Oracle® Communications Convergence

Installation and Configuration Guide

Release 3.0.2

E69225-02

April 2020

ORACLE

Oracle Communications Convergence Installation and Configuration Guide, Release 3.0.2

E69225-02

Contents

5 Installing Convergence

6 Convergence Post-Installation Tasks

7 Upgrading Convergence

8 Uninstalling Convergence

A commpkg Reference

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
- GlassFish or Oracle WebLogic Server
- Directory server management
- Structure and use of a lightweight directory access protocol (LDAP)
- System administration and networking
- General deployment architecture

Related Documents

For more information, see the following documents:

- *Convergence System Administrator's Guide*: Describes how to manage and administer Convergence.
- *Convergence Security Guide*: Describes security concepts and features that help you install and configure Convergence in a secure configuration.
- *Convergence Customization Guide*: Describes how to customize the appearance and functionality of Convergence.
- *Convergence Release Notes*: Describes any known issues for Convergence.

Convention

The following convention is used throughout the document.

Convention	Meaning
Oracle certified application server	GlassFish Server and Oracle WebLogic Server are the certified application servers on which Convergence is supported. Oracle certified application server is used in this document to refer to either of the two application servers. **Note**: Convergence is additionally supported on Oracle WebLogic Server from release 3.0.2.1.0 onwards.

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.

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 certified application server
- Other Oracle Unified Communications products, such as:
  - Oracle Communications Messaging Server
  - Oracle Communications Calendar Server
  - Oracle Communications Contacts Server
  - Oracle Communications Instant Messaging Server
  - Oracle Communications Indexing and Search Service
  - Oracle Communications Delegated Administrator
- 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 certified application server
   - Java

- Oracle Directory Server Enterprise Edition

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.
   - Instant Messaging Server: used by Convergence to provide instant messaging services.
   - Indexing and Search Service: used by Convergence to provide enhanced indexing and searching capabilities of emails and attachments.
   - Delegated Administrator: used to provision users and services in the directory server.
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 certified application 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 certified application 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/**.
GlassFish_Home	The directory in which the GlassFish Server software is installed. For example: **/opt/glassfish3/glassfish** for GlassFish 3.1.2, **/opt/glassfish5/glassfish** for GlassFish 5.0.
WebLogic_Home	The directory in which Oracle WebLogic Server software is installed. For example: WLS_HOME.
Convergence_Domain	The application server directory containing the configuration files for the domain in which Convergence is deployed. Convergence_Domain is created in *GlassFish_Home***/domains** or *WLS_HOME*/*Oracle_Home*/*user_projects***/domains**. *Convergence_Domain* for GlassFish Server deployment is: ■ *GlassFish_Home***/domains/domain1** *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.

  Note: Instant Messaging service is available only in GlassFish deployments.

- 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. Users accessing Convergence with Internet Explorer 10 or later must do the following:

  – Configure their browser not to run Convergence in **Compatibility View**.

  – Not include the Convergence URL in the **Websites you've added to Compatibility View** list.

  - Disable **Display intranet sites in Compatibility View** if Convergence is deployed to an intranet site.

  See the discussion about compatibility view settings in the Internet Explorer online Help for more information.

- Secure/Multipurpose Internet Mail Extension (S/MIME) support:

  You can configure Convergence to send encrypted or digitally signed email messages. Convergence uses S/MIME to sign and encrypt email. S/MIME features work only if email is sent using Internet Explorer or Firefox on a Windows computer.

- Web Real-Time Communication (WebRTC) support:

  You can enhance Convergence with WebRTC features such as voice and video calling and screen sharing. WebRTC features are supported as follows:

  - A screen sharing session can be initiated only from a Google Chrome browser.
  - Mozilla Firefox users cannot initiate screen sharing but can receive screen-sharing requests. Once a screen sharing session has begun, a Firefox user has the same capabilities as a Chrome user.
  - Chrome version 67 must be launched manually from a command line with the **enable-usermedia-screen-capturing** flag to initiate a screen sharing session. For example, from a Windows command line, enter:

    ```
    start chrome --enable-usermedia-screen-capturing
    ```

  - Microsoft Internet Explorer, Microsoft Edge, and Apple Safari do not support any WebRTC features.
  - You can deliver WebRTC features in Convergence using either WIT Software or Oracle WebRTC Session Controller. See the discussion about configuring WebRTC services in Convergence in *Convergence System Administrator's Guide* for more information.

- 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, and Instant Messaging 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	10, 11
Oracle Solaris on x64	10, 11
Oracle Linux on x64 (64-bit), Red Hat Enterprise Linux on x64 (64-bit)	6, 7

Software Requirements

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

Table 3–2 Convergence Software Requirements

Software	Version	Required or Optional
Oracle Directory Server Enterprise Edition	11*g*R1 PS2 (11.1.1.7.0)	Required, server-side
Directory Server Schema	6.4.0.29 or later	Required, on directory server
Application Server	Oracle WebLogic Server 12.2.1.3 **Note**: Convergence is additionally supported on Oracle WebLogic Server from release 3.0.2.1.0 onwards. GlassFish Server Open Source Edition 5.0 Oracle GlassFish Server 3.1.2 with latest patch update	Required, server-side

Table 3–2 (Cont.) Convergence Software Requirements

Software	Version	Required or Optional
Java Runtime Environment (JRE)	JDK8u144 and above if Convergence is deployed on Oracle WebLogic Server. JDK8u144 to JDK8u152 if Convergence is deployed on GlassFish 5.0 JDK7 with latest critical patch update if Convergence is deployed on GlassFish 3.x	Required, server-side and client-side
Desktop web browser	Google Chrome 75 Mozilla Firefox 67 Mozilla Firefox ESR 52 (for SMIME) Microsoft Internet Explorer 11 Microsoft Edge 40 Apple Safari 11.0.2	Required, client-side See note below table.
Tablet web browser	Apple iPad: Safari Android: Google Chrome	Required, client-side See note below table.
Oracle Communications Messaging Server	8.0.x	Required, server-side
Oracle Communications Calendar Server	8.0.x	Required, server-side
Oracle Communications Contacts Server	8.0.x	Optional, server-side
Oracle Communications Instant Messaging Server	10.0.x	Optional, server-side
Oracle Communications Delegated Administrator	7.0.x	Optional, server-side
Oracle Communications Indexing and Search Service	1.0.5.x	Optional, server-side
Oracle Access Manager	11*g*R1 PS2 (11.1.1.7.0)	Optional, server-side
Oracle Communications WebRTC Session Controller	7.2.0.2.0	Optional, server-side
Oracle Outside In Transformation Server	8.5.1	Optional, server-side
WIT Communications Application Server	Latest	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.

Note: 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, " GlassFish Server Information"
- Table 3–6, " Oracle WebLogic Server Information"
- Table 3–7, " Directory Server Information"
- Table 3–8, " 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 the GlassFish Server information that you provide during initial configuration.

Table 3–5 GlassFish Server Information

Information Type	Description
GlassFish Server installation directory	Directory in which GlassFish Server is installed. For GlassFish 3.1.2, the default is: **/opt/glassfish3** For GlassFish 5.0, the default is: **/opt/glassfish5**
GlassFish Server domain directory	The directory in which domain directories are created. For GlassFish 3.1.2, the default is: **/opt/glassfish3/glassfish/domains** For GlassFish 5.0, the default is: **/opt/glassfish5/glassfish/domains**
GlassFish Server document root directory	The GlassFish Server document root directory. For GlassFish 3.1.2, the default is: **/opt/glassfish3/glassfish/domains/***Convergence_Domain***/docroot** For GlassFish 5.0, the default is: **/opt/glassfish5/glassfish/domains/***Convergence_Domain***/docroot**
GlassFish Server target instance name	The name of the server target name. Default: server
GlassFish Server virtual server	The virtual server identifier. Default: server
GlassFish Server Instance port	The HTTP port number for the server instance. Default: 8181 (HTTPS)
GlassFish Server administration server port	The HTTP port number for the target server instance. Default: 4848
Is administration server port secure	Whether the GlassFish Server administration server port is running over SSL. Default: Enabled
GlassFish Server administrator user name and password	The user name and password for the GlassFish Server administration server.

Table 3–6 lists Oracle WebLogic Server information that you provide during initial configuration.

Table 3–6 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

Table 3–6 (Cont.) Oracle WebLogic Server Information

Information Type	Description
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 3–7 lists the directory server information that you provide during the initial configuration.

Table 3–7 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*
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 3–8 lists the information required for other software that you provide during the initial configuration.

Table 3–8 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.

Table 3–8 (Cont.) Software Information

Information Type	Description
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.
Instant Messaging Server domain name	The domain name of the Instant Messaging Server. For example: *MyIMDomain***.com**
Instant Messaging Server host name	The host name where Instant Messaging Server is installed. For example: **im.***MyIMDomain***.com**
Instant Messaging Server port number	The Instant Messaging Server HTTP port number. Default: 5269
Instant Messaging Server httpbind component JID and password	The Instant Messaging Server httpbind component Jabber ID (JID) and password. The JID must match the value in the Instant Messaging Server **iim.conf.xml** configuration file. For example: **httpbind.***MyIMDomain***.com**
Instant Messaging Server avatar component JID and password	The Instant Messaging Server avatar component JID and password. For example: **avatar.***MyIMDomain***.com**
Indexing and Search Service host name	The host name where Indexing and Search Service is installed. For example: **iss.***MyDomain***.com**
Indexing and Search Service port number	The Indexing and Search Service HTTP port number. Default: 8181 (HTTPS)
Access (Indexing and Search Service) in SSL mode	Whether the Indexing and Search Service port is running over SSL. Default: Enabled
Indexing and Search Service administration user name and password	The administration user name and password for Indexing and Search Service.
Convergence address book service	How the address book service is provided. You can select either Convergence or Contacts Server. Default: Contacts Server
Contacts Server host name	The Contacts Server host name. Syntax: **cos.***Default_Domain* For example: **cos.***MyDomain***.com**

Table 3–8 (Cont.) Software Information

Information Type	Description
Contacts Server port number	The Contacts Server HTTP port number. Default: 8181 (HTTPS)
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

GlassFish Server or Oracle WebLogic Server is a Java application and needs a Java environment in which 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 (**comm_dssetup.pl**) 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 prepare the directory server:

1. Download the **comm_dssetup.pl** script from the Oracle software delivery web site:

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

   The **comm_dssetup.pl** 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 **comm_dssetup.pl** script.
6. Install the **comm_dssetup.pl** 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. Run the **comm_dssetup.pl** script without any arguments.

   ```
   /usr/bin/perl comm_dssetup.pl
   ```

   Answer the command-line prompts.

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

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*.

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

Preparing Instant Messaging Server for Convergence Integration

If you are configuring Convergence with the Instant Messaging service, do the following to prepare Instant Messaging Server:

1. Configure Instant Messaging Server with the XMPP/HTTP Gateway Deployment parameter set to false.

   As the XMPP/HTTP Gateway is deployed through Convergence, its value is set to true when you configure Convergence.

   See *Instant Messaging Server Installation and Configuration Guide* for more information.

2. Using the Instant Messaging Server **imconfutil** command-line utility, add the **c2s** component:

   ```
   imconfutil -u set-listener-prop  s2s protocols="s2s,component,c2s" -c /opt/
   sun/comms/im/config/iim.conf.xml
   ```

3. Using the **imconfutil** command, set the **iim_agent.enable** property to **true**:

   ```
   imconfutil set-prop iim_agent.enable=true -c /opt/sun/comms/im/config/
   iim.conf.xml
   ```

4. Using the **imconfutil** command, configure the httpbind component Jabber ID (JID) and password. For example:

   ```
   imconfutil add-component id=httpbind1
   jid=convergence1-jid.httpbind.MyDomain.com password=secret -c /opt/sun/comms/
   im/config/iim.conf.xml
   ```

5. Using the **imconfutil** command, configure the avatar component JID and password. For example:

   ```
   imconfutil add-component id=avatar1 jid=avatar1-jid.avatar.MyDomain.com
   password=secret -c /opt/sun/comms/im/config/iim.conf.xml
   ```

Note: The httpbind and avatar JIDs can be any string. These values do not have to identify a particular Instant Messaging host and domain name. However, it is a good practice to make these values meaningful. For example, include the host and domain name in these JIDs to make the identifiers easy to recognize.

The passwords for the httpbind and the avatar JIDs can be unique. They do not have to match any other password used for Instant Messaging Server or other back-end servers.

The JIDs and passwords configured in the **iim.conf.xml** file must match the httpbind and Avatar JIDs that you specify when you run the Convergence initial configuration program.

---

6. See "Configuring Instant Messaging for Multiple Convergence Instances" if you intend to configure multiple instances of Convergence to use the same Instant Messaging server.

Configuring Instant Messaging for Multiple Convergence Instances

If you are configuring multiple instances of Convergence to use one Instant Messaging server, you must set up a unique httpbind and avatar JID value for each instance of Convergence. See "Preparing Instant Messaging Server for Convergence Integration" for information about setting httpbind and avatar JID values.

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 GlassFish Server or 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://edelivery.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: To install Convergence on Oracle Linux 7, 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**

Table 5–1 (Cont.) State File Options

Option	Description	Example
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 Indexing and Search Service: **COMPONENTS=JISS** 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.

Configuring Convergence as Non-Root User for GlassFish Server

If you set up GlassFish Server as a non-root user, you must do one of the following:

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

  ```
  ln -s /usr/jdk/jdk1.7.0_75 /usr/jdk/latest
  ```

- Define the **JAVA_HOME** and **PATH** variables in the GlassFish Server user profile. It is not enough to only define the variable in the current shell that you are using to run the initial configuration script.

  If the GlassFish Server user is referencing a JDK in a different location, set that location in the user **.profile** file by adding the following line.

  ```
  export JAVA_HOME=JDK_location
  ```

  Alternatively, you can add the line to the system-wide profile (**/etc/profile**) instead.

- If you are deploying Convergence on GlassFish Server 5, set the Java path with the **AS_JAVA** property in the *GlassFish_Home***/config/asenv.conf** file.

  where, *GlassFish_Home* is the directory in which the GlassFish Server software is installed

  ```
  Example, AS_JAVA=/usr/jdk/jdk1.8.0_152
  ```

Running the Convergence Initial Configuration Script for GlassFish 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.

The configuration program can launch a GUI or run at the command line. This section describes the GUI version of the program, even though both are similar and collect the same information.

To configure Convergence using the initial configuration script:

1. Verify that GlassFish 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 for GlassFish Server:

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

   The Convergence configuration Welcome screen appears.

   Note: To run the configuration program at the command line, enter the following command instead:

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

   Click **Next**. The Select the Directory to Store Configuration and Data Files screen appears.

5. When prompted, select the directory in which to store the Convergence configuration and data files.

   Do not select *Convergence_Home* as the location directory.

   Click **Next**. The Select Services to Configure screen appears.

6. Select the services to configure with Convergence:

   - Mail Service
   - Calendar Service
   - Instant Messaging Service
   - Indexing and Search Service
   - Address Book Service

   Click **Next**. The Convergence Server Host Name and DSN Domain Name screen appears.

7. Enter the host name of the system on which Convergence is being configured. Also, enter the DNS domain name of the Convergence host system.

   Click **Next**. The GlassFish Server Configuration Details screen appears.

8. Specify the following:

   - Installation directory
   - Domain directory
   - Document root directory
   - Server target name
   - Virtual server identifier
   - Server instance port

   Click **Next**. The GlassFish Server Administration Instance Details screen appears.

9. Specify the following:

   - GlassFish administration server port
   - GlassFish server administration user ID
   - GlassFish server administration password
   - Whether HTTP access to the administration server is secure.

   Click **Next**. The program tests the connection to the GlassFish administration server. The Web Container User and Group screen appears.

10. Specify the GlassFish Server installation user ID and group.

    Click **Next**. The Enter the URI Path Where Convergence Will be Deployed screen appears.

11. Specify the URI path to where you want to deploy Convergence.

    For example: **/iwc**.

    Click **Next**. The Specify Whether You Want Hosted Domain Support screen appears.

12. Specify whether you want to support for hosted domains in the Convergence deployment.

Click **Next**. The Specify LDAP User/Group Configuration Details screen appears.

13. Provide the following:

    - **User/Group LDAP URL**: URL for the User/Group LDAP used by Messaging Server, Calendar Server, and Instant Messaging 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.

    Click **Next**. The Confirm the Base DN of the DC Tree Suffix screen appears.

14. Confirm the base DN.

    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.

    Click **Next**. The Enter the Default Domain Name screen appears.

15. 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**.

    Click **Next**.

16. If you chose to configure the mail service, the Specify the Mail Service Configuration Details screen 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

    Click **Next**. The program tests the connection to the Messaging server.

17. If you chose to configure the calendar service, the Calendar Server Version screen appears.

    Specify the version of Calendar Server you are integrating with Convergence to deliver the calendar service.

For example, select **CS 7 and up** for Calendar Server version 8.x.

Click **Next**.

18. If you chose to configure the calendar service, the Specify the Calendar Service Configuration Details screen 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

    Click **Next**. The program tests the connection to the Calendar server.

19. If you chose to configure the instant messaging service, the Specify the Instant Messaging Service Configuration Details screen appears.

    Specify the following:

    - Server domain name
    - Server host name
    - Server port number
    - httpbind component JID
    - httpbind component password
    - Avatar component JID
    - Avatar component password

    Click **Next**.

20. If you chose to configure the indexing and search service, the Specify the Indexing and Search Service Configuration Details screen appears.

    Specify the following:

    - Indexing and search service host name
    - Indexing and search service port number

      The SSL port is provided by default.
    - Access in SSL mode
    - Indexing and search service user ID
    - Indexing and search service password

    Click **Next**. The program tests the connection to Instant Indexing And Search Service.

21. If you chose to configure the address book service, the Specify the Contacts Server Selection screen appears.

    Select how to provide the address book service:

- Select **Convergence Address Book Service** to provide the address book service through Convergence and the directory server.
- Select **Contacts Server Address Book Service** to provide the address book service with Contacts Server.

22. If you chose to provide the address book service with Contacts Server, the Specify 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

    Click **Next**. The program tests the connection to the Contacts server.

23. The Specify the Convergence Administrator Details screen appears.

    Provide the Convergence administrator user name and 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.

    Click **Next**. The Ready to Configure screen appears.

24. Review the list of items to be configured.

    Click **Next**. The Task Sequence screen appears.

25. The Task Sequence screen displays the configuration tasks being performed.

    Click **Cancel** to stop the configuration process.

    When the screen displays the message `All Tasks Passed`, click **Next**. The Installation Summary screen appears.

26. The Installation Summary screen displays a summary of the completed configuration tasks.

    Click **Details** to display more information about the completed configuration tasks.

    Click **Close** to exit the configuration program.

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.

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 Installers` for information on Oracle WebLogic Server download location.
2. Create a Domain, Administration Server, and Managed Server. See `Configuring the WebLogic Domain` for more information.

   See the following Oracle WebLogic Server resources for more information:
   - `Oracle WebLogic Server 12.2.1.3 documentation`
   - `Starting the Installation Program`
   - `A Oracle Universal Installer Installation Screens`
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 the Oracle WebLogic Server documentation at:

     `https://docs.oracle.com/middleware/12213/wls/SECMG/identity_trust.htm#SECMG365`

   - 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 Sever 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.

The configuration program can launch a GUI or run at the command line. This section describes the GUI version of the program, even though both are similar and collect the same information.

Set the environment variable for Oracle WebLogic Server:

```
export ORACLE_IWC_APPSERVTYPE=WebLogic
```

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
   ```

   The Convergence configuration Welcome screen appears.

Note: To run the configuration program at the command line, enter the following command instead:

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

Click **Next**. The Select the Directory to Store Configuration and Data Files screen appears.

5. When prompted, select the directory in which to store the Convergence configuration and data files.

   Do not select *Convergence_Home* as the location directory.

   Click **Next**. The Select Services to Configure screen appears.

6. Select the services to configure with Convergence:

   - Mail Service
   - Calendar Service
   - Indexing and Search Service
   - Address Book Service

   Click **Next**. The Convergence Server Host Name and DSN Domain Name screen appears.

7. Enter the host name of the system on which Convergence is being configured. Also, enter the DNS domain name of the Convergence host system.

   Click **Next**. Oracle WebLogic Server Configuration Details screen appears.

8. Specify the following:

   - Oracle WebLogic Server Installation directory
   - Oracle WebLogic Server Domain directory
   - Oracle WebLogic Server Document root directory
   - Oracle WebLogic Server target name
   - Oracle WebLogic Server Virtual server identifier
   - Oracle WebLogic Server instance port

   Click **Next**. Oracle WebLogic Server Administration Instance Details screen appears.

9. Specify the following:

   - Oracle WebLogic Server Administration server port
   - Oracle WebLogic Server Administration user ID
   - Oracle WebLogic Server Administration password
   - Is Administration Server port secure
   - Whether HTTP access to the administration server is secure.

   Click **Next**. The program tests the connection to Oracle WebLogic administration server. The Web Container User and Group screen appears.

10. Specify Oracle WebLogic Server installation user ID and group.

Click **Next**. The Enter the URI Path Where Convergence Will be Deployed screen appears.

11. Specify the URI path to where you want to deploy Convergence.

    For example: **/iwc**.

    Click **Next**. The Specify Whether You Want Hosted Domain Support screen appears.

12. Specify whether you want to support for hosted domains in the Convergence deployment.

    Click **Next**. The Specify LDAP User/Group Configuration Details screen appears.

13. Provide the following:

    - **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.

    Click **Next**. The Confirm the Base DN of the DC Tree Suffix screen appears.

14. Confirm the base DN.

    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.

    Click **Next**. The Enter the Default Domain Name screen appears.

15. 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**.

    Click **Next**.

16. If you chose to configure the mail service, the Specify the Mail Service Configuration Details screen 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

Click **Next**. The program tests the connection to the Messaging server.

17. If you chose to configure the calendar service, the Calendar Server Version screen appears.

    Specify the version of Calendar Server you are integrating with Convergence to deliver the calendar service.

    For example, select **CS 7 and up** for Calendar Server version 8.x.

    Click **Next**.

18. If you chose to configure the calendar service, the Specify the Calendar Service Configuration Details screen 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

    Click **Next**. The program tests the connection to the Calendar server.

19. If you chose to configure the indexing and search service, the Specify the Indexing and Search Service Configuration Details screen appears.

    Specify the following:

    - Indexing and search service host name
    - Indexing and search service port number

      The SSL port is provided by default.
    - Access in SSL mode
    - Indexing and search service user ID
    - Indexing and search service password

    Click **Next**. The program tests the connection to Instant Indexing And Search Service.

20. If you chose to configure the address book service, the Specify the Contacts Server Selection screen appears.

    Select how to provide the address book service:

    - Select **Convergence Address Book Service** to provide the address book service through Convergence and the directory server.
    - Select **Contacts Server Address Book Service** to provide the address book service with Contacts Server.

21. If you chose to provide the address book service with Contacts Server, the Specify 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

    Click **Next**. The program tests the connection to the Contacts server.

22. The Specify the Convergence Administrator Details screen appears.

    Provide the Convergence administrator user name and 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.

    Click **Next**. The Ready to Configure screen appears.

23. Review the list of items to be configured.

    Click **Next**. The Task Sequence screen appears.

24. The Task Sequence screen displays the configuration tasks being performed.

    Click **Cancel** to stop the configuration process.

    When the screen displays the message `All Tasks Passed`, click **Next**. The Installation Summary screen appears.

25. The Installation Summary screen displays a summary of the completed configuration tasks.

    Click **Details** to display more information about the completed configuration tasks.

    Click **Close** to exit the configuration program.

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/Iwc-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 GlassFish Server or 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 -noconsole -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 many add-on services, including:

- One-way and two-way short message service (SMS)
- Web real-time communication
- 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 the 3.0.1.x version.

See "Upgrading from 3.0.1.x to 3.0.2" for more information.

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 certified application 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 3.0.1.x to 3.0.2

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
- Oracle WebRTC Session Controller Upgrade

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.

Oracle WebRTC Session Controller Upgrade

The new version of Convergence requires an updated version of WebRTC Session Controller. If you already integrate Convergence with WebRTC Session Controller to provide Web real-time communication services, you must upgrade WebRTC Session Controller and reconfigure Convergence. See "System Requirements" for more information.

Upgrading from 3.0.1.x to 3.0.2

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

- Pre-Upgrade Tasks (3.0.1.x to 3.0.2)
- Upgrading Convergence (3.0.1.x to 3.0.2)
- Post-Upgrade Tasks (3.0.1.x to 3.0.2)

Pre-Upgrade Tasks (3.0.1.x to 3.0.2)

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 Oracle Directory Server Enterprise Edition (ODSEE) based LDAP client
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 (3.0.1.x to 3.0.2)

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 GlassFish 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 GlassFish Server domain on which Convergence is deployed:

   ```
   asadmin restart-domain Convergence_Domain
   ```

Post-Upgrade Tasks (3.0.1.x to 3.0.2)

After the Convergence upgrade has completed successfully, do any of 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.
- If, in a previous release of Convergence, you integrated Convergence with Oracle WebRTC Session Controller to deliver Web real-time communications services, you must upgrade WebRTC Session Controller. Refer to the WebRTC Session Controller documentation for information. Then you must reconfigure the integration between Convergence and WebRTC Session Controller. See the discussion about configuring WebRTC services in Convergence in *Convergence System Administrator's Guide* for more information.
- All logging configurations except for the HTTPBIND, HTTPBIND_XFER, and HTTPBIND_AVATAR components are preserved. Configure logging properties for the HTTPBIND, HTTPBIND_XFER, and HTTPBIND_AVATAR components of Convergence using the **iwcadmin** command. The existing changes to HTTPBIND logging will not be preserved in the **httpbind_log4j.conf** file in Convergence configuration directory.

  After upgrade, HTTPBIND logs will be in the **httpbind.log** file in Convergence log directory even if they are changed before the upgrade. However, you can set the logging properties for the HTTPBIND, HTTPBIND_XFER, and HTTPBIND_AVATAR components by running the **iwcadmin** command. Setting

the logging properties for these components is a one-time activity. So, once the logging properties are configured by using the **iwcadmin** command, you can freely upgrade to some other version later and the configuration changes will be preserved.

This example shows how to set the logging properties for the HTTPBIND component after the appender reference is set for the component:

```
iwcadmin -o log.HTTPBIND.appendername -v HTTPBIND_APPENDER
iwcadmin -o log.appender.[HTTPBIND_APPENDER].type -v FILE
iwcadmin -o log.appender.[HTTPBIND_APPENDER].location -v /var/opt/sun/comms/
iwc/logs/iwc_httpbind.log
iwcadmin -o log.appender.[HTTPBIND_APPENDER].sizetriggerval -v 5120
iwcadmin -o log.appender.[HTTPBIND_APPENDER].maxbackupindex -v 7
iwcadmin -o log.appender.[HTTPBIND_APPENDER].pattern -v '[%d{DATE}] %-5p %c
[%t] %m%n'
```

Similarly, you can set the logging properties for the HTTPBIND_XFER and HTTPBIND_AVATAR components by running the **iwcadmin** command.

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

About Migrating Convergence Deployment from GlassFish Server 3 to GlassFish Server 5

Convergence supports both GlassFish Server 3 and GlassFish Server 5. If you are migrating Convergence deployment from GlassFish Server 3 to GlassFish Server 5, do the following to prepare Convergence for migration:

Note: You have to manually install and configure GlassFish Server 5.

Note: GlassFish Server 5 requires Oracle JDK 8 Update 144 to Oracle JDK 8 Update 152.

Planning Backup

You must implement a backup for the following directories before migrating Convergence deployment from GlassFish Server 3 to GlassFish Server 5:

- Backup Convergence configuration directory.
- Backup Convergence customization directory in case of any customization is done in Convergence GlassFish Sever 3 deployment.
- Backup output of **iwcadmin -l** command.
- Stop GlassFish Server 3 domain where Convergence is deployed. In the following example, the domain is *iwcdomain*:

  ```
  GlassFish_Home/bin/asadmin stop-domain iwcdomain
  ```

  where, *GlassFish_Home* is the directory in which the GlassFish Server software is installed.

Migrating Convergence Deployment from GlassFish Server 3 to GlassFish Server 5

You can not upgrade GlassFish Server 3 to GlassFish Server 5 directly, as Update Tool and pkg command are no longer part of GlassFish Server5. However, there are different approaches that you can use to migrate an existing Convergence deployment in GlassFish Server 3 to GlassFish Server 5.

The different approaches that you can use to migrate the Convergence deployment to GlassFish Server 5 from GlassFish Server 3 are as follows:

Approach 1

In this approach, you configure and deploy Convergence in GlassFish Server 5 and copy the changes from GlassFish Server 3 deployment. This approach can be used to migrate any previous Convergence deployment to the latest.

In this approach, you perform the following steps:

1. Download the **glassfish5.zip** file and unzip the file under required location.

   GlassFish Server 5 contains default domain, **domain1**. A new domain can also be created for deploying Convergence. If the default domain is used, the admin password and master password has to be updated.

2. Configure **AS_JAVA** variable in the *GlassFish_Home*/**config/asenv.conf** file.

   where, *GlassFish_Home* is the directory in which the GlassFish Server software is installed.

   ```
   Example, AS_JAVA=/usr/jdk/jdk1.8.0_152
   ```

3. Enable secure admin to login into admin console remotely. In this example, the administrator port is 4848.

   ```
   GlassFish_Home/asadmin enable-secure-admin --port 4848
   ```

4. Start GlassFish Server 5 domain. In the following example, the domain is domain1:

   ```
   GlassFish_Home/bin/asadmin start-domain domain1
   ```

5. From *dir*, run the installer:

   ```
   ./commpkg install
   ```

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

6. Run the Convergence initial configuration script to configure Convergence.
7. Login to Convergence to check deployment in GlassFish Server 5.
8. Check the configuration details from previous deployment using **iwcadmin -l** output and redo the changes using iwcadmin command.
9. If you want to enable customization , enable the Convergence server for customization using the iwcadmin command:

   ```
   iwcadmin -o client.enablecustomization -v true
   ```

10. Make sure to have customization directory available for GlassFish Server 5 as required and copy the changes in the customization directory from previous deployment to GlassFish Server 5 location.
11. Restart GlassFish Server 5 and check the deployment.

Approach 2

In this approach, Convergence is upgraded to 3.0.2 by modifying **savestate** file with GlassFish Server 5 installation details. The silent configuration file, called **saveState** is created in the *Convergence_Home***/data/setup/Iwc-config-***YYYYMMDDHHMMSS* directory.

where, *Convergence_Home* is installation location for the Convergence software and *YYYYMMDDHHMMSS* represents the date and time of the saveState file.

In this approach, you perform the following steps:

1. Download the **glassfish5.zip** file and unzip the file under required location.

   GlassFish Server 5 contains default domain, **domain1**. If the default domain is used, the admin password and master password has to be updated. A new domain can also be created for deploying Convergence, with same admin user details as with GlassFish Server 3.

2. Configure **AS_JAVA** variable in the *GlassFish_Home***/config/asenv.conf** file.

   where, *GlassFish_Home* is t.he directory in which the GlassFish Server software is installed.

   ```
   Example, AS_JAVA=/usr/jdk/jdk1.8.0_152
   ```

3. Enable secure admin to login into admin console remotely. In this example, the administrator port is 4848.

   ```
   GlassFish_Home/asadmin enable-secure-admin --port 4848
   ```

4. Start GlassFish Server 5 domain. You will need to specify the GlassFish domain in which you plan to deploy Convergence. In the following example, the domain is domain1:

   ```
   GlassFish_Home/bin/asadmin start-domain domain1
   ```

5. Modify the saveState file created when Convergence is deployed using GlassFish Server 3. Modify GlassFish Server 3 locations by GlassFish Server 5 location and port details. The parameters like iwc.appsrv.* (iwc.appsrv.installDirectory, v, or iwc.appsrv.DocumentRootDirectory) has to be updated properly. Following is the example of saveState file created in GlassFish Server 3 deployment:

   ```
   iwc.appsrv.installDirectory = /opt/glassfish3
   iwc.appsrv.DomainDirectory = /opt/glassfish3/glassfish/domains/domain1
   iwc.appsrv.DocumentRootDirectory = /opt/glassfish3/glassfish/domains/domain1/
   docroot
   iwc.appsrv.TargetName = server
   iwc.appsrv.virtualServerID = server
   iwc.appsrv.portNumber = 443
   iwc.appsrv.AdminHost =hostname
   iwc.appsrv.AdminPort = 4848
   iwc.appsrv.AdminUserID = admin
   iwc.appsrv.AdminUserPassword = encrypted_password
   iwc.appsrv.IsSecureAdminServerInstance = true
   ```

6. From *dir*, run the upgrade installer:

   ```
   ./commpkg upgrade
   ```

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

7. Restart GlassFish domain.

8. Login to Convergence to check deployment in GlassFish Server 5.
9. If customization was enabled in GlassFish Server 3 deployment, make sure the parameter **client.enablecustomization** is set to true after Convergence upgrade. Otherwise, you can enable the Convergence server for customization using the following iwcadmin command:

   ```
   iwcadmin -o client.enablecustomization -v true
   ```

10. Make sure to have customization directory available for GlassFish Server 5 as required and copy the changes in the customization directory from previous deployment to GlassFish Server 5 location.
11. Restart GlassFish Server 5 and check the deployment.

Approach 3

In this approach, the GlassFish Server 3 installation directory contents will be replaced with GlassFish Server 5 installation directory contents.

In this approach you perform the following steps:

1. Move the GlassFish Server 3 location to a different location by using the following command:

   ```
   mv GlassFish3_Home GlassFish3_backup_location
   ```

   where, *GlassFish3_Home* is the directory in which the GlassFish Server 3 software is installed and *GlassFish3_backup_location* is the directory where the GlassFish Server 3 software is moved.

2. Download the **glassfish5.zip** file and unzip the file into the same installation directory as the GlassFish Server 3.

   GlassFish Server 5 contains default domain, **domain1**. A new domain can also be created for deploying Convergence. If the default domain is used, the admin password and master password has to be updated. You should provide the same username and password as in GlassFish Server 3.

3. Configure **AS_JAVA** variable in the *GlassFish_Home***/config/asenv.conf** file.

   where, *GlassFish_Home* is t.he directory in which the GlassFish Server software is installed

   ```
   Example, AS_JAVA=/usr/jdk/jdk1.8.0_152
   ```

4. Enable secure admin to login into admin console remotely. In this example, the administrator port is 4848.

   ```
   GlassFish_Home/asadmin enable-secure-admin --port 4848
   ```

5. Start GlassFish Server 5 domain. You will need to specify the GlassFish domain in which Convergence is deployed. In the following example, the domain is domain1:

   ```
   GlassFish_Home/bin/asadmin start-domain domain1
   ```

6. From *dir*, run the upgrade installer:

   ```
   ./commpkg upgrade
   ```

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

7. Restart GlassFish Server 5 domain.

8. Login to Convergence to check deployment in GlassFish Server 5.
9. Check the configuration details from previous deployment using **iwcadmin -l** output and redo the changes using iwcadmin command. This is done to make sure that most of the configurations is retained.
10. If you want to enable customization , enable the Convergence server for customization using the iwcadmin command:

    ```
    iwcadmin -o client.enablecustomization -v true
    ```

11. Make sure to have customization directory available for GlassFish Server 5 as required and copy the changes in the customization directory from previous deployment to GlassFish Server 5 location.
12. Restart GlassFish Server 5 and check the deployment.

> **Note:** Existing customization may not work for three-pane layout. The same customization has to be done for GlassFish Server 5.

After the deployment of Convergence has been migrated from GlassFish Server 3 to GlassFish Server 5 successfully, login to convergence. The default layout selected is three-pane layout. You can change the layout by performing any of the following:

- To change the layout for all the users, you can use the following **iwcadmin** command:

  ```
  iwcadmin -o user.common.layoutPreference -v classic
  ```

  Restart GlassFish Server.
- To change the layout for specific users, you can perform either of the following:
  - You can change the layout to two-pane by using the User Interface. See the instruction to change the layout in Convergence Online Help.
  - You can change the layout to two-pane by adding the objectclass:sunUCPreferences and sunUCExtendedUserPrefs:layoutPreference=classic LDAP attributes for a user.

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 12.2.1.3 and deployed Convergence on Oracle WebLogic Server.

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

1. Back up the configuration folder, c11n folder, and output of **iwcadmin -1** command.
2. Install the latest version of Convergence using **commpkg** tool and upgrade to Convergence 3.0.2.1.0 on GlassFish 3 or GlassFish 5.
3. After successful upgrade, restart GlassFish Server.

4. Copy the **c11n** folder to the **docroot** folder of the GlassFish domain.
5. Restart the GlassFish Server to verify everything in the new version of Convergence is fine. For example, login to Convergence and verify that customizations that you have performed work appropriately with the upgraded version of Convergence.
6. Stop GlassFish Server and start Oracle WebLogic Admin Server and Managed Server.
7. Configure Convergence.
8. Copy the backed up c11n folder to the path that is provided in the Document Root Directory (for example, */var/opt/sun/comms/iwc/web-src/client/iwc_static)*.
9. Update the missing required configurations on Oracle WebLogic Deployment by comparing the outputs 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 certified application server domain.
   - You can use the **asadmin** command or GlassFish Administration Console to undeploy Convergence. See GlassFish Server documentation for more information.
   - 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
   ```
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.
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.