT* path or the name that is registered in the software list.

info Verb Syntax

```
commpkg info [verb_options]
```

Table A-7 describes the **commpkg info** verb options.

Table A-7 commpkg info Options

commpkg info Options	Description
-? or **--help**	Displays help for the info verb.
-V or **--version**	Displays the Installer version.
--clean	Removes entries in the software list. If *installroot* is specified, the option removes the entry from the software list. If *installroot* is not specified, the option removes all entries from the software list.
--listPackages	Lists the packages that make up each Convergence, shared components, and operating system auxiliary product. This option also displays the mnemonic for Convergence and components such as **comm_dssetup.pl**.
--verbose	Prints product information installed in the *installroots*. To print information for a specific *installroot*, run the following command: **commpkg info --verbose** *installroot*
--components *comp1 comp2...*	A space delimited set of component products. Each product has mnemonic associated with it. Use **commpkg info --listPackages** to see the mnemonic for a product. In most shells you need to escape the space between each mnemonic, that is, by adding double quotes around all the components.

About the Alternate Root

You can install multiple copies of the same product version on the same Solaris machine or Solaris zone by specifying an alternate root directory when you enter **commpkg install** command. For example, you might deploy a host with an installation in the default root directory, **/opt/sun/comms**, and a second, separate installation in the **/opt/sun/comms2** alternate root directory. The alternate root installation directory is the top-level directory underneath which the Convergence component product and shared components are installed in their respective directories.

Some possible uses for multiple installations include:

1. Performing a side-by-side upgrade.
2. Enabling an installation to be easily moved from one machine to another.

> **Note:**
>
> The alternate root feature is available only on Solaris. This feature is a “power user" feature.

ALTROOT | name Syntax and Examples

You can use *ALTROOT* or *name* option with the **commpkg install**, **commpkg upgrade**, **commpkg uninstall**, and **commpkg verify** commands. You use either *ALTROOT* or *name*. The *name* acts as an alias for the alternate root installation path. The *name* is registered in an internal software list maintained by the Installer. You can use *name* in place of the alternate root's path in commands that accept the alternate root. The distinction between the alternate root and name is that the alternate root always begins with a slash (/) whereas the name does not.

Syntax:

```
commpkg verb ALTROOT|name
```

Example 1:

```
commpkg install /opt/sun/comms2
```

In this example, the path **/opt/sun/comms2** is the alternate root, which becomes the top-level directory underneath which Convergence software and shared components are installed.

Example 2:

```
commpkg install Comms2
```

In this example, **Comms2** is the name for the alternate root. During the installation process, the Installer prompts you to type in the alternate root installation directory.

Example 3:

In this example, you avoid installing the shared components in the alternate root by using the **--excludeSC** option:

```
commpkg install --excludeSC /opt/sun/comms2
```

Example 4:

To install only the shared components, run the **commpkg install** command and select the product you want to install, but prepend a tilde (~).

For example, if you plan to install Convergence in the alternate root, you select ~1 during the default installation. This tells the Installer to install the dependencies but not the product itself.

Notes on the *ALTROOT|name* option:

- Specifying a slash (/) as an alternate root is the same as specifying the default root installation directory. That is, specifying a slash is interpreted by the Installer as having specified no alternate root.

- Likewise, specifying “" as an alternate root is interpreted as having specified no alternate root. (The “friendly name" for the default alternate root is “".)
- If you specify the **--installroot** option in addition to *ALTROOT*|*name*, the two must match.
- Operating system patches are always installed into the default root (/). Some shared components are installed into the *ALTROOT* and some are installed into the default root (/).
- You can quickly uninstall an *ALTROOT* installation by using the **rm -r** command on the alternate root directory. The next time that you run the **commpkg info** command, the internal software list that maintains the alternate root information is updated.
- You can create as many alternate roots as you like. Running the **commpkg info** command reports on the various alternate roots.

Understanding the Difference Between ALTROOT and INSTALLROOT

The following concepts define an alternate root (ALTROOT):

- An alternate root directory is a Solaris feature that is used by the **commpkg** command to enable multiple product installations on the same host.
- The default alternate root is the standard root directory (/) and is always present.

The following concepts define an installation root (*InstallRoot*):

- An *InstallRoot* is the top-level umbrella installation path for Convergence.
- On the default alternate root (that is, /), you can specify an *InstallRoot*.
- On an alternate root, the *InstallRoot* is the same as the alternate root.

Default Root

If you use the default root, the default *InstallRoot* is:

/opt/sun/comms/

Using Both Default Root and Alternate Root

Suppose you want to install one instance of Convergence in the **/opt/sun/mycompany/comms/** directory, and another instance of the same product in the **/opt/sun/mycompany/comms2/** directory. You would use the following commands:

For the default root:

```
commpkg install --installroot /opt/sun/mycompany/comms
```

For the alternate root:

```
commpkg install /opt/sun/mycompany/comms2/
```

Running Multiple Installations of the Same Product on One Host: Conflicting Ports

By default, after you initially configure the product on alternate roots, the ports used by the different product installations are the same and thus conflict with each other.

This is not a problem if you install multiple installations of the same product on the same host but only intend to have one instance running at one time. For example, you may perform a side-by-side upgrade scenario in which you plan to stop the old instance before you start the new instance.

However, you may plan to test the new instance while the old instance is still running (and supporting end users). In this scenario, the ports are used simultaneously, and you need to take steps to resolve the port conflicts.

B

rundssetup Reference

Before Configuring UCS Products , you must prepare your Directory Server host. This is done by running the directory server setup script (rundssetup) against the directory Server Instance.

This appendix provides information about the rundssetup script.

Convergence release 3.0.3.0.0 is certified using Oracle Unified Directory. DS Setup 6.4.0.30.0 is required for Oracle Unified Directory support.

DS Setup version 6.4.0.30.0 uses rundssetup script which is an enhanced version of **comm_dssetup.pl** script available in earlier versions of DS Setup. This appendix provides information on rundssetup script usage to prepare Oracle Unified Directory.

Downloading and Installing DS Setup

1. Download the DS Setup from: https://support.oracle.com

   The rundssetup script is available in the same software package as the Convergence software.

2. Copy the directory server setup ZIP file to a temporary directory on your directory server hosts and extract the files.
3. Log on to the directory server host machine as the superuser (root).
4. Change to the directory where you extracted the DS Setup.
5. Install the DS Setup using:

   ```
   ./commpkg install
   ```

6. Select Comms DSsetup from the list of applications to install and proceed with the installation.

   See "commpkg Reference" for more information about the commpkg command.

About the rundssetup Script

This section provides information you need to understand before running the rundssetup script.

The rundssetup script performs the following steps:

1. Prompts you for your deployment's Directory Server and schema information.

   For a list of the specific information this step requests, see Information Needed to Run the rundssetup Script

2. Generates a shell script and LDIF file from the information that you supply that is used to modify the Directory Server LDAP.
3. Runs the generated shell script and modifies your Directory Server.

At the end of each step, the rundssetup script prompts you to continue. No changes are made to the Directory Server LDAP until the last step.

Executing rundssetup script

Prerequisite: before running DS Setup, make sure the following are installed:

- Directory Server (Oracle Unified Directory)
- Python 2.7 and above

To install Oracle Unified Directory, see Install the Oracle Unified Directory Software

For Setting up Directory Server, see Setting Up Oracle Unified Directory as a Directory Server

Make sure a Directory Server instance is already created and is started. rundssetup script can be executed in interactive mode or silent mode

To run the script for preparing OUD, run the command:

```
python rundssetup --dsType OUD
```

Answer the command-line prompts.

> **Note:**
>
> You can use either LDAP Schema 2 or Schema 1. Schema 2 is recommended.

To execute rundssetup script in silent mode, see "Running rundssetup in silent mode" below.

If the directory server is already installed at your site, users have already been provisioned. If you have just installed the directory server at your site, then you need to provision users. For information about provisioning users and schema, see Communications Suite Schema Reference.

Directory Server Considerations for the rundssetup Script

When running the rundssetup script, consider the following points.

- rundssetup configures local Directory Server instances, and thus you must:
  - Install the rundssetup script on every host on which a Directory Server instance resides.
  - Run the rundssetup script on the same host as your Directory Server. The tool runs locally for a specific instance (specified by path of Directory Server or path of instance).
- You can run the rundssetup script against any Directory Server instance on the local host. If you have multiple Directory Information Trees (DITs) on one host, you can maintain and update one installation of rundssetup, and apply it to every Directory Server instance on the host.
- rundssetup must configure every Directory Server instance for the same DIT. This assumes that:
  - A Directory Server has already been installed, configured, and is running before you launch the rundssetup script.
  - When adding an additional Directory Server host (such as a replica), at a future date, you must run the rundssetup script against it, too.

- If you have customized your Directory Server, the following considerations might apply:
  - If you have indexed some attributes, you might have to reindex those attributes after running the rundssetup script.
  - If you have added other LDIF files (schema definitions), they should not be affected, so no action should be necessary. However, back up your custom schema definition files before running the rundssetup script. The rundssetup script backs up old schema files to the **/var/tmp/dssetup_timestamp/save** directory.
  - For all Directory Server customizations, including the first two just listed, stop the rundssetup script after it generates the script and before it actually updates the LDAP directory. Then inspect the script to evaluate how its proposed actions affect your LDAP directory. Take whatever actions you think necessary to protect your customizations before running the script against your Directory Server.

Information Needed to Run the rundssetup Script

Table B-1 describes the information about your deployment that you need to gather before running the rundssetup script.

Table B-1 rundssetup Information

Information Item Needed	Default Value
Directory Server's Instance Path	The instance of Directory Server to be used (if more than one). (Absolute path of the Directory Server instance where it is running). The script displays an example of instance path of Directory Server, depending on the Directory Server type selected. The rundssetup script does attempt to heuristically determine the default. By default, the dstype is ODSEE. Example for Directory Server instance path when dstype is OUD: **/opt/oracle/Oracle/Middleware/asinst_1**
User and group root suffix	The default depends on what is detected. The rundssetup script does attempt to heuristically determine the value. For example, o=usergroup
Schema version? (pick one of the following): • 1 - Schema 1 • 1.5 - Schema 2 Compatibility Mode • 2 - Schema 2 Native Mode For more information on how to choose a schema, see "About the rundssetup Script Schema Choices". For new deployments , Schema 2 is preferred.	2
Do you want to update the schema files	Yes
Do you want to configure new indexes	Yes
Do you want to Reindex the new indexes now	Yes

Table B-1 (Cont.) rundssetup Information

Information Item Needed	Default Value
DC Tree base suffix (This option is not prompted when schema type is chosen as 2). If you choose Schema 1 or 1.5, you need a DC tree. If the DC tree does not yet exist, the rundssetup script creates only the root suffix node, its does not create the rest of the DC tree. You must create the rest of your DC tree yourself.	o=internet However, if you run rundssetup again, it defaults to the value that you chose the previous time.

About the rundssetup Script Schema Choices

Attribute Indexes Created by the rundssetup Script

Attribute indexes improve the performance of search algorithms. The rundssetup script offers you the choice to index attributes.

Table B-2 lists all the attributes the rundssetup script indexes, grouped by suffix category. It also lists the type of indexes created for each attribute. For more information about Directory Server indexing, see the Directory Server documentation at: https://docs.oracle.com/cd/E52734_01/oud/OUDAG/indexing.htm#OUDAG00048

Attribute indexes improve the performance of search algorithms. The rundssetup script offers you the choice to index attributes.

Table B-2 Attributes Indexed by rundssetup

Suffix	Attributes Indexed	Types of Indexes Added
User/Group (schema 1 & 2)	mail	'presence','equality','approximate','substring'
N/A	mailAlternateAddress	'presence','equality','approximate','substring'
N/A	mailEquivalentAddress	'presence','equality','approximate','substring'
N/A	mailUserStatus	'presence','equality'
N/A	member	'equality'
N/A	ou	'presence'
N/A	groupid	'presence','equality','substring'
N/A	uniquemember	'equality'
N/A	memberOf	'substring','equality'
N/A	cn	'equality'
N/A	mgrpUniqueId	'equality'
N/A	deleted	'presence','equality'
N/A	davuniqueid	'presence','equality'
N/A	inetCos	'equality'
User/Group (schema 2)	inetDomainBaseDN	'presence','equality'

Table B-2 (Cont.) Attributes Indexed by rundssetup

Suffix	Attributes Indexed	Types of Indexes Added
N/A	sunPreferredDomain	'presence','equality'
N/A	associatedDomain	'presence','equality'
N/A	o	'presence','equality'
N/A	mailDomainStatus	'presence','equality'
N/A	sunOrganizationAlias	'presence','equality'
DC Tree (Schema 1)	inetDomainBaseDN	'presence','equality'
(o=internet)	mailDomainStatus	'presence','equality'
N/A	inetCanonicalDomainName	'presence','equality'
New PAB (o=PiServerDb)	displayname	'presence','equality','substring'
N/A	memberOfPIBook	'equality'
N/A	memberOfPIGroup	'equality'
o=mlusers	mail	'equality'
N/A	mlsubListIdentifier	'equality'
N/A	mlsubMail	'equality'

DS Setup command line options

Table B-3 describles rundssetup command line options. All options are not mandatory. The options not specified are picked from default values. But if options are provided, they override the default ones.

Table B-3 DS Setup Command Line Options

Option and Argument	Description
-h, --help	Shows the help message and exits
--version	Show program's version number and exit
--debug	Turns on debugging output
--verbose	Verbose output
-D BINDDN, --bindDN BINDDN	DS bind DN credential, e.g. "cn=Directory Manager"
-j PASSWDFILE, --bindPasswordFile PASSWDFILE	file containing DS bind DN password, e.g. "mypasswdfile"
-i {yes,no}, --addIndex {yes,no}	add new indexes yes/no, e.g. "yes"
-R {yes,no}, --reIndex {yes,no}	execute reindexing
-d INSTLOC, --instanceLocation INSTLOC	location of DS instance, e.g. "/oracle/Oracle/Middleware/asinst_1"
-r DCTREE, --dctree DCTREE	DC tree suffix, e.g. "o=internet"
-u UGSUFFIX, --ugtree UGSUFFIX	User/Group tree suffix, e.g. "o=usergroup"
-s {yes,no}, --updateSchema {yes,no}	whether to update schema (yes/no), e.g. "yes"
-t {1,1.5,2}, --schemaType {1,1.5,2}	the schema type (1, 1.5, or 2), e.g. "2"

Table B-3 (Cont.) DS Setup Command Line Options

Option and Argument	Description
-m {yes,no}, --modifyDS {yes,no}	whether to modify the Directory Server (yes/no), e.g."yes"
-f {yes,no}, --force {yes,no}	force the application of this version of dssetup, even if the same version or later has been applied before
--silent SILENTFILE	run silently, taking the input from SILENTFILE and the command line. Command line arguments override entries in SILENTFILE. Specify NONE for the SILENTFILE if you want silent mode but with no silent file
--dsType {OUD,DSEE}	The Directory Server type, e.g. "OUD"
--createSuffixes {yes,no}	Power User switch - whether to create suffixes (yes/no), e.g. "yes", default is yes
--createSuffixDN {yes,no}	Power user switch (OUD only) - whether to create the DN associated with the suffix (yes/no). If --createSuffixes is no, then this switch is ignored (i.e. will be "no"), e.g. "yes", default is yes
--createMLusersSuffix {yes,no}	Power user switch - whether to create the o=mlusers suffix (yes/no), e.g. "yes", default is yes
--createPiServerDbSuffix {yes,no}	Power user switch - whether to create the o=mlusers suffix (yes/no), e.g. "yes", default is yes

Running the rundssetup Script in Silent Mode

To run the rundssetup script in silent mode:

1. On the host where Directory Server is installed, log in as or become the superuser(root).
2. Start Directory Server, if necessary.
3. Change to the directory where you installed or copied the Directory Server Setup rundssetup script.
4. Run the script followed by the silent mode options.

   For more information, see "Silent Mode Options".

   ```
   rundssetup [-h] [--version] [--debug] [--verbose] [-D BINDDN]

   [-j PASSWDFILE] [-i {yes,no}] [-R {yes,no}] [-d INSTLOC]

   [-r DCTREE] [-u UGSUFFIX] [-s {yes,no}] [-t {1,1.5,2}]

   [-m {yes,no}] [-f {yes,no}] [--silent SILENTFILE]

   [--dsType {OUD,DSEE}] [--createSuffixes {yes,no}]

   [--createSuffixDN {yes,no}] [--createMLusersSuffix {yes,no}]

   [--createPiServerDbSuffix {yes,no}]
   ```

   The script creates the following LDIF file and shell script to update the LDAPindexes and schema:

- **/var/tmp/dssetup_timestamp/dssetup.ldif**
- **/var/tmp/dssetup_timestamp/dssetup.sh**

5. If you answered no to the -R and -m options, you need to manually run the dssetup.sh script that was created. If you answered yes to the -R and -m options, the dssetup.sh script is runautomatically.

   For example:

   schema 2:

   ```
   rundssetup -D "cn=Directory Manager" -j /tmp/ds_pass -i yes -R yes -d /oracle/Oracle/
   Middleware/asinst_1 -u o=usergroup -s yes -t 2 -m yes -f yes --silent=NONE --
   dsType=OUD --createSuffixes yes --createSuffixDN no --createMLusersSuffix yes --
   createPiServerDbSuffix yes
   ```

   schema 1:

   ```
   rundssetup -D "cn=Directory Manager" -j /tmp/ds_pass -i yes -R yes -d /oracle/Oracle/
   Middleware/asinst_1 -r "o=internet" -u "o=usergroup" -s yes -t 1 -m yes -f yes --
   silent=NONE --dsType=OUD --createSuffixes yes --createSuffixDN no --
   createMLusersSuffix yes --createPiServerDbSuffix yes
   ```

Silent Mode Options

Following are the options supported for running in silent mode:

```
rundssetup [-h] [--version] [--debug] [--verbose] [-D BINDDN]

[-j PASSWDFILE] [-i {yes,no}] [-R {yes,no}] [-d INSTLOC]

[-r DCTREE] [-u UGSUFFIX] [-s {yes,no}] [-t {1,1.5,2}]

[-m {yes,no}] [-f {yes,no}] [--silent SILENTFILE]

[--dsType {OUD,DSEE}] [--createSuffixes {yes,no}]

[--createSuffixDN {yes,no}] [--createMLusersSuffix {yes,no}]

[--createPiServerDbSuffix {yes,no}]
```

Explanation of the above options can be seen by running:

```
./rundssetup --help
```

C
Convergence Configuration Scripts

This appendix provides information about the Oracle Communications Convergence configuration scripts.

init-config Script

The init-config script enables you to perform an initial configuration of your Convergence Server deployment. Table C-1 describes the init-config options.

Table C-1 init-config Options

Option	Description
-appserver <appsvrtype>	Specify Application Server Type. Default is weblogic
-state <statefile>	Statefile containing configuration information. The example savestate file 'saveState.example' can be used as a reference.
-nodisplay -s	Perform a silent install, requires -state option.
-saveState <statefile>	Saves all responses to named state file.
-h	Display help message

To see more about the usages of init-config:

```
 /opt/sun/comms/iwc/sbin/init-config -h
Usage:/opt/sun/comms/iwc/sbin/init-config [-appserver <appsvrtype>] [-state <statefile>]
[-nodisplay|-s] [-saveState <statefile>] [-h]
```

extractSSLArgs.sh Script

When you configure Convergence for the first time with Oracle WebLogic Server in a secure mode, run the extractSSLArgs.sh script. This script validates the SSL configuration details in Oracle WebLogic Server and stores the valid details in a format that is required by Convergence Server for all future deployments and processing.

Options

Table C-2 lists the options for validating and storing Oracle WebLogic Server SSL details.

Table C-2 WebLogicServer Options

Option	Description
-u	WebLogic Server Administrator User ID
-p	WebLogic Server Administrator User Password

Table C-2 (Cont.) WebLogicServer Options

Option	Description
-l	WebLogic Server Administrator URL t3|t3s://FQDN:Weblogic AdminServer (SSL|NonSSL)Port For example, t3://hostname.com:7001 Or t3s://hostname.com:7002

To Process the Script

Validate the SSL and Keystore configurations on WebLogic Server setup. Perform the steps in the "Installing and Configuring Oracle WebLogic Server for Convergence" section to set up WebLogic Server in a secure mode.

Keep the configuration details of WebLogic Server handy. To validate and store Oracle WebLogic Server SSL details for Convergence Server in a secure mode:

1. Open a new terminal and prepare the terminal by sourcing the setDomainEnv.sh script of the Oracle WebLogic Server domain:

   ```
   cd Weblogic_Domain/bin
   source ./setDomainEnv.sh OR . ./setDomainEnv.sh
   ```

2. Set the WLST_PROPERTIES environment variable depending on the selected Oracle WebLogic Server keystore configuration. If the Custom Identity and Custom Trust keystore option is configured as the Oracle WebLogic Server keystore configuration, set the WLST_PROPERTIES variable to:

   ```
   export WLST_PROPERTIES="-Dweblogic.security.TrustKeyStore=CustomTrust ,
   -Dweblogic.security.CustomTrustKeyStoreFileName=Weblogic_
   Domain/mytrust.jks"
   ```

   where **Weblogic_Domain/mytrust.jks** is the location of truststore file location.

   If the Custom Identity and Java Standard Trust keystore option is configured as the Oracle WebLogic Server keystore configuration, set the **WLST_PROPERTIES** variable to:

   ```
   export WLST_
   PROPERTIES="-Dweblogic.security.TrustKeyStore=JavaStandardTrust"
   ```

3. Run the **extractSSLArgs.sh** bash shell script **extractSSLArgs.sh** which is available under the Convergence Server installed location, **Convergence_Server_Installedlocation/sbin**:

   ```
   sh ./extractSSLArgs.sh -u weblogic_admin_user -p weblogic_admin_user_password
   -l t3s://weblogic_server_host:SSL_port
   ```

D

ODSEE to OUD Migration

This appendix provides information about migrating from ODSEE to OUD.

Overview

This document outlines the steps for migrating ODSEE11g deployment having DSsetup version (6.4.0.27.0 or above) to the OUD12c with DSsetup version 6.4.0.30.0. For general guidelines on transitioning from ODSEE to OUD, see the links provided under the Reference section below.

The example dealt with in this document uses the tightly coupled co-existence migration strategy and shows setting up three servers listed below.

1. ODSEE (skip if it already exists)
2. OUD
3. OUD replication gateway

For the example in this document, all these servers are set up on a single host and hence non-standard ports will be used by these servers.

> **Note:**
>
> If you already have ODSEE11g with DSsetup version (6.4.0.27.0 or above), then skip steps 1, 2, and 3 in "Migrating ODSEE Deployment to OUD".
>
> References to Hostname of this example machine have been masked as "HOSTNAME" throughout this document. Use FQDN of your machine for such references.

Assuming that the ODSEE11g deployment with DSsetup(6.4.0.27.0 or above) exists, along with the directory data, follow these steps:

- Setting ODSEE password compatibility to DS mode
- Setup an empty OUD instance
- Analyzing the ODSEE data (export ODSEE data to do the analysis)
- Migrating ODSEE schema to OUD
- Migrating ODSEE configuration to OUD
- Enable ODSEE replication
- Setup the OUD replication gateway
- Apply DSsetup 6.4.0.30.0 to update the schema on OUD
- Export ODSEE data
- Run dsreplication pre-external-initialization

- Import ODSEE data into OUD
- Run dsreplication post-external-initialization

The keys are:

- Must use an empty OUD instance
- Must use a single OUD instance (not replicated)
- Must set up the OUD replication gateway before exporting ODSEE data for import into OUD
- Must use the switches to set up the OUD replication gateway
- ODSEE must have password compatibility in DS6-mode
- ODSEE must have replication enabled

References

This document outlines the extra reference to see while transitioning to OUD.

Transition to OUD (Technical Brief and Guide)

- Transitioning from Oracle Directory Server Enterprise Edition to Oracle Unified Directory
- Oracle® Fusion Middleware Transition Guide for Oracle Unified Directory

More Information on Migration from ODSEE to OUD

This document contains resources with more online resources on the migration from ODSEE to OUD:

- Simple OUD 11g Migration Example Using Replication Gateway and "ds2oud"
- How to Install and Configure Standalone Replication Gateway (RGW) Instances With Standalone OUD Instances and ODSEE Instances

OUD 12c Documentation Library

- Planning Oracle Unified Directory Installation
- Performing OUD 12.2.1.4 Silent Installation
- Setting up OUD 12.2.1.4 as Directory Server

ODSEE 11.1.7 Documentation Library

- Oracle Directory Server Enterprise Edition

About Migration Data Cleanup and Issues

This document outlines the process of migration data cleanup and the issues that you might face during the process.

Migration steps depend on product-specific data

The entire process of migration depends on the UCS Products used in the deployment and thereby the type of data residing in the ODSEE. The steps and issues covered in this document will therefore be subjective to the sample ODSEE data used to begin this migration scenario. For each UCS Product, you must pay special attention to product-specific migration issues that might be occurring during certain steps described here, in particular at step 6 "Execute ds2oud –diagnose" and step 8 "Analyze ODSEE data" in "Migrating ODSEE Deployment to OUD".

Migrating Schema and Indexes

When analyzing the ODSEE data, several issues will be flagged by "ds2oud" tool regarding schema issues. These schema issues fall under the responsibility of DSsetup. The migration step shown in this document- where DSsetup is run against OUD - should fix all schema issues. The indexes removal step with the sample data is also shown in this document. If you encounter any issues with respect to schema or indexes, please refer to the links provided under the respective section or consult Oracle support for further assistance.

Objectclass and Attributes cleanup Issues

When ODSEE data is diagnosed against OUD Schema, there may be issues shown for unsupported Objectclass and Attributes, due to schema cleanup. Refer to the following UCS Schema Reference guides to know about the objectclass and attributes support:

- UCS 8.0 Schema Reference guide (The deprecated objectclass/attributes which were flagged as incompatible while running ds2oud step were found listed in this guide)
- UCS 8.1 Schema Reference guide (Refer to this guide to read about various objectclasses and attributes)

For UCS Product-specific support or issues, refer to the respective product documentation or consult Oracle support for further assistance.

Prerequisites

These are the prerequisites for the process of migration:

- ODSEE must be version 11.1.1.7.0 or greater
- ODSEE password compatibility must be set to DS6 mode
- Create the file /tmp/passwd containing your password
- DSsetup version 6.4.0.27.0 or above (to be applied on ODSEE) (For the example in this document, 6.4.0.29.0 is used)
- DSsetup version 6.4.0.30.0 (to be applied on OUD)
- OUD version 11g or 12c (As of this document, OUD 12.2.1.4 has been certified)

Ports used in the Migration Example

In this example deployment, the following ports are used for servers setup on a single machine:

N/A	LDAP	LDAPS	ADMIN	SYNC
OUD DS	1389	1636	1444	1989
OUD Repl GW	1390	1637	1445	N/A
ODSEE DS	1393	1640	N/A	N/A

Migrating ODSEE Deployment to OUD

To migrate from ODSEE deployment to OUD, follow these steps:

1. **Installing ODSEE and creating an instance**

   If you already have ODSEE, you may skip this step.

   a. **Install ODSEE bits**

      - **cd /opt**
      - **unzip -q /export/ODSEE_ZIP_Distribution/sun-dsee7.zip**

      Sample Session

      ```
      # cd /opt

      # unzip -q /export/ODSEE_ZIP_Distribution/sun-dsee7.zip
      ```

   b. **Create ODSEE instance**

      - **/opt/dsee7/bin/dsadm create –port 1393 –secure-port 1640 –pwd-file /tmp/passwd /var/opt/sun/directory/ds7**
      - **/opt/dsee7/bin/dsadm start /var/opt/sun/directory/ds7**

      Sample Session

      ```
       # /opt/dsee7/bin/dsadm create --port 1393 --secure-port 1640 --pwd-
      file /tmp/passwd /var/opt/sun/directory/ds7

       Use command 'dsadm start '/var/opt/sun/directory/ds7'' to start the
      instance

       # /opt/dsee7/bin/dsadm start /var/opt/sun/directory/ds7

       Directory Server instance '/var/opt/sun/directory/ds7' started:
      pid=3295
      ```

2. **Install and run DSsetup 6.4.0.29.0**

   If you already have ODSEE with DSsetup 6.4.0.27.0 or above, then you may skip this step. In this example, here we are setting up DSsetup 6.4.0.29.0 for the ODSEE installed in the above step.

   a. Run **commpkg install** to install DSsetup 6.4.0.29.0.

   b. Run **/opt/sun/comms/dssetup/sbin/comm_dssetup.pl**.

   Sample Summary

Here is a sample summary from the **comm_dssetup.pl**.

```
Server Root                  : /var/opt/sun/directory

Server Instance              : ds7

Users/Groups Directory       : yes

Update Schema                : yes

Schema Type                  : 2

DC Root                      : o=usergroup

User/Group Root              : o=usergroup

Add New Indexes              : yes

ReIndex New Indexes Now      : yes

Directory Manager DN         : cn=Directory Manager
```

3. **UCS Products setup with ODSEE and Provisioning**

   If you already have UCS Products configured to backend ODSEE(having DSsetup 6.4.0.27.0 or above), along with existing domains/users/groups provisioned, then you may skip this step. At this stage, we can install and configure any required UCS products pointing to the ODSEE setup above. Refer to the respective product documentation for configuring UCS products. Then, provision the domains/users/groups required in ODSEE (populating ODSEE with data). If you have this data already in a valid LDIF format, then you may populate it into ODSEE as shown in the example below:

   Example: Populated ODSEE with data

   ```
   ldapmodify -D 'cn=Directory Manager' -j /tmp/passwd -h <HOSTNAME> -p 1393 -a -f /
   shared/resources/ucs_data.ldif
   ```

   As another example, shown below is the basic setup of Messaging Server(MS) product and also a sample "testuser1" created:

   - Unzip the Messaging Server ZIP file downloaded from MOS.
   - **./commpkg install**
   - **/opt/sun/comms/messaging64/bin/configure –ldapport=1393**
   - **/opt/sun/comms/messaging64/lib/inetuser create -D 'cn=Directory Manager' -j /tmp/passwd testuser1**

   > **Note:**
   >
   > If you installed a UCS product whose version does not support OUD yet, then the next steps are to perform specific steps for that product and then upgrade that product to a version that supports OUD. Refer UCS Product documentation for product-specific install or upgrade instructions.

4. **Change ODSEE password compatibility to DS6 mode**

Execute the following commands:

```
/opt/dsee7/bin/dsconf pwd-compat -port 1393 -accept-cert -user-dn 'cn=Directory
Manager' -pwd-file /tmp/passwd to-DS6-migration-mode

/opt/dsee7/bin/dsconf pwd-compat -port 1393 -accept-cert -user-dn 'cn=Directory
Manager' -pwd-file /tmp/passwd to-DS6-mode
```

Sample session

```
# /opt/dsee7/bin/dsconf pwd-compat --port 1393 --accept-cert --user-dn 'cn=Directory
Manager' --pwd-file /tmp/passwd to-DS6-migration-mode

## Beginning password policy compatibility changes.

## Password policy compatibility changes finished.

 Task completed (slapd exit code: 0).

 # /opt/dsee7/bin/dsconf pwd-compat --port 1393 --accept-cert --user-dn
'cn=Directory Manager' --pwd-file /tmp/passwd to-DS6-mode

 ## Beginning password policy compatibility changes.

 ## Password policy compatibility changes finished.

 Task completed (slapd exit code: 0).
```

5. **Install OUD and setup OUD Instance**

   a. **Installation of OUD**

      In this document example, the OUD 12.2.1.4.0 has been installed in Standalone mode.

   b. **OUD Instance setup**

      /opt/oracle/Oracle/Middleware/Oracle_OUD1/oud-setup --cli --no-prompt --rootUserPasswordfile /tmp/passwd --ldapPort 1389 --ldapsPort 1636 --adminConnectorPort 1444 --generateSelfSignedCertificate

      Sample Session

```
 #/opt/oracle/Oracle/Middleware/Oracle_OUD1/oud-setup --cli --no-prompt --
rootUserPasswordfile /tmp/passwd --ldapPort 1389 --ldapsPort 1636 --
adminConnectorPort 1444 --generateSelfSignedCertificate

 Oracle Unified Directory 12.2.1.4.0

 Please wait while the setup program initializes...

 Creating instance directory /opt/oracle/Oracle/Middleware/asinst_1/OUD .....
Done.

 See /opt/oracle/Oracle/Middleware/asinst_1/OUD/logs/oud-setup for a detailed
log of this operation.



Configuring Directory Server ..... Done.

Configuring Certificates ..... Done.

Starting Directory Server ....... Done.
```

```
    To see basic server configuration status and configuration you can launch /opt/
    oracle/Oracle/Middleware/asinst_1/OUD/bin/status
```

6. **Execute ds2oud –diagnose**

   This step diagnoses the ODSEE data for OUD migration problems, using "ds2oud".

   ds2oud -diagnose:

   /opt/oracle/Oracle/Middleware/asinst_1/OUD/bin/ds2oud --diagnose --odseeBindDN 'cn=Directory Manager' --odseeHostname <HOSTNAME> --odseePort 1393 --odseeBindPasswordFile /tmp/passwd --no-prompt

   Sample Session

```
# /opt/oracle/Oracle/Middleware/asinst_1/OUD/bin/ds2oud --diagnose --odseeBindDN
'cn=Directory Manager' --odseeHostname <HOSTNAME> --odseePort 1393 --
odseeBindPasswordFile /tmp/passwd --no-prompt

 ********************************************************************************

 Diagnose ODSEE Server : <HOSTNAME>:1393

 ********************************************************************************

 <...output snipped...>

 ** Encrypted attributes

 No encrypted attributes are defined, no action is required
```

7. **Export ODSEE data to ldif**

   run dsconf export

```
/opt/dsee7/bin/dsconf export --accept-cert --user-dn 'cn=Directory Manager' --pwd-
file /tmp/passwd -f opends-export -f output-not-folded -h <HOSTNAME> -p 1393
o=usergroup o=mlusers o=PiServerDb odsee-data.ldif
```

> **Note:**
>
> - **-f opends-export**: is used to have it suitable for import-ldif later on OUD side. However, do not use the data from this **run/step** for **import-ldif**. After the replication gateway is setup the data will be exported and that must be used for **import-ldif**.
> - Do not include **o=comms-config**.
> - **-f output-not-folder** option: This is to avoid line folding. If not given, export causes bigger lines to get folder into multiple lines - which leads to issues while doing search/replace in data cleanup steps later (if required to clean ODSEE ldif data)
> - **o=usergroup**: is the user/group suffix considered in this sample. Ensure to include your suffix accordingly.
> - **o=mlusers**: this is for MS mailing lists
> - The case above is schema 2 (see output of DSsetup run). For schema 1, add for example o=internet (typically DC tree).

Sample Session

```
# /opt/dsee7/bin/dsconf export --accept-cert --user-dn 'cn=Directory Manager' --pwd-
file /tmp/passwd -f opendsexport -f output-not-folded -h <HOSTNAME> -p 1393
o=usergroup o=mlusers o=PiServerDb odsee-data.ldif

 ## Beginning export of 'usergroupdb2'

 ## usergroupdb2: Start processing.

 ## usergroupdb2: Processed 123 entries (100%), 123.0 entries/sec average, 123
exported.

 ## Beginning export of 'mlusersdb2'

 ## mlusersdb2: Start processing.

 ## mlusersdb2: Processed 1 entries (100%), 1.0 entries/sec average, 1 exported.

 ## Beginning export of 'PiServerDbdb2'

 ## PiServerDbdb2: Start processing.

 ## PiServerDbdb2: Processed 36 entries (100%), 36.0 entries/sec average, 36
exported.

 ## Export finished.
```

8. **Analyze ODSEE data**

   a. **Move odsee-data.ldif to an accessible location**

      - `cp /var/opt/sun/directory/ds7/logs/odsee-data.ldif /tmp`
      - If it is on a different machine, set permissions (chmod the file) and then:
        – `scp <HOSTNAME>:/var/opt/sun/directory/ds7/logs/odsee-data.ldif /tmp`

   b. **run ds2oud –ldifDBFile**

```
/opt/oracle/Oracle/Middleware/asinst_1/OUD/bin/ds2oud --ldifDBFile /tmp/odsee-
data.ldif --userSchemaFile /opt/sun/comms/dssetup/lib/foranalysis-oud-schema.ldif
```

If it shows any incompatible objectclass/attributes, then cleanup those from ODSEE LDIF data. Refer to the UCS Schema Reference guides provided in the section above "Objectclass and Attributes cleanup Issues" to know such deprecated information. This run might also show any unsupported/invalid keyword. Must fix the LDIF data by replacing those invalid keywords accordingly with the suggested keyword in the output. See the sample session below:

Sample Session

```
********************************************************************************
* Diagnose ODSEE LDIF data file : /tmp/odsee-data.ldif
********************************************************************************

Error validating data against OUD schema
Entry : unknown
org.opends.sdk.DecodeException: Entry o=usergroup read from LDIF starting at
line 8 includes value "(target="ldap:///o=usergroup")(targetattr="*")(version
3.0;acl "Contacts Server End User Administrator Proxy Rights -
product=nabserver,schema 2 support,class=admin,num=1,version=1"; allow (proxy)
roledn="ldap:///cn=Contacts End User Administrators Group, ou=Groups,
o=usergroup";)" for attribute aci that is invalid according to the
associated syntax: The provided Access Control Instruction (ACI) expression
```

```
value "ldap:///cn=Contacts End User Administrators Group, ou=Groups,
o=usergroup" is invalid because it contains the roledn keyword, which is not
supported, replace it with the groupdn keyword
```

> **Note:**
>
> Following replacements were required during this run with our test data:
>
> - Replaced **roledn** with **groupdn**
> - Replaced **groupdnattr** with **groupdn**

9. **Install DSsetup 6.4.0.30.0 for OUD**

   Install DSsetup 6.4.0.30.0

   On the machine where OUD is residing, download DSsetup 6.4.0.30.0 and configure this DSsetup version with OUD.

   - Download DSsetup 6.4.0.30.0 and unzip the ZIP obtained.
   - Run **commpkg install**

10. **Run DSsetup 6.4.0.30.0 on OUD to install just the schema**

    Run DSsetup 6.4.0.30.0 as shown below, to install just the schema on the OUD instance. It is important that this step be done prior to running migrateUserSchema, which migrates the ODSEE schema into OUD. (Note: Observation - If this step is not done, then the schema attribute such as "iplanet-am-managed-group" could show up twice in 99-user.ldif on the OUD side).

    rundssetup command:

    ```
    bin/rundssetup --dsType=OUD \

      --instanceLocation /opt/oracle/Oracle/Middleware/asinst_1 \

      --bindPasswordFile /tmp/passwd \

      --updateSchema yes \

      --createSuffixes no \

      --silent NONE \

      --modifyDS yes
    ```

11. **Process ds2oud migrateUserSchema(optional)**

    This will migrate ODSEE schema into OUD. This is an optional step. In fact, we would recommend not doing it and seeing if entries have an illegal schema, and correct them. Schema violations would occur during the import-ldif step.

    a. **Run ds2oud –migrateUserSchema**

       ```
       /opt/oracle/Oracle/Middleware/asinst_1/OUD/bin/ds2oud --migrateUserSchema --
       odseeBindDN "cn=Directory Manager" --odseeHostname <HOSTNAME> --odseePort 1393 --
       odseeBindPasswordFile /tmp/passwd --oudBindDN "cn=Directory Manager" --
       oudHostname <HOSTNAME> --oudPort 1389 --oudBindPasswordFile /tmp/passwd --
       oudAdminPort 1444 --no-prompt
       ```

> **Note:**
>
> This might take all the ODSEE user schema into OUD, including obsolete schema.

b. **Note about extra schema files in config/schema**

   Note that there were no schema files in config/schema prior to running the command, and after there is only **99-user.ldif**. Running DSsetup later pulls in some other files into the config/schema area due to overwriting of OUD default schema. The various files are: **00-core.ldif**, **05-solaris.ldif** , and **05-oraclefa.ldif**. The middlename is in **05-oraclefa.ldif**, the location is in **00-core.ldif**, the mail rfc822mailbox is in **00-core.ldif**, and the mgrpRFC822MailMember is in **05-solaris.ldif**.

   In a pristine (fresh) OUD instance:

```
attributeTypes: ( 2.16.840.1.113894.200.1.3 NAME 'middleName' SUP name SINGLE-
VALUE USAGE userApplications )
attributeTypes: ( 1.3.6.1.4.1.26027.2.1.71 NAME 'location' SYNTAX
1.3.6.1.4.1.26027.2.5.2 SINGLE-VALUE X-ORIGIN 'OUD' )
attributeTypes: ( 0.9.2342.19200300.100.1.3 NAME ( 'mail' 'rfc822Mailbox' )
EQUALITY caseIgnoreIA5Match SUBSTR caseIgnoreIA5SubstringsMatch
SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{256} X-ORIGIN 'RFC 4524' )

attributeTypes: ( 2.16.840.1.113730.3.1.30 NAME 'mgrpRFC822MailMember' SYNTAX
1.3.6.1.4.1.1466.115.121.1.15 X-ORIGIN 'Solaris Specific' )
attributeTypes: ( 2.5.4.41 NAME 'name' EQUALITY caseIgnoreMatch SUBSTR
caseIgnoreSubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 {32768} X-ORIGIN
'RFC 4519' )
```

   It is recommended to use the OUD default schema for such items.

> **Note:**
>
> The change for the middle name, location, and mgrpRFC822MailMember. The location and mgrpRFC822Mailmmember are identical to UCS definitions. The middle name is slightly different but will go with the OUD default. However, for mail, you need to use the UCS definition since it defines its syntax to be UTF-8 for EAI (Email Address Internationalization) reasons. So 00-core.ldif appears in config/schema along with 99-user.ldif only once that is done.

12. **Process migrateConfiguration**

    This will generate a script to migrate the ODSEE configuration to OUD using "dsconf".

    a. Run **ds2oud –migrateConfiguration**

```
/opt/oracle/Oracle/Middleware/asinst_1/OUD/bin/ds2oud --migrateConfiguration --
odseeBindDN "cn=Directory Manager" --odseeHostname <HOSTNAME> --odseePort 1393 --
odseeBindPasswordFile /tmp/passwd --oudBindDN "cn=Directory Manager" --
oudHostname <HOSTNAME> --oudPort 1389 --oudBindPasswordFile /tmp/passwd --
oudAdminPort 1444 --batchFile /tmp/migrate-config --no-prompt
```

Note:

- If you run without –no-prompt

  DELETE if it asks to create index displayName on piserverdb - say NO

  DELETE if it asks to create index cosspecifier on usergroup - say NO

  DELETE if it asks to create index inetDomainBaseDN on usergroup - say NO
- For schema 1, **inetDomainBaseDN** would be on the DC tree "internet" instead of "usergroup"

b. Edit /tmp/migrate-config

With –no-prompt, edit the migrate-config file and remove the following cases:

i. displayName

ii. cosspecifier

iii. inetDomainBaseDN

iv. icsCalendarOwned

Sample Session

```
# /opt/oracle/Oracle/Middleware/asinst_1/OUD/bin/ds2oud --migrateConfiguration --
odseeBindDN 'cn=Directory Manager' --odseeHostname <HOSTNAME> --odseePort 1393 --
odseeBindPasswordFile /tmp/passwd --oudBindDN'cn=Directory Manager' --
oudHostname <HOSTNAME> --oudPort 1389 --oudBindPasswordFile /tmp/passwd --
oudAdminPort 1444 --batchFile /tmp/migrate-config --no-prompt
** Naming context(s) available on the ODSEE server :
o=comms-config
o=mlusers
o=pab
o=PiServerDb
o=usergroup
Creation of naming context o=comms-config
Creation of naming context o=mlusers
Creation of naming context o=pab
Creation of naming context o=PiServerDb
Creation of naming context o=usergroup
** Global Configuration Parameters
Configuration of the Global Parameters
** Global ACIs
No action was required, the default OUD configuration applies
** Indexes
<...output snipped...>
** Default Build-in Plugins
** Default Password Policy
Configuration of the Default Password Policy
```

Sample Session

Edited **/tmp/migrate-config** to fix the following:

```
sed -e /inetDomainBaseDN/d -e /cosspecifier/d -e /displayname/d -e /
icsCalendarOwned/d /tmp/migrate-config > /tmp/migrate-config.new
```

After all such replacements that was required, move/rename this **migrate-config.new** as latest **/tmp/migrate-config** for operations in the next steps.

13. **Process migrate-config**

    Run **dsconf -F migrate-config**

    ```
    /opt/oracle/Oracle/Middleware/asinst_1/OUD/bin/dsconfig -F /tmp/migrate-config -n -X
    -p 1444 -D "cn=Directory Manager" -j /tmp/passwd
    ```

    > **Note:**
    >
    > This command creates naming contexts and indexes.

    ### Sample Session

    ```
    # /opt/oracle/Oracle/Middleware/asinst_1/OUD/bin/dsconfig -F /tmp/migrate-config -n -
    X -p 1444 -D 'cn=Directory Manager' -j /tmp/passwd

    create-workflow-element --set base-dn:o=comms-config --set enabled:true --type db-
    local-backend --element-name comms-config -n create-workflow --set base-dn:o=comms-
    config --set enabled:true --set workflow-element:comms-config --workflow-name comms-
    config_workflow -n set-network-group-prop --group-name network-group --add
    workflow:comms-config_workflow -n

    create-workflow-element --set base-dn:o=mlusers --set enabled:true --type db-local-
    backend --element-name mlusers -n create-workflow --set base-dn:o=mlusers --set
    enabled:true --set workflow-element:mlusers --workflow-name mlusers_workflow -n set-
    network-group-prop --group-name network-group --add workflow:mlusers_workflow -n

    create-workflow-element --set base-dn:o=pab --set enabled:true --type db-local-
    backend --element-name pab -n create-workflow --set base-dn:o=pab --set enabled:true
    --set workflow-element:pab --workflow-name pab_workflow -n set-network-group-prop --
    group-name network-group --add workflow:pab_workflow -n

    create-workflow-element --set base-dn:o=PiServerDb --set enabled:true --type db-
    local-backend --element-name PiServerDb -n create-workflow --set base-
    dn:o=PiServerDb --set enabled:true --set workflow-element:PiServerDb --workflow-name
    PiServerDb_workflow -n set-network-group-prop --group-name network-group --add
    workflow:PiServerDb_workflow -n

    create-workflow-element --set base-dn:o=usergroup --set enabled:true --type db-local-
    backend --element-name usergroup -n create-workflow --set base-dn:o=usergroup --set
    enabled:true --set workflow-element:usergroup --workflow-name usergroup_workflow -n
    set-network-group-prop --group-name network-group --add workflow:usergroup_workflow -
    n

     <...output snipped...>
    ```

14. **List OUD backends**

    Run tests

    - `/opt/oracle/Oracle/Middleware/asinst_1/OUD/bin/list-backends`
    - `/opt/oracle/Oracle/Middleware/asinst_1/OUD/bin/status -sn`
    - **ldapsearch:**

      ```
      /opt/oracle/Oracle/Middleware/asinst_1/OUD/bin/ldapsearch -T -X -h HOSTNAME -p
      1389 -D 'cn=Directory Manager' -j /tmp/passwd -b 'o=usergroup' -s sub
      '(objectclass=*)'
      ```

    ### Sample Search

```
# /opt/oracle/Oracle/Middleware/asinst_1/OUD/bin/list-backends

Backend ID : Base DN

---------------:------------------

 PiServerDb : o=PiServerDb

 adminRoot : cn=admin data

 ads-truststore : cn=ads-truststore

 backup : cn=backups

 comms-config : o=comms-config

 mlusers : o=mlusers

 monitor : cn=monitor

 pab : o=pab

 schema : cn=schema

 tasks : cn=tasks

 usergroup : o=usergroup

 virtualAcis : cn=virtual acis

 # /opt/oracle/Oracle/Middleware/asinst_1/OUD/bin/status -sn

Server Run Status: Started

Open Connections: 0

Host Name: <HOSTNAME>

Administrative Users: cn=Directory Manager

Installation Path: /opt/oracle/Oracle/Middleware/oud

Instance Path: /opt/oracle/Oracle/Middleware/asinst_1/OUD

Version: Oracle Unified Directory 12.2.1.4.0

<...output snipped...>
```

15. **Enable replication on ODSEE**

    Enable ODSEE replication, but do not create a replication agreement syntax: **dsconf enable-repl -h host -p port -d ReplicaID master suffix-DN**. Run the command for each suffix.

    - **/opt/dsee7/bin/dsconf enable-repl -p 1393 –pwd-file /tmp/passwd -d 1 master o=usergroup**
    - **/opt/dsee7/bin/dsconf enable-repl -p 1393 –pwd-file /tmp/passwd -d 1 master o=mlusers**
    - **/opt/dsee7/bin/dsconf enable-repl -p 1393 –pwd-file /tmp/passwd -d 1 master o=PiServerDb**

- For schema 1 only: **/opt/dsee7/bin/dsconf enable-repl -p 1393 –pwd-file /tmp/passwd -d 1 master o=internet**

Sample Session

```
# /opt/dsee7/bin/dsconf enable-repl -p 1393 --pwd-file /tmp/passwd -d 1 master
o=usergroup

Use "dsconf create-repl-agmt" to create replication agreements on "o=usergroup".

# /opt/dsee7/bin/dsconf enable-repl -p 1393 --pwd-file /tmp/passwd -d 1 master
o=mlusers

Use "dsconf create-repl-agmt" to create replication agreements on "o=mlusers".

# /opt/dsee7/bin/dsconf enable-repl -p 1393 --pwd-file /tmp/passwd -d 1 master
o=PiServerDb

Use "dsconf create-repl-agmt" to create replication agreements on "o=PiServerDb".
```

16. **Setup the OUD replication gateway**

Run oud-replication-gateway-setup.

> **Note:**
>
> For schema 1 add: **–baseDN o=internet**

```
/opt/oracle/Oracle/Middleware/Oracle_OUD1/oud-replication-gateway-setup --cli --
hostname <HOSTNAME> --adminConnectorPort 1445 --replicationPortForLegacy 1390 --
rootUserDN "cn=Directory Manager" --rootUserPasswordFile /tmp/passwd --baseDN
o=usergroup --baseDN o=mlusers --baseDN o=PiServerDb --hostNameLegacy <HOSTNAME> --
portLegacy 1393 --doNotUpdateTrustStoreWithLegacyCertsArg --bindDNLegacy
"cn=Directory Manager" --bindPasswordFileLegacy /tmp/passwd --hostNameNg <HOSTNAME>
--portNg 1444 --adminUID admin --adminPasswordFile /tmp/passwd --trustAll --no-
prompt --noPropertiesFile --doNotMonitorUsingDsccLegacy --replicationPortNg 1989 --
verbose --bindDNNg 'cn=Directory Manager' --bindPasswordFileNg /tmp/passwd
```

Sample Session

```
#/opt/oracle/Oracle/Middleware/oud/oud-replication-gateway-setup --cli --hostname
localhost --adminConnectorPort 2445 --replicationPortForLegacy 1391 --rootUserDN
"cn=Directory Manager" --rootUserPasswordFile /tmp/passwd --baseDN o=usergroup --
baseDN o=mlusers --baseDN o=PiServerDb --hostNameLegacy localhost --portLegacy 1389
--doNotUpdateTrustStoreWithLegacyCertsArg --bindDNLegacy "cn=Directory Manager" --
bindPasswordFileLegacy /tmp/passwd --hostNameNg localhost --portNg 1444 --adminUID
admin --adminPasswordFile /tmp/passwd --trustAll --noPropertiesFile --
doNotMonitorUsingDsccLegacy --replicationPortNg 1989 --verbose --bindDNNg
'cn=Directory Manager' --bindPasswordFileNg /tmp/passwd

Oracle Unified Directory 12.2.1.4.0

Please wait while the replication gateway setup program initializes ..... Done.

Once the setup of the replication gateway will be completed (if not already done)
you have to initialize the contents of the Oracle Unified Directory servers with the
contents of the ODSEE server for replication to work.

You can follow these steps to synchronize the contents of the replicated base DNs:
```

1. Run the following command in the ODSEE host (<HOSTNAME>):

```
dsadm export \

-f opends-export \

/var/opt/sun/directory/ds7 \

o=usergroup \

o=mlusers \

o=PiServerDb \

{exportedLDIFPath}
```

Where {exportedLDIFPath} is the path of the resulting LDIF file containing the replicated data.

2. Run the following command:

```
<instancePath>/bin/dsreplication pre-external-initialization \

--hostname <HOSTNAME> \

--port 1444 \

--adminUID admin \

--adminPasswordFile ****** \

--baseDN o=usergroup \

--baseDN o=mlusers \

--baseDN o=PiServerDb \

--trustAll \

--no-prompt \

--noPropertiesFile
```

3. Copy the LDIF file generated in the first step in a directory accessible by the Oracle Unified Directory servers and run the following command for every Oracle Unified Directory server that contains data to be replicated:

```
<instancePath>/bin/import-ldif \

--hostname <HOSTNAME> \

--port 1444 \

--bindDN cn=Directory\ Manager \

--bindPasswordFile ****** \

--includeBranch o=usergroup \

--includeBranch o=mlusers \

--includeBranch o=PiServerDb \
--ldifFile {exportedLDIFPath} \

--clearBackend \

--trustAll \

--noPropertiesFile

4. Run the following command:

<instancePath>/bin/dsreplication post-external-initialization \

--hostname <HOSTNAME> \

--port 1444 \

--adminUID admin \

--adminPasswordFile ****** \

--baseDN o=usergroup \

--baseDN o=mlusers \

--baseDN o=PiServerDb \

--trustAll \

--no-prompt \

--noPropertiesFile

<...output snipped...>

The replication gateway setup has completed successfully
```

17. **Global admin is created**

    The "global admin" is created when you run **oud-replication-gateway-setup**. You can verify that by doing a **ldapsearch** for **cn=admin**, **cn=Administrators**, and **cn=admin data**.

    Run **ldapsearch**.

    ```
    /opt/oracle/Oracle/Middleware/Oracle_OUD1/bin/ldapsearch -T -X -h <HOSTNAME> -p 1444
    -D 'cn=Directory Manager' -j /tmp/passwd --useSSL -b 'cn=Administrators,cn=admin
    data' -s sub '(objectclass=*)'
    ```

Sample Session

```
 # /opt/oracle/Oracle/Middleware/Oracle_OUD1/bin/ldapsearch -T -X -h HOSTNAME -p
1444 -D 'cn=Directory Manager' -j /tmp/passwd --useSSL -b
'cn=Administrators,cn=admin data' -s sub '(objectclass=*)'
'cn=Administrators,cn=admin data' -s sub '(objectclass=*)'

 dn: cn=Administrators,cn=admin data

objectClass: top

objectClass: groupofurls

description: Group of identities which have full access.
```

```
cn: Administrators

memberURL: ldap:///cn=Administrators,cn=admin data??one?(objectclass=*)



dn: cn=admin,cn=Administrators,cn=admin data

userPassword: {SSHA512}YvhmnmRBgN8sAQHFffwTTd4XR0JT+U2GtN4kx3L9a6uBO68uKpqGiifL\

/kV3XdyzaUjjcJsPts9DA6mPaRj55URa5aHkaGTX

objectClass: person

objectClass: top

description: The Administrator that can manage all the server instances.

 <...output snipped...>
```

18. **Process DSsetup 6.4.0.30.0 to pull in the corrected schema**

    This is the second run of DSsetup 6.4.0.30.0 (the first time was in Step 16 above). Note that you must run DSsetup 6.4.0.30.0 at least once before import-ldif, otherwise entries are not pulled in due to schema violations. It is important that you match the schema type and u/g suffix that exists on the ODSEE side.

    > **Note:**
    >
    > For schema 1: specify **–schemaType 1 –dctree o=internet**

    ```
    rundssetup
    bin/rundssetup --dsType=OUD\

     --instanceLocation /opt/oracle/Oracle/Middleware/asinst_1 \

     --bindPasswordFile /tmp/passwd \

     --schemaType 2 \

     --addIndex no \

     --reIndex no \

     --ugtree o=usergroup \

     --updateSchema yes \

     --modifyDS yes
    ```

19. **Export ODSEE data to ldif Again and Cleanup/prepare**

    Must do this export again after **oud-replication-gateway-setup** was run (as it is known to update ODSEE). Hence must use this exported ODSEE data after you run **oud-replication-gateway-setup**. Recheck using **ds2oud** and fix any invalid entries. Ensure this ldif file is validated successfully against OUD Schema and is ready for import in the next steps.

    a. **Run dsconf export**

Note:

For schema 1 add: **o=internet**. Also use "output-not-folder" option when running this export command, so that data is exported without folding/ truncation (it enables correct search/ replace in the next steps).

```
/opt/dsee7/bin/dsconf export --accept-cert --user-dn 'cn=Directory Manager' --
pwd-file /tmp/passwd -f opends-export -f output-not-folded -h <HOSTNAME> -p 1393
o=usergroup o=mlusers o=PiServerDb odsee-data2.ldif
```

b. **Copy it to /tmp , Cleanup and Check ds2oud**

```
cp /var/opt/sun/directory/ds7/logs/odsee-data2.ldif /tmp/
odsee_before_roledn_rep.ldif

 Fixed any occurrences of "roledn" or "groupdnattr" :

 sed "s@) roledn@) groupdn@;s@) groupdnattr@) groupdn@;s@)roledn@)groupdn@;s@and
roledn@and groupdn@;s@or

 roledn@or groupdn@" /tmp/odsee_before_roledn_rep.ldif > /tmp/odsee-data2.ldif

 Ran ds2oud :

 /opt/oracle/Oracle/Middleware/asinst_1/OUD/bin/ds2oud --ldifDBFile /tmp/odsee-
data2.ldif --userSchemaFile /opt/sun/comms/dssetup/lib/foranalysis-oud-
schema.ldif
```

Note:

Diagnose ODSEE LDIF data file: **/tmp/odsee-data2.ldif**

The data was validated successfully regarding the OUD schema. This file **/tmp/odsee-data2.ldiff** is now ready for import into OUD.

20. **Run dsreplication pre-external-initialization**

for schema 1: add **–baseDN o=internet**.

```
/opt/oracle/Oracle/Middleware/asinst_1/OUD/bin/dsreplication pre-external-
initialization --hostname <HOSTNAME> --port 1444 --adminUID admin --
adminPasswordFile /tmp/passwd --baseDN o=usergroup --baseDN o=mlusers --baseDN
o=PiServerDb --trustAll --no-prompt --noPropertiesFile
```

Sample Session

```
# /opt/oracle/Oracle/Middleware/asinst_1/OUD/bin/dsreplication pre-external-
initialization --hostname <HOSTNAME> --port 1444 --adminUID admin --
adminPasswordFile /tmp/passwd --baseDN o=usergroup --baseDN o=mlusers --baseDN
o=PiServerDb --trustAll --no-prompt --noPropertiesFile

Establishing connections ..... Done.

Preparing base DN o=mlusers to be initialized externally ..... Done.

Preparing base DN o=PiServerDb to be initialized externally ..... Done.
Preparing base DN o=usergroup to be initialized externally ..... Done.

Now you can proceed to the initialization of the contents of the base DN's on all
the replicated servers. You can use the command import-ldif or the binary copy to do
so. You must use the same LDIF file or binary copy on each server.

 When the initialization is completed you must use the subcommand 'post-external-
initialization' for replication to work with the new base DN's contents.

 See /var/tmp/oud-replication-3459260775445051714.log for a detailed log of this
operation.
```

21. **Execute import-ldif into OUD**

    The ODSEE data prepared above **/tmp/odsee-data2.ldiff** is now imported into OUD, using the respective backend IDs.

    a. Run list-backends to find out Backend ID to use for **import-ldif**

    ```
    /opt/oracle/Oracle/Middleware/asinst_1/OUD/bin/list-backends
    ```

    ### Sample Session

    ```
    # /opt/oracle/Oracle/Middleware/asinst_1/OUD/bin/list-backends
    Backend ID : Base DN
    ---------------:------------------
    PiServerDb : o=PiServerDb
    adminRoot : cn=admin data
    ads-truststore : cn=ads-truststore
    backup : cn=backups
    comms-config : o=comms-config
    mlusers : o=mlusers
    monitor : cn=monitor
    pab : o=pab
    schema : cn=schema
    tasks : cn=tasks
    usergroup : o=usergroup
    virtualAcis : cn=virtual acis
    ```

    b. Run **import-ldif**

    > **Note:**
    >
    > Use backendID obtained from list-backends above.

    ```
    /opt/oracle/Oracle/Middleware/asinst_1/OUD/bin/import-ldif --hostname <HOSTNAME>
    --port 1444 --bindDN cn=Directory\ Manager --bindPasswordFile /tmp/passwd --
    includeBranch o=usergroup --backendID usergroup --ldifFile /tmp/odsee-data2.ldif
    --clearBackend --trustAll --noPropertiesFile

    /opt/oracle/Oracle/Middleware/asinst_1/OUD/bin/import-ldif --hostname <HOSTNAME>
    --port 1444 --bindDN cn=Directory\ Manager --bindPasswordFile /tmp/passwd --
    includeBranch o=mlusers --backendID mlusers --ldifFile /tmp/odsee-data2.ldif --
    clearBackend --trustAll --noPropertiesFile

    /opt/oracle/Oracle/Middleware/asinst_1/OUD/bin/import-ldif --hostname <HOSTNAME>
    --port 1444 --bindDN cn=Directory\ Manager --bindPasswordFile /tmp/passwd --
    includeBranch o=PiServerDb --backendID PiServerDb --ldifFile /tmp/odsee-
    data2.ldif --clearBackend --trustAll --noPropertiesFile
    ```

    For schema 1 only:

```
/opt/oracle/Oracle/Middleware/asinst_1/OUD/bin/import-ldif --hostname <HOSTNAME>
--port 1444 --bindDN cn=Directory\ Manager --bindPasswordFile /tmp/passwd --
includeBranch o=internet --backendID internet --ldifFile /tmp/odsee-data2.ldif --
clearBackend --trustAll --noPropertiesFile
```

22. **Run dsreplication post-external-initialization**

    dsreplication post-external-initialization

    > **Note:**
    >
    > For schema 1 add:
    >
    > ```
    >  -baseDN o=internet
    > ```

    ```
    /opt/oracle/Oracle/Middleware/asinst_1/OUD/bin/dsreplication post-external-
    initialization --hostname <HOSTNAME> --port 1444 --adminUID admin --
    adminPasswordFile /tmp/passwd --baseDN o=usergroup --baseDN o=mlusers --baseDN
    o=PiServerDb --trustAll --no-prompt --noPropertiesFile
    ```

    Sample Session:

    ```
    # /opt/oracle/Oracle/Middleware/asinst_1/OUD/bin/dsreplication post-
    external-initialization --hostname <HOSTNAME> --port 1444 --adminUID admin
    --adminPasswordFile /tmp/passwd --baseDN o=usergroup --baseDN o=mlusers --
    baseDN o=PiServerDb --trustAll --no-prompt --noPropertiesFile

     Establishing connections ..... Done.

     Executing post-external initialization on base DN o=mlusers ..... Done.

     Executing post-external initialization on base DN o=PiServerDb ..... Done.

     Executing post-external initialization on base DN o=usergroup ..... Done.

     Post initialization procedure completed successfully.

     See /var/tmp/oud-replication-3702816444427427726.log for a detailed log
    of this operation.
    ```

23. **Test Replication**

    To verify that replication is working write an attribute to ODSEE and see if it shows up on the OUD side.

    Example shown below is with ldapmodify and ldapsearch commands (used on sample 'testuser1' account):

    Sample Session:

    ```
    # /opt/oracle/Oracle/Middleware/Oracle_OUD1/bin/ldapsearch -T -h
    <HOSTNAME> -p 1389 -D 'cn=Directory Manager' -j /tmp/passwd -b
    'o=usergroup' -s sub '(uid=testuser1)'

    dn: uid=testuser1,ou=People,o=example.com,o=usergroup

    dataSource: Messaging Server Initial Configuration
    ```

```
mailHost: <HOSTNAME>

objectClass: person

objectClass: ipUser

objectClass: organizationalPerson

objectClass: inetOrgPerson

objectClass: top

objectClass: userPresenceProfile

objectClass: inetUser

objectClass: inetLocalMailRecipient

objectClass: iplanet-am-managed-person

objectClass: inetMailuser

mailUserStatus: active

inetUserStatus: active

uid: testuser1

cn: testuser1

sn: testuser1

userPassword: {SSHA}g02arnhXqR7S7Qc10Z9MhGnvh+cpdzwY4FfOGA==

mail: testuser1@example.com

mailDeliveryOption: mailbox



# /opt/oracle/Oracle/Middleware/Oracle_OUD1/bin/ldapsearch -T -h
<HOSTNAME> -p 1393 -D 'cn=Directory Manager' -j /tmp/passwd -b
'o=usergroup' -s sub '(uid=testuser1)'

dn: uid=testuser1,ou=People,o=example.com,o=usergroup

objectClass: top

objectClass: person

objectClass: inetOrgPerson

objectClass: organizationalPerson

objectClass: iplanet-am-managed-person
```

```
objectClass: inetUser

objectClass: ipUser

objectClass: userPresenceProfile

objectClass: inetMailuser

objectClass: inetLocalMailRecipient

sn: testuser1

cn: testuser1

uid: testuser1

userPassword: {SSHA}g02arnhXqR7S7Qc10Z9MhGnvh+cpdzwY4FfOGA==

inetUserStatus: active

mailDeliveryOption: mailbox

dataSource: Messaging Server Initial Configuration

mailUserStatus: active

mail: testuser1@example.com

mailHost: <HOSTNAME>



# cat /tmp/add.ldif

dn: uid=testuser1,ou=People,o=example.com,o=usergroup

changetype: modify

add: mailEquivalentAddress

mailEquivalentAddress: testuser1@example.com



# /opt/oracle/Oracle/Middleware/Oracle_OUD1/bin/ldapmodify -h <HOSTNAME> -
p 1393 -D 'cn=Directory Manager' -j /tmp/passwd --filename /tmp/add.ldif

Processing MODIFY request for
uid=testuser1,ou=People,o=example.com,o=usergroup

MODIFY operation successful for DN
uid=testuser1,ou=People,o=example.com,o=usergroup
```

```
# /opt/oracle/Oracle/Middleware/Oracle_OUD1/bin/ldapsearch -T -h
<HOSTNAME> -p 1393 -D 'cn=Directory Manager' -j /tmp/passwd -b
'o=usergroup' -s sub '(uid=testuser1)'

dn: uid=testuser1,ou=People,o=example.com,o=usergroup

mailEquivalentAddress: testuser1@example.com

objectClass: top

objectClass: person

objectClass: inetOrgPerson

objectClass: organizationalPerson

objectClass: iplanet-am-managed-person

objectClass: inetUser

objectClass: ipUser

objectClass: userPresenceProfile

objectClass: inetMailuser

objectClass: inetLocalMailRecipient

sn: testuser1

cn: testuser1

uid: testuser1

userPassword: {SSHA}g02arnhXqR7S7Qc10Z9MhGnvh+cpdzwY4FfOGA==

inetUserStatus: active

mailDeliveryOption: mailbox

dataSource: Messaging Server Initial Configuration

mailUserStatus: active

mail: testuser1@example.com

mailHost: <HOSTNAME>



# /opt/oracle/Oracle/Middleware/Oracle_OUD1/bin/ldapsearch -T -h
<HOSTNAME> -p 1389 -D 'cn=Directory Manager' -j /tmp/passwd -b
'o=usergroup' -s sub '(uid=testuser1)'

 dn: uid=testuser1,ou=People,o=example.com,o=usergroup
```

```
dataSource: Messaging Server Initial Configuration
mailHost: <HOSTNAME>
mailEquivalentAddress: testuser1@example.com
objectClass: person
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: ipUser
objectClass: top
objectClass: inetUser
objectClass: userPresenceProfile
objectClass: iplanet-am-managed-person
objectClass: inetLocalMailRecipient
objectClass: inetMailuser
uid: testuser1
inetUserStatus: active
mailUserStatus: active
cn: testuser1
sn: testuser1
userPassword: {SSHA}g02arnhXqR7S7Qc10Z9MhGnvh+cpdzwY4FfOGA==
mail: testuser1@example.com
mailDeliveryOption: mailbox

# cat /tmp/add.ldif
dn: uid=testuser1,ou=People,o=example.com,o=usergroup
changetype: modify
add: mailEquivalentAddress
mailEquivalentAddress: testuser1alt@example.com
```

```
# /opt/oracle/Oracle/Middleware/Oracle_OUD1/bin/ldapmodify -h <HOSTNAME> -
p 1389 -D 'cn=Directory Manager' -j /tmp/passwd --filename /tmp/add.ldif

Processing MODIFY request for
uid=testuser1,ou=People,o=example.com,o=usergroup

MODIFY operation successful for DN
uid=testuser1,ou=People,o=example.com,o=usergroup



# /opt/oracle/Oracle/Middleware/Oracle_OUD1/bin/ldapsearch -T -h
<HOSTNAME> -p 1389 -D 'cn=Directory Manager' -j /tmp/passwd -b
'o=usergroup' -s sub '(uid=testuser1)'

dn: uid=testuser1,ou=People,o=example.com,o=usergroup

dataSource: Messaging Server Initial Configuration

mailEquivalentAddress: testuser1@example.com

mailEquivalentAddress: testuser1alt@example.com

mailHost: <HOSTNAME>

objectClass: person

objectClass: ipUser

objectClass: organizationalPerson

objectClass: inetOrgPerson

objectClass: top

objectClass: userPresenceProfile

objectClass: inetUser

objectClass: inetLocalMailRecipient

objectClass: iplanet-am-managed-person

objectClass: inetMailuser

mailUserStatus: active

inetUserStatus: active

uid: testuser1

cn: testuser1

sn: testuser1

userPassword: {SSHA}g02arnhXqR7S7Qc10Z9MhGnvh+cpdzwY4FfOGA==
mail: testuser1@example.com

mailDeliveryOption: mailbox



# /opt/oracle/Oracle/Middleware/Oracle_OUD1/bin/ldapsearch -T -h
<HOSTNAME> -p 1393 -D 'cn=Directory Manager' -j /tmp/passwd -b
'o=usergroup' -s sub '(uid=testuser1)'

 dn: uid=testuser1,ou=People,o=example.com,o=usergroup

mailEquivalentAddress: testuser1@example.com

mailEquivalentAddress: testuser1alt@example.com

objectClass: top

objectClass: person

objectClass: inetOrgPerson

objectClass: organizationalPerson

objectClass: iplanet-am-managed-person

objectClass: inetUser

objectClass: ipUser

objectClass: userPresenceProfile

objectClass: inetMailuser

objectClass: inetLocalMailRecipient

sn: testuser1

cn: testuser1

uid: testuser1

userPassword: {SSHA}g02arnhXqR7S7Qc10Z9MhGnvh+cpdzwY4FfOGA==

inetUserStatus: active

mailDeliveryOption: mailbox

dataSource: Messaging Server Initial Configuration

mailUserStatus: active

mail: testuser1@example.com

mailHost: <HOSTNAME>
```

24. **Switch UCS products from ODSEE to OUD**

    Refer Product specific documentation to switch the UCS products in your deployment to this OUD as the directory service backend.

    For each product, refer to its LDAP configuration-related parameter names, to ensure all relevant LDAP settings are now switched to this OUD Hostname (FQDN) and ports. It must be done on all your product instances (based on single or distributed deployment).

    (Example: For MS Product, this hostname and port can be set using configuration parameters: local.ugldaphost and local.ugldapport . Similarly, each UCS product has its own configuration parameters for LDAP settings and it must be set now to OUD).

> **Note:**
>
> If you see any issues with OCUCS Admin Password Policy (example: in cases like Calendar or Contact Servers), then you will have to re-run that product-specific configurator with this backend OUD instance setup.

Setting up Loosely Coupled Migration

To use a loosely coupled migration scenario instead of a tightly coupled migration scenario, you may add a switch to the oud-replication-gateway-setup "**–doNotSendUpdateToLegacyServer**"

Setting up a direct transition migration

Instead of a tightly coupled migration scenario, to do one-off direct transition/migration, follow the procedure of exporting from ODSEE, and importing that data into OUD. You will have to ensure the following :

- ODSEE data exported into ldif
- Prepare ODSEE data ldif : Diagnose using ds2oud, Fix/clean up any invalid or incompatible issues that is flagged. Ensure this ODSEE ldif file is validated successfully against OUD's schema
- Import that ODSEE ldif into OUD.

Uninstall Commands

This document outlines the process of uninstalling OUD, ODSEE, and replication gateway instances.

Uninstall replication gateway instance

```
/opt/oracle/Oracle/Middleware/asinst_2/OUD/uninstall \
--cli \
--hostname <HOSTNAME> \
--adminUID admin \
--adminPasswordFile /tmp/passwd \
--bindDNLegacy cn=Directory\ Manager \
--bindPasswordFileLegacy /tmp/passwd \
--trustAll \
--no-prompt \
--noPropertiesFile
```

Uninstall OUD instance

```
/opt/oracle/Oracle/Middleware/asinst_1/OUD/uninstall \
--cli \
--remove-all \
-h <HOSTNAME> \
--adminUID admin \
-j /tmp/passwd \
--trustAll \
--no-prompt \
--noPropertiesFile
```

Uninstall ODSEE

```
/opt/dsee7/bin/dsadm delete/var/opt/sun/directory/ds7
```