Oracle® Communications Instant Messaging Server

Installation and Configuration Guide

Release 9.0.2

E53651-01

August 2014

ORACLE®

Oracle Communications Instant Messaging Server Installation and Configuration Guide, Release 9.0.2

E53651-01

Contents

Preface

This guide provides instructions for installing and configuring Oracle Communications Instant Messaging Server.

Audience

This document is intended for system administrators or software technicians who install and configure Instant Messaging Server. This guide assumes you are familiar with the following topics:

- Oracle Communications Unified Communications Suite component products
- Oracle Directory Server Enterprise Edition and LDAP
- System administration and networking

Related Documents

For more information, see the following documents in the Instant Messaging Server documentation set:

- *Instant Messaging Server Release Notes*: Describes the fixes, known issues, troubleshooting tips, and required third-party products and licensing.
- *Instant Messaging Server System Administrator's Guide*: Provides instructions for administering Instant Messaging Server.
- *Instant Messaging Server Security Guide*: Provides guidelines and recommendations for setting up Instant Messaging Server in a secure configuration.

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 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

Instant Messaging Server Installation Overview

This chapter provides an overview of the Oracle Communications Instant Messaging Server installation process.

Overview of Instant Messaging Server Installed Components

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

- Java
- Instant Messaging Server

Instant Messaging Server depends on Oracle Communications Directory Server Enterprise Edition for LDAP services. If your site does not currently have Directory Server deployed and you need to install it, see the Oracle Directory Server Enterprise Edition documentation for instructions, at:

http://docs.oracle.com/cd/E29127_01/index.htm

For Instant Messaging Server to use notifications offline, you must have an email server installed, such as Oracle Communications Messaging Server. For Instant Messaging Server to use the calendar agent, you must have Oracle Communications Calendar Server installed. See the Messaging Server and Calendar Server documentation for information on installing those products.

Overview of the Instant Messaging Server Installation Procedure

The installation procedure follows these steps:

1. Plan your installation. When planning your installation, do the following:
   - Determine the scale of your implementation, for example, a small development system, or a large production system.
   - Determine how many physical machines you need, and which software components to install on each machine.
   - Plan the system topology, for example, how the system components connect to each other over the network.
2. Review system requirements. System requirements include:
   - Hardware requirements, such as disk space.
   - System software requirements, such as operating system (OS) versions and OS patch requirements.
   - Information requirements, such as IP addresses and host names.

3. Install and configure software upon which Instant Messaging Server is dependent, including Java.
4. Prepare the Directory Server schema by installing and running the most current **comm_dssetup** script from the Communications Suite distribution.
5. Install and configure Instant Messaging Server.
6. Perform post-installation configuration tasks.
7. Verify the installation.

After Instant Messaging Server is installed, you might perform additional security-related tasks, such as configuring Secure Sockets Layer (SSL) communications between Instant Messaging Server front ends and back ends. For more information, see *Instant Messaging Server Security Guide*.

Instant Messaging Server Installation Options

You install Instant Messaging Server by running the Unified Communications Suite installer in either interactive or silent mode. When you run the Communications Suite installer in silent mode, you are running a non-interactive session. The installation inputs are taken from the following sources:

- A silent installation file
- Command-line arguments
- Default settings

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.

For more information, see the topic on installing Communications Suite in silent mode in *Unified Communications Suite Installation Guide* at:

https://wikis.oracle.com/display/CommSuite/Installing+Communications+Suite+7.0.6+in+Silent+Mode

Ensuring a Successful Instant Messaging Server Installation

Only qualified personnel should install the product. You must be familiar with the UNIX operating system. You should be experienced with installing Java-related packages.

Follow these guidelines:

- As you install each component, for example, 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 re-enter configuration values later in the procedure.

Directory Placeholders Used in This Guide

Table 1–1 lists the placeholders that are used in this guide:

Table 1–1 Instant Messaging Server Directory Placeholders

Placeholder	Directory
InstantMessaging_home	Specifies the installation location for the Instant Messaging Server software. The default for both Solaris and Linux is **/opt/sun/comms/im**.
InstantMessaging_cfg	Specifies the installation location for the configuration directory. The default for Solaris is **/etc/opt/sun/comms/im/default/config**. The default for Linux is **/etc/opt/sun/im/default/config**.
InstantMessaging_database	Specifies the location for the database directory, if you are using a file-based property store. The default for both Solaris and Linux is **/var/opt/sun/im/default/db**.
InstantMessaging_runtime	Specifies the location for the configurable directory for the files generated by the server at runtime. The default for both Solaris and Linux is **/var/opt/sun/im/default**.

2

Planning Your Instant Messaging Server Installation

This chapter provides information about planning your Oracle Communications Instant Messaging Server installation. It also describes the Instant Messaging Server logical and physical architectures.

> **Note:** As of Instant Messaging Server 9.0.2, support for Access Manager has been removed.

About Instant Messaging Server

Instant Messaging Server enables secure, real-time communication and collaboration, combining presence awareness with instant messaging capabilities such as chat, conferences, and file transfers to create a rich collaborative environment. These features enable one-to-one as well as group collaboration through either short-lived communications or persistent venues such as conference rooms or news channels. Instant Messaging Server ensures the integrity of communications through its multiple authentication mechanisms and Secure Sockets Layer (SSL) connections. For more information about Instant Messaging Server, see *Oracle White Paper—Oracle Communications Instant Messaging Server* at:

http://www.oracle.com/us/industries/communications/oracle-instant-messaging-wp-1449642.pdf

Instant Messaging Server Components

Instant Messaging Server consists of the following internal core components that must integrate and inter-operate with external services to provide an instant messaging environment.

- **Instant Messaging Server**. The Instant Messaging server component provides core services required for real time communications such as the presence engine, message handling and routing, roster management, security and authorization. The Instant Messaging server supports the connection of an Instant Messaging multiplexer that concentrates connections over one socket.
- **Instant Messaging Multiplexor**. The Instant Messaging multiplexer adds scalability to the Instant Messaging environment. You can install multiple multiplexers as needed, depending on your configuration. As the user population grows beyond what is easily supported by a single Instant Messaging server, you can deploy additional servers to which you can connect additional multiplexers.

- **Access, Communication, and Transfer Protocols**. These protocols, such as LDAP, HTTP, TCP/IP, and SMTP, can be found in "Instant Messaging Server Supported Standards".
- **Instant Messaging API**. Enables you to create custom Instant Messaging clients.

Instant Messaging Server Gateways

Instant Messaging Server provides the following gateways to enable connectivity to other systems:

- **XMPP/HTTP Gateway**. Enables Instant Messaging Server to provide access to HTTP-based clients, such as HTML-based clients, and clients behind firewalls that allow HTTP traffic, but do not permit XMPP traffic. The gateway proxies instant messaging traffic to the XMPP server on behalf of HTTP clients.
- **SMS Gateway**. Enables Instant Messaging Server to deliver chat messages and alerts in the form of SMS to offline users.
- **SIP Gateway**. Instant Messaging Server implements a SIP/SIMPLE (Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions/Session Initiation Protocol) gateway, enabling federation and translation between the two protocols, and interoperation between XMPP and SIP/SIMPLE servers.
- **Facebook Gateway**. Enables Instant Messaging Server users to interact with the Facebook Instant Messaging Service.

Components Related to Instant Messaging Server

The software components discussed in this section work with Instant Messaging Server, but are installed separately. See "Planning Your Instant Messaging Server Installation" for more information on how these components interact with Instant Messaging Server.

LDAP Server

(Required) Instant Messaging Server uses an LDAP server, such as Directory Server, for end user authentication and search. If you do not have an LDAP directory already installed, you must install one. This directory can either be dedicated for use by Instant Messaging Server, or be shared by other components.

The Instant Messaging server does not store the Instant Messenger end-user authentication information. This information is stored in the LDAP server.

By default, Instant Messaging Server relies on the common end-user attributes **cn** and **uid** to search for end-user and group information. If you want, you can configure the server to use another attribute for search. In addition, Instant Messaging Server properties (such as contact lists and subscriptions) can be stored in files on the Instant Messaging server or in the LDAP server.

For instructions on configuring the server to use a non-default attribute for user search, see *Instant Messaging Server System Administrator's Guide*.

Note: Because a proper Directory Server implementation is instrumental to a successful Instant Messaging Server deployment, see the Directory Server documentation at:

http://www.oracle.com/technetwork/documentation/legacy-sun-identity-mgmt-193462.html

Web Container

(Optional) You may need to install a web container, such as Web Server or GlassFish Server. You can also use any open standard web server (for example, Apache).

Instant Messaging Server 8 and previous versions require a web container to serve the Instant Messenger resources. The Instant Messenger resource files include:

- The **index.html** file, provided by Instant Messenger, or a home page with a link to invoke Instant Messenger
- Instant Messenger jar files (**messenger.jar, imres.jar**, **imbrand.jar**, **imdesktop.jar**, **imnet.jar**, and **imjni.jar**)
- The Instant Messenger Online Help

You must install Instant Messenger resources on the same host where the web container is installed. In most cases, the resources will be installed on the same host where you installed the Instant Messaging server software. It is possible to locate the Instant Messenger resources on a host other than the Instant Messaging server or multiplexor.

Note: Install the web container before configuring Instant Messaging Server.

SMTP Server

(Optional) An SMTP messaging server, such as Oracle Communications Messaging Server, is used to forward instant messages, in the form of email, to end users who are offline. The SMTP server can also be used to archive instant messaging communications. The SMTP server does not have to reside on the same host as the Instant Messaging Server host.

Calendar Server

(Optional) Oracle Communications Calendar Server is used to notify users of calendar-based events.

Instant Messaging Server Supported Standards

This section lists national, international, industry, and de-facto standards related to electronic messaging and for which support is claimed by Oracle Communications Instant Messaging Server. Most of these are Internet standards, published by the RFC Editor and approved by the Internet Engineering Task Force (IETF). Standards for documents from other sources are noted.

Protocols Support by Instant Messaging Server

Instant Messaging Server supports the following protocols:

- Extensible Messaging and Presence Protocol(XMPP):
  - XMPP Core Protocols (RFC 3920, RFC 3921)
  - XMPP Extensions
- Short message peer-to-peer protocol (SMPP)

Table 2–1 shows the supported XMPP Extensions.

Table 2–1 Supported XMPP Extensions

Number	Name	Comments
XEP-0004	Data Forms	No comments
XEP-0016	Privacy Lists	No comments
XEP-0022	Message Events	No comments
XEP-0030	Service Discovery	No comments
XEP-0045	Multi-User Chat	No comments
XEP-0047	In-Band Bytestreams	No comments
XEP-0048	Bookmarks	No comments
XEP-0049	Private XML Storage	No comments
XEP-0054	vcard-temp	No comments
XEP-0055	Jabber Search	No comments
XEP-0065	SOCKS5 Bytestreams	No comments
XEP-0066	Out of Band Data	Implemented by Client
XEP-0071	XHTML-IM	Implemented by Client
XEP-0077	In-Band Registration	No comments
XEP-0078	Non-SASL Authentication	No comments
XEP-0079	Advanced Message Processing	No comments
XEP-0085	Chat State Notifications	Implemented by Client
XEP-0092	Software Version	No comments
XEP-0095	Stream Initiation	No comments
XEP-0096	SI File Transfer	No comments
XEP-0100	Gateway Interaction	No comments
XEP-0106	JID Escaping	No comments
XEP-0114	Jabber Component Protocol	No comments
XEP-0124	Bidirectional-streams Over Synchronous HTTP (BOSH)	No comments
XEP-0126	Invisibility	No comments
XEP-0153	vCard-Based Avatars	No comments
XEP-0160	Best Practices for Handling Offline Messages	No comments
XEP-0166	Jingle	Implemented by Client
XEP-0167	Jingle RTP Sessions	Implemented by Client

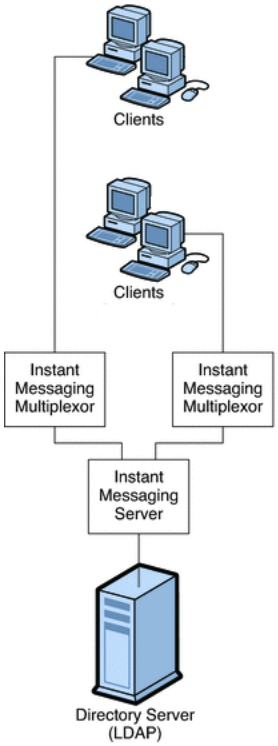
Table 2–1 (Cont.) Supported XMPP Extensions

Number	Name	Comments
XEP-0177	Jingle Raw UDP Transport Method	Implemented by Client
XEP-0191	Simple Communications Blocking	No comments
XEP-0206	XMPP Over BOSH	No comments
XEP-0107	User Mood	No comments
XEP-0108	User Activity	No comments
XEP-0118	User Tune	No comments
XEP-0163	Personal Eventing Protocol	No comments
XEP-0060	Publish-Subscribe	Partially implemented
XEP-0199	XMPP Ping	No comments

Instant Messaging Server Software Architecture

Figure 2–1 shows the Instant Messaging Server software architecture.

Figure 2–1 Instant Messaging Server Software Architecture



For Instant Messaging Server 9, clients send messages to the multiplexor, which forwards the messages to the Instant Messaging server. However, in Instant Messaging Server 8 and previous versions, a web server (or an application server with a web service embedded), downloads the Instant Messenger resources from a browser to the clients. The resource files make up the client. Clients send messages to one another through a multiplexor, which forwards the messages to the Instant Messaging server.

Directory Server stores and retrieves local user and group delivery information such as preferences, location, and to which multiplexor to route messages for this user. When the Instant Messaging server receives a message, it uses this information to determine where and how the message should be delivered. In addition, Directory Server can contain user information such as contact lists and subscriptions.

In this basic configuration, Instant Messaging Server directly accesses Directory Server to verify user login name and passwords for mail clients that use Instant Messaging.

Outgoing instant messages from clients go directly to the multiplexor. The multiplexor sends the message to the appropriate Instant Messaging server, which in turn forwards the message to another Instant Messaging server, or if the message is local, to the multiplexor with which the recipient is associated.

New users are created by adding user entries to Directory Server. Entries in the directory can be created through Instant Messaging Server (by enabling new-user registration feature) or changed by using the tools provided with Directory Server. You can then assign services to the user. For more information about new user registration for Instant Messaging Server, see the topic on administering end users in *Instant Messaging Server System Administrator's Guide*.

You administer Instant Messaging Server components through a set of command-line interfaces and text-based configuration files.

Note: Typical Instant Messaging Server deployments are not installed on a single machine. They also have additional features like multiplexing and high availability enabled. See "Planning Your Instant Messaging Server Installation" for more information.

Planning Your Instant Messaging Server Installation

This section contains the following planning topics you must consider before installing Instant Messaging Server:

Planning to Protect Instant Messaging Server

Instant Messaging Server supports Transport Layer Security (TLS). (Support for legacy SSL was removed in Instant Messaging Server 9.0.2.) Instant Messaging Server uses a startTLS extension to the TLS 1.0 protocol for client-to-server and server-to-server encrypted communications and for certificate-based authentication between servers.

When planning for SSL for Instant Messaging Server, keep in mind the following:

- You can secure the Instant Messaging Server deployment by enabling SSL on the web container port (either Web Server or Application Server) and accessing Instant Messaging Server functionality by using the XMPP/HTTP Gateway (httpbind).
- Set the proper file and directory permissions for the Instant Messaging Server configuration files (**im.conf.xml** and **httpbind.conf** in the *InstantMessaging_cfg*/**config** directory):
  - Solaris OS:

    ```
    /etc/opt/sun/comms/im/default/config/
    ```

  - Red Had Linux:

    ```
    /etc/opt/sun/im/default/config/
    ```

    Instant Messaging Server runs as the user specified in the **iim.conf.xml** file. This user needs read access to the file. If you use httpbind, the user that runs the web container should be able to access the Instant Messaging Server directory path and configuration file. When you create additional Instant Messaging server or multiplexor instances manually, you must also ensure that the file and directory permissions are correct. The default installation sets the file and directory permissions. The default instance directory has the following permissions:

    ```
    drwx------   5 root     other        512 Oct 16 14:24 default
    ```

- Take care while enabling Instant Messaging Server monitoring, as this exposes server statistics that could be considered security issues. The default configuration does not enable the monitoring feature. You enable this property through the **iim.conf.xml** file.
- Enable debug logging only when needed, as this impacts overall system performance. Though passwords are not logged, the protocol communication between users is logged, which could be a potential security issue.
- When you enable startTLS, use a single server certificate for both client-to-server and server-to-server communication.
- An Instant Messaging Server deployment that leverages LDAP needs proper authentication for access.

The Instant Messaging Server default installation supports only SASL Plain. If you require a higher level of security, use the Instant Messaging public Service Provider Interface. SASL Plain and jabber:iq:auth are two forms of plain text authentication. That is, in both, the password is sent in the clear (encoded perhaps, but still clear text) and so both are insecure forms of authentication. Nevertheless, this is an issue only if end-to-end encryption (through startTLS for direct socket connection, and HTTPS for httpbind) is not enabled. If end-to-end encryption is enabled, the password is not "seen" in the clear on the network.

Alternatively, if you do not want to transmit passwords in the clear (even if over an encrypted stream), use the Instant Messaging SPI for plugging in authentication mechanism's at the server side through SASLRealm. You can implement custom SASL mechanisms as implementations but you will then need an Instant Messaging client that supports this custom mechanism. The Instant Messaging client supports only SASL Plain, jabber:iq:auth (both insecure).

See *Instant Messaging Server Security Guide* for more information on using TLS.

Planning Instant Messaging User Authentication

User authentication enables your users to log in through their Instant Messaging clients to chat and access other features of Instant Messaging.

Instant Messaging Server and Passwords

User IDs and passwords are stored in your LDAP directory. Password security criteria, such as minimum length, are determined by directory policy requirements. Password security criteria is not part of Instant Messaging Server administration. See the Directory Server documentation to understand directory server password policies.

Instant Messaging Server and LDAP

All Instant Messaging Server deployments require a directory server to perform end user authentication and to search for end users. For various ways to secure the directory, see the Directory Server documentation.

The default Instant Messaging Server configuration makes the following assumptions regarding the schema used by this directory:

- End user entries are identified by the **inetOrgPerson** object class.
- Group entries are identified by the **groupOfUniqueNames** or **groupofURLs** object class.
- Instant Messenger user ID attribute of an end user is provided by the **uid** attribute (from **inetOrgPerson** objectclass).
- The email address of an end user is provided by the **mail** attribute.
- The display name of an end user or group is provided by the **cn** attribute.
- The list of members of a group is provided by the **uniqueMember** attribute (**groupOfUniqueNames** object class).

Note: Some user attributes might contain confidential information. Ensure that your directory access control is set up to prevent unauthorized access by non-privileged users.

Planning for Anonymous Directory Server Searching

Instant Messaging Server needs to be able to search the directory to function correctly. You need to ensure that your directory is configured to be searchable by anonymous users. If your directory is not readable or searchable by anonymous users, you must take configuration additional steps.

For more information, see *Instant Messaging Server Security Guide*.

Planning Instant Messaging Server Privacy, Security, and Site Policies

Instant Messaging Server provides the ability to control access to Instant Messaging Server features and preserve end-user privacy.

Instant Messaging Server Site Policies

Site policies specify end-user access to specific functionality in Instant Messaging Server. When developing your site policies for Instant Messaging Server, keep in mind the following questions:

- Can users access the presence status of other end users?

- Can users send alerts to other end users?
- Do you want users to save properties on the server?
- Who do you want to be able to create and manage conference rooms?
- Who do you want to be able to create and manage news channels?

For more information, see *Instant Messaging Server Security Guide*.

Controlling Instant Messaging Server End User and Administrator Privileges

Different sites using Instant Messaging Server have different needs in terms of enabling and restricting the type of access end users have to the Instant Messaging service. The process of controlling end user and administrator Instant Messaging Server features and privileges is referred to as *policy management*. You can manage policies to adjust end-user privileges in the following areas: news channel management, conference room management, the ability to change preferences in the User Settings dialog, and ability to send alerts. It also enables specific end users to be assigned as system administrators.

For more information, see *Instant Messaging Server Security Guide*.

Planning to Protect the Instant Messaging Archive

Instant Messaging Server has the capability to archive instant messages for later retrieval and searching. If you enable the email archive, you must decide which administrators are to receive email containing archived instant messages. You can configure a separate list of administrators to receive polls, news, conference, alerts, or chat sessions. You can also configure Instant Messaging Server to use the extended RFC 822 header. Doing so enables mail clients to filter messages based on the header content.

Planning for a Basic Installation

The basic Instant Messaging Server architecture provides such functionality as presence, roster management, chat, news alerts, and conferences. To provide this basic functionality, you need to install the following components:

- Instant Messaging server and one or more Instant Messaging multiplexors:
- LDAP server such as Directory Server

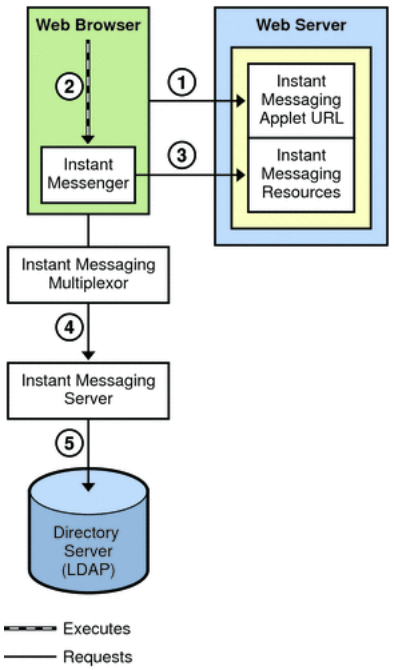
In the basic architecture:

- The LDAP server provides user entries for authentication and lookup.
- The clients download the Instant Messaging resources from either a web server or Application Server
- Clients always connect to the Instant Messaging server through an Instant Messaging multiplexor.

Authentication in a Basic Architecture

Figure 2–2 shows the interaction of the software components in the authentication process of a basic architecture of Instant Messaging Server. The focus is on the flow of authentication requests. An explanation of the steps in this process follows the figure.

Figure 2–2 Flow of Authentication Requests in a Basic Instant Messaging Server Architecture



The authentication process in a basic architecture works as follows:

1. End user accesses the Instant Messenger applet URL from a browser and chooses a method to invoke the client.
2. The browser invokes Java Web Start or the Java plugin.
3. Java Web Start or the Java plugin downloads the necessary Instant Messenger resource files and starts Instant Messenger.
4. The login window appears and the end user enters the login name and password. The login data is sent to the Instant Messaging server through the multiplexor.
5. The Instant Messaging server communicates with the LDAP server to authenticate the end user and to request end-user information, such as contact lists or subscriptions.

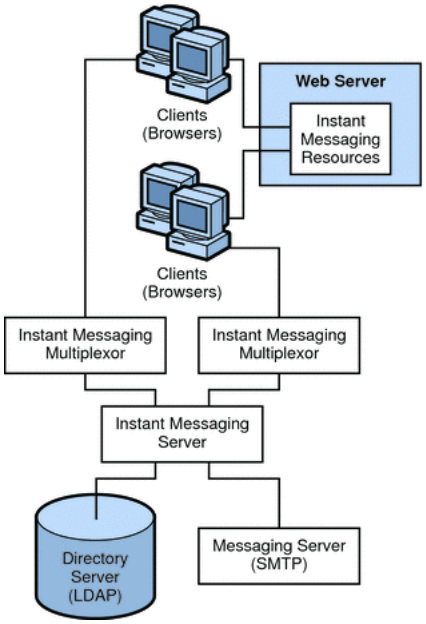
When the end-user authentication is complete, the Instant Messaging main window appears, displaying the contact list for the end user. The end user can now start and participate in Instant Messaging sessions with the other end users.

Planning for Email Notification (Calendar Alert) Architecture

Figure 2–3 shows an Instant Messaging Server deployment that supports email notification to offline users, as well as Instant Messaging based notification of calendar events to users.

An Instant Messaging Server architecture that supports email notification and calendar alerts provides the same functionality as Basic Instant Messaging Architecture. To provide this functionality, you need to include the components listed in "Planning for a Basic Installation". To support email alerts, you also install an SMTP server such as Oracle Communications Messaging Server. To support calendar alerts, you also install Oracle Communications Calendar Server.

Figure 2–3 Instant Messaging Architecture with Email Notification



To enable email notification, you are prompted during installation to identify the SMTP server to use with Instant Messaging. If you do not have an SMTP server installed, you must install one before installing the Instant Messaging software.

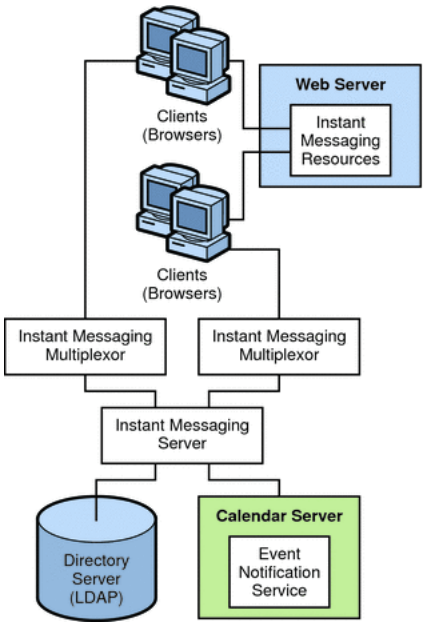
Authentication flow in this architecture is the same as in a basic deployment. See "Authentication in a Basic Architecture" for more information.

In this example:

- The LDAP server provides user entries for authentication and lookup.
- The Instant Messaging server forwards messages intended for offline users to the SMTP server. The SMTP server then sends the message as an email to the user's mailbox.
- The clients download the Instant Messaging resources from a web server (or application server).
- Clients always connect to the Instant Messaging server through an Instant Messaging multiplexor.

Figure 2–4 shows Instant Messaging Server with calendar notification enabled on the network. If you do not have Calendar Server installed, you must install it before installing the Instant Messaging software.

Figure 2–4 Instant Messaging Architecture with Calendar Alerts



In this example:

- The LDAP server provides user entries for authentication and lookup.
- The Event Notification Server (ENS) sends notifications of calendar events to the Instant Messaging server which then forwards the notification on to the appropriate end user.
- The clients download the Instant Messaging resources from a web server (or application server).
- Clients always connect to the Instant Messaging server through an Instant Messaging multiplexor.

Planning for Instant Messaging With All Features Enabled

To deploy Instant Messaging Server and enable all the features listed in this section, you must first install the following components prior to installing Instant Messaging Server:

- Directory Server
- Web Server
- Calendar Server
- Messaging Server

System Deployment Planning

This section contains the following system-level planning topics you must consider before installing Instant Messaging Server:

Planning for High Availability

Configuring Instant Messaging Server for high availability (HA) provides monitoring and recovery from software and hardware failures. The HA feature is implemented as a failover data service and not as a scalable service. This feature is supported only on the Oracle Solaris operating system.

For more information, see the topic on configuring Instant Messaging Server for HA in *Instant Messaging Server System Administrator's Guide*.

Providing Instant Messaging Client Access Through a Firewall

The XMPP/HTTP Gateway (httpbind) provides Instant Messaging access to XMPP-based clients, such as HTML based clients, and clients that are behind firewalls that allow HTTP traffic only and do not permit XMPP traffic. The gateway proxies Instant Messaging Server traffic to the XMPP server on behalf of HTTP clients.

When planning to use the XMPP/HTTP Gateway, keep in mind the following:

- Use port 5222 at the Gateway if the Gateway is communicating to the server through a multiplexor. Also, use port server port 5269 if no multiplexor is involved. You can specify port 5222 or 5269 in the **httpbind.conf** file.
- The XMPP/HTTP gateway supports startTLS and legacy SSL. If you want legacy SSL support, enable SSL on the Web Server port. If you want startTLS support, enable startTLS on the server and all communications is encrypted.
- Do not expose the Instant Messaging server to direct access. In a typical deployment scenario, locate the multiplexor in the DMZ, and open the multiplexor to server communication port (45222 usually) in the second firewall.

Using Load Balancing

Instant Messaging Server supports the use of load balancers located in front of the Instant Messaging multiplexors. However, you cannot currently use load balancers between the Instant Messaging multiplexors and the Instant Messaging server.

Planning Backup Strategies

Backing up and restoring data is one of the most important administrative tasks for your Instant Messaging Server deployment. You must implement a backup and restore policy for your Instant Messaging Server deployment to ensure that data is not lost if the system crashes, hardware fails, or information is accidentally deleted.

You must back up the following Instant Messaging Server information:

- Configuration Information
- Instant Messaging end user data
- Instant Messenger resources

The configuration information is stored in the configuration directory (*InstantMessaging_cfg*). The Instant Messaging data is stored in the database directory (*InstantMessaging_database*).

The Instant Messenger resources must be backed up if they have been customized. The location of the Instant Messenger resources are provided during installation.

For more information on backing up your Instant Messaging Server deployment, see *Instant Messaging Server System Administrator's Guide*.

Sample Instant Messaging Server Physical Architecture

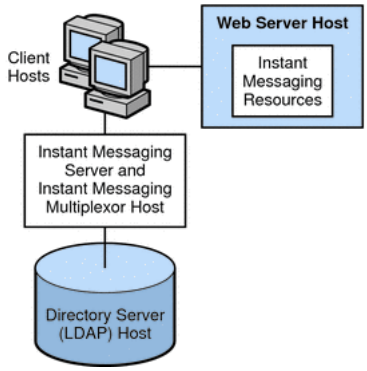
This section explains variations to the deployment scenario described in "Planning for a Basic Installation". For example, you can install the various required servers and components in the following physical configurations, or any combination of each example:

- Physical Deployment Example: Web Server on Separate Host
- Physical Deployment Example: Multiplexors on Separate Hosts
- Physical Deployment Example: Multiple Instant Messaging Hosts

Physical Deployment Example: Web Server on Separate Host

Figure 2–5 shows a configuration consisting of the Instant Messaging server and multiplexor installed on the same host. The web server is installed on a separate host. The Instant Messaging resources are also present on the web server host. Use this configuration when there is an existing instance of a web server and an LDAP server, and you do not want to install other applications on these hosts.

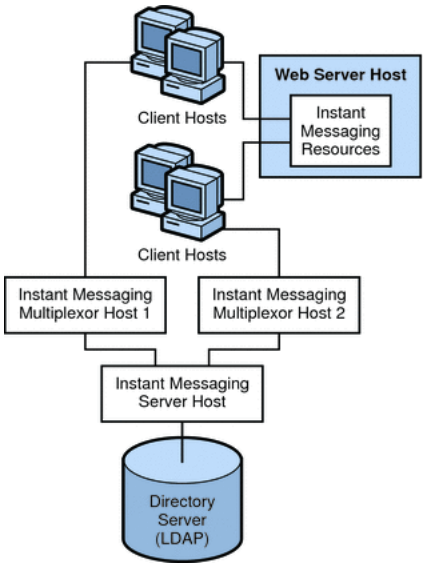
Figure 2–5 Separate Web Server and Instant Messaging Hosts



Physical Deployment Example: Multiplexors on Separate Hosts

Figure 2–6 shows a configuration consisting of two multiplexors installed on two separate hosts. The Instant Messaging server is installed on a different host. This configuration enables you to place a multiplexor outside your company's firewall. Installing multiplexors on multiple hosts distributes the load of Instant Messaging Server across multiple systems.

Figure 2–6 Instant Messaging Multiplexors Installed on Separate Hosts

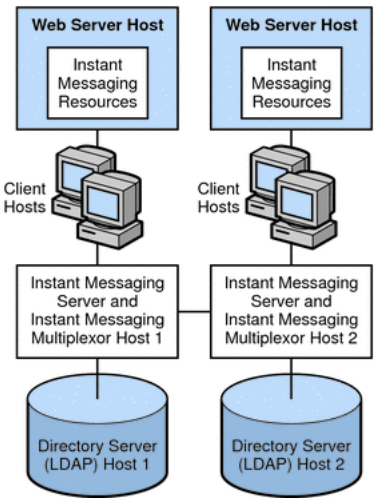


Note: The multiplexor can be resource-intensive, so putting it on a separate host can improve the overall performance of the system.

Physical Deployment Example: Multiple Instant Messaging Hosts

Figure 2–7 shows a configuration consisting of two Instant Messaging servers. This configuration is used when the site contains multiple administrative domains. The server configuration on each Instant Messaging server host has to be set up so that end users on one Instant Messaging server can communicate with end users on other Instant Messaging servers.

Figure 2–7 Multiple Instant Messaging Server Hosts



About Installing a Secure System

In conjunction with the TLS protocol, Instant Messaging Server provides client-to-server and server-to-server encrypted communications as well as certificate-based authentication between servers. For information about secure installation and configuration of Instant Messaging Server, see *Instant Messaging Server Security Guide*.

3

Instant Messaging Server System Requirements

This chapter describes the hardware, operating system, software, and database requirements for installing Oracle Communications Instant Messaging Server.

Software Requirements

This section describes the software and information requirements to install Instant Messaging Server.

Supported Operating Systems

Table 3–1 lists operating systems that support Instant Messaging Server.

Table 3–1 Instant Messaging Server Operating System Requirements

Operating System	CPU	Required Patches
Solaris OS 11	SPARC, x64	See the Solaris 11 Release and Installation documentation for more information.
Oracle Linux 6 and Red Hat Enterprise Linux 6 64-bit	x64	See the Oracle Linux documentation and Red Hat Enterprise Linux documentation for more information.

Required Software

Table 3–2 lists other software required for installing and running Instant Messaging Server.

Table 3–2 Instant Messaging Server Software Requirements

Product	Version	Notes
Oracle Directory Server Enterprise Edition (formerly Sun Java System Directory Server)	6.x, 7, 11gR1	If doing a fresh installation, use 11gR1.
Java	7	Java 7u45 is the latest version at time of this writing. Use the most current version.

Table 3–2 (Cont.) Instant Messaging Server Software Requirements

Product	Version	Notes
Oracle Communications Converged Application Server	5.1	Required for Instant Messaging Server 9 SIP/SIMPLE deployments.

Client Requirements

As of Instant Messaging Server 9, the product no longer ships with the Instant Messaging client. Pidgin is the tested and supported XMPP client. Ideally any XMPP-compliant client should work with Instant Messaging Server.

Hardware Requirements

The number and configuration of the systems that you employ for your Instant Messaging Server installation depends on the scale and the kind of deployment you have planned.

Note: The sizing estimates in this section assume proper application configuration and tuning, in a manner consistent with leading practices of Oracle Communications consulting and performance engineering. This information is provided for informational purposes only and is not intended to be, nor shall it be construed as a commitment to deliver Oracle programs or services. This document shall not form the basis for any type of binding representation by Oracle and shall not be construed as containing express or implied warranties of any kind. You understand that information contained in this document will not be a part of any agreement for Oracle programs and services. Business parameters and operating environments vary substantially from customer to customer and as such not all factors, which may impact sizing, have been accounted for in this documentation.

Table 3–3 provides the minimum hardware requirements for Instant Messaging Server installed on a single managed server in a GlassFish Server domain.

Table 3–3 Instant Messaging Server Minimum Hardware Requirements

Component	Requirement
Disk Space	Approximately 300 MB required for Instant Messaging Server software.
RAM	At least 256 MB of RAM. The amount of RAM needed depends on the number of concurrent client connections, and whether the server and multiplexor are deployed on the same host.

Information Requirements

During Instant Messaging Server installation, you must enter values for configuration items such as host names and port numbers. This section describes the information that you must provide during the installation and initial configuration process.

Component Information

Table 3–4 lists the component information that you provide during initial configuration.

Table 3–4 Component Information

Information Type	Default Value
Server components	**Selected**
Web components	**Selected**

Service Runtime Information

Table 3–5 lists the service runtime information that you provide during initial configuration.

Table 3–5 Service Runtime Information

Information Type	Default Value	Comments
Runtime user ID	**inetuser**	If the **configure** utility does not create a UNIX user, you need to create it manually. After you create the user for Instant Messaging Server, set permissions appropriately for the directories and files owned by that user. Do not choose **root** as a server user ID.
Runtime group ID	**integroup**	If the **configure** utility does not create a UNIX group, you need to create it manually. After you create the group for Instant Messaging Server, set permissions appropriately.
Runtime directory	**/var/opt/sun/comms/im**	Runtime files are read, created, and modified by the server during its normal operations. Some examples include log files, and persistent state information tied to client actions such as roster information, conferences, and so on. If you are configuring Instant Messaging Server for high availability, this path must be globally available. The **configure** utility appends a directory (**/default**) to the path you provide for the runtime files. The name of this directory is the instance to which the runtime files apply. Later, you can create multiple Instant Messaging Server instances by creating additional instance directories with different names (for example **/secure**) and copying over files from the **/default** instance runtime directory.

Network Access Information

Table 3–6 lists the network access information that you provide during initial configuration.

Table 3–6 Network Access Information

Information Type	Default Value	Comments
Domain name	*domain name of host*	No comment.
XMPP port	**5222**	The port number on which the Instant Messaging server listens for incoming requests from Instant Messenger clients.
Gateway connector port	**55222**	The port number on which you communicate with external Facebook instant messaging users.
Multiplexed XMPP port	**45222**	The port number on which the Instant Messaging server listens for incoming requests from the multiplexor.
XMPP Server Port	**5269**	The port number on which the Instant Messaging server listens for incoming requests from other Instant Messaging servers. In addition, if no multiplexor is installed, the server listens for incoming requests from Instant Messenger clients on this port. The port is also used by components such as HTTPBIND gateway, Calendar Agent, and the SMS gateway for creating a component session with the serve
Disable server (enable only multiplexor)	**No**	Select this option if the instance you installed acts as a multiplexor and not a server. If you select this option, you must provide a value for Remote Instant Messaging Server Host Name.
Enable SSL	**Yes**	When enabling SSL, you are prompted for a keystore file and password file. Also, the respective server configuration is mandatorily set to TLS for all communication. To disable mandating TLS, set **iim_server.requiressl** to **false** by using the **imconfutil** command.
Server keystore file	No default value.	No comment.
Server password file	No default value.	No comment.

If you decide to enable SSL, the respective server configuration is mandatorily set to TLS for all communication. To disable mandating TLS, set **iim_server.requiressl=false** by using the **imconfutil** command.

LDAP Information

Table 3–7 lists the LDAP information that you provide during initial configuration.

Table 3–7 LDAP Information

Information Type	Default Value	Comments
LDAP host name	*FQDN of host*	In a deployment with an LDAP server, specifies the host name of the LDAP server that contains user and group information for Instant Messaging. For example, **directory.example.com**. Dependencies: LDAP server such as Oracle Directory Server Enterprise Edition (formerly Sun Java System Directory Server Enterprise Edition).
LDAP port number	**389**	In a deployment with an LDAP server, specifies the port number on which the directory server listens for incoming requests. For example, **389**. Dependencies: LDAP server such as Oracle Directory Server Enterprise Edition (formerly Sun Java System Directory Server Enterprise Edition).
SSL enabled	**No**	No comment.
Base DN	**dc=siroe,dc=com**	In a deployment with an LDAP server, specifies the base distinguished name in the directory tree that contains user and group information for Instant Messaging. For example, **o=example.com**. Dependencies: LDAP server such as Oracle Directory Server Enterprise Edition (formerly Sun Java System Directory Server Enterprise Edition).
Directory manager DN	**Directory Manager**	Instant Messaging Server uses this Bind DN to search users and groups in the directory. Leave this blank if the directory can be searched anonymously. You can change the bind credentials later if required. Dependencies: LDAP server such as Oracle Directory Server Enterprise Edition (formerly Sun Java System Directory Server Enterprise Edition).
Directory manager password	No default value.	In a deployment with an LDAP server, the Bind DN password.

Email Information

Table 3–8 lists the email information that you provide during initial configuration.

Table 3–8 Email Information

Information Type	Default Value	Comments
Enable Email Integration	**Yes**	If selected, enables Instant Messaging Server email integration. Dependencies: SMTP Server such as Oracle Communications Messaging Server
SMTP Server	**smtphost**	The host name of the SMTP server used to send email notification of messages to offline users. For example, **mail.example.com**. If the SMTP server does not use port 25, specify the port along with the host name. For example, if the SMTP server uses port 1025, then use **mail.example.com:1025**. Dependencies: SMTP server such as Oracle Communications Messaging Server.
Enable email archiving	**yes**	If selected, enables Instant Messaging Server email archiving. Dependencies: SMTP Server such as Oracle Communications Messaging Server

HTTP Gateway Information

Table 3–9 lists the HTTP gateway information that you provide during initial configuration.

Table 3–9 HTTP Gateway Information

Information Type	Default Value	Comments
Deploy IM HTTP gateway	**Yes**	Determines if the XMPP/HTTP gateway is deployed. If you choose to deploy the gateway, the **configure** utility creates a default gateway configuration file (**httpbind.conf**) in the default Instant Messaging server instance's *InstantMessaging_cfg* directory if one does not already exist. If **httpbind.conf** already exists, the **configure** utility does not alter or overwrite the file. If you are configuring Instant Messaging Server to support Convergence, do not enable the XMPP/HTTP Gateway Deployment here. Set this value to **false**. The XMPP/HTTP Gateway is deployed through the Convergence server. Its value is set when you configure Convergence.
Context root	**http://***imhost***:80/httpbind**	Defines the URI for the HTTP component of the XMPP/HTTP gateway.
Web container path	*Web container base directory*	No comment.
Web administrator URL	No default value.	No comment.
Web administrator user ID	**admin**	No comment.
Web administrator password	No default value.	No comment.

Calendar Agent Information

Table 3–10 lists the calendar agent information that you provide during initial configuration.

Table 3–10 Calendar Agent Information

Information Type	Default Value	Comments
Enable calendar agent	**No**	If you choose to enable the Calendar agent, you need to provide the following information: From the **configure** panel: ■ Choose to Enable Calendar Agent by typing **yes** ■ Choose to Enable local component by typing **yes** ■ Specify XMPP server host name ■ Specify XMPP server port ■ Specify JMQ user name ■ Specify JMQ password ■ Specify Notification Server host name ■ Specify Notification Server port ■ Specify Topic If you choose not to enable the Calendar agent, you can manually configure the Calendar agent later.
Enable local component	**No**	No comment.

SMS Gateway Information

Table 3–11 lists the Short Message Services gateway information that you provide during initial configuration.

Table 3–11 SMS Gateway Information

Information Type	Default Value	Comments
Enable SMS gateway	**No**	Enables the Instant Messaging server to deliver chat messages and alerts in the form of SMS to the Instant Messaging users who are offline.
Enable local component	**No**	No comment.

Facebook Gateway Information

Table 3–12 lists the Facebook gateway information that you provide during initial configuration.

Table 3–12 Facebook Gateway Information

Information Type	Default Value	Comments
Enable Facebook gateway	**No**	Enables you to communicate with Facebook instant messaging servers. Enter **Yes** if you want to enable the gateway on the server. Then enter the Facebook API Key, Facebook API Secret, and Gateway Connectors (*host*:*port*).

Services Information

Table 3–13 lists the Instant Messaging services startup information that you provide during initial configuration.

Table 3–13 Services Information

Information Type	Default Value
Start services after successful configuration	**Yes**
Start services when system starts	**Yes**

4

Instant Messaging Server Pre-Installation Tasks

This chapter describes the pre-installation tasks that you must complete before you can install Oracle Communications Instant Messaging Server.

Pre-installation and configuration tasks include:

- Installing Java
- Installing Directory Server

Installing Java

The 32-bit and 64-bit JDKs require manual installation. Install both JDKs, rather than the JRE, on your Instant Messaging Server hosts.

To get the Java software, go to the Java SE Downloads at:

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

For information about installing Java, see the Installing Java for Communications Suite documentation at:

https://wikis.oracle.com/display/CommSuite/Installing+Java+For+Communications+Suite+7.0.6

Installing Directory Server

Instant Messaging Server uses Oracle Directory Server Enterprise Edition to store and access LDAP data for individual users, groups, and domains.

If you need to install Directory Server (that is, your site does not currently have Directory Server deployed), see the Oracle Directory Server Enterprise Edition documentation at:

http://docs.oracle.com/cd/E29127_01/index.htm

Prior to installing and configuring Instant Messaging Server, you must also prepare the Directory Server LDAP schema by running the **comm_dssetup.pl** script. This script, which is provided as part of the Unified Communications Suite installer, adds the necessary Communications Suite schema to the LDAP. See "Preparing Directory Server" for more information.

Some additional LDAP object classes were added to the Communications Suite schema specifically to support Instant Messaging Server. To understand the schema that is used by Instant Messaging Server, refer to *Communications Suite Schema Reference* at:

https://wikis.oracle.com/display/CommSuite/Communications+Suite+Schema+Reference

5

Installing Instant Messaging Server

This chapter describes how to install and configure Oracle Communications Instant Messaging Server. After you install the Instant Messaging Server software by using the Communications Suite installer, you must configure Instant Messaging Server to complete the installation. You use the Instant Messaging Server configuration command-line utility, **configure**, to perform this initial runtime configuration.

Before installing Instant Messaging Server, read these chapters:

- Instant Messaging Server Installation Overview
- Planning Your Instant Messaging Server Installation
- Instant Messaging Server System Requirements
- Instant Messaging Server Pre-Installation Tasks

Installation Assumptions

The instructions in this chapter assume:

- You are deploying Instant Messaging Server on a single host, or multiple hosts or Solaris zones.
- A Directory Server host is already installed.

Installing Instant Messaging Server

The tasks to install Instant Messaging Server are as follows:

- Downloading the Instant Messaging Server Software
- Preparing Directory Server
- Installing the Instant Messaging Server Software
- Configuring Instant Messaging Server After Installation

Downloading the Instant Messaging Server Software

1. Download the media pack for Oracle Communications Unified Communications Suite, which contains the Instant Messaging Server software, from the Oracle software delivery website, located at:

   `http://edelivery.oracle.com/`

2. Copy the Communications Suite distribution ZIP file to a temporary directory on your Instant Messaging Server hosts and extract the files.

Preparing Directory Server

To prepare Directory Server:

1. On your Directory Server hosts, install and run the **comm_dssetup.pl** script from the Communications Suite distribution.

   For more information, see the Communications Suite Directory Server Setup Script documentation at:

   https://wikis.oracle.com/display/CommSuite/Communications+Suite+7.0.6+Directory+Server+Setup+Script+(comm_dssetup.pl)

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

2. (Optional) Provision users in the Directory Server.

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

   https://wikis.oracle.com/display/CommSuite/Communications+Suite+Schema+Reference

Installing the Instant Messaging Server Software

You install the Instant Messaging Server software by running the Communications Suite installer. The installer is a single unified utility called **commpkg**. It installs (but does not configure) the Instant Messaging Server software. You configure Instant Messaging Server after first installing the software (see "Configuring Instant Messaging Server").

To install the Instant Messaging Server software:

1. Go to the directory where you unzipped the Communications Suite distribution files.
2. Run the Communications Suite Installer.

   ```
   ./commpkg install
   ```

   For more information about running the installer, see the **commpkg install** usage documentation at:

   https://wikis.oracle.com/display/CommSuite/commpkg+install+7.0.6+Usage

3. Select **Instant Messaging Server** and proceed with the installation.

   The default installation directory for Instant Messaging Server is **/opt/sun/comms/im**.

Configuring Instant Messaging Server

After you install the Instant Messaging Server software by using the Communications Suite installer, you must configure Instant Messaging Server to complete the installation. You use the Instant Messaging Server configuration command-line script, **configure**, to perform this initial runtime configuration.

Creating a UNIX System User and Group

System users run specific server processes. Certain privileges need to be designated for these users to ensure they have appropriate permissions for the processes they run. Normally, the **configure** utility creates the following users and groups:

- User: **inetuser**
- Group: **inetgroup**

If the **configure** utility does not create a UNIX user and group for Instant Messaging Server, you need to create them manually as described in this section. After you create the user and group, set permissions appropriately for the directories and files owned by that user.

Do not choose **root** as a server user ID.

To create the appropriate UNIX user and group:

1. Log in as superuser (**root**).
2. Create a group to which your system user belongs. For example, to create a group named **imgroup** on an Oracle Solaris platform, enter the following command:

   ```
   groupadd imgroup
   ```

3. Create the system user and associate it with the group you just created. In addition, set the password for that user. For example, to create a user named **imuser** and associate it with the group **imgroup** on an Oracle Solaris platform, enter the following command:

   ```
   useradd -g imgroup imuser
   ```

   For more information on adding users and groups, refer to your operating system documentation.
4. Examine the **/etc/groups** file to ensure that the user and group were added.

Running the configure Utility

After you install Instant Messaging Server, use the **configure** utility to configure the software and to generate the configuration files.

This section contains the following topics:

Syntax and Options of the configure Utility

This section describes the **configure** utility's syntax.

configure Syntax

configure [*options*]

configure Options

Table 5–1 shows the options for the **configure** utility.

Note: The **--id**, **--noconsole**, and **--loglevel** options were removed in Instant Messaging Server 8.

Table 5–1 Configure Options

Option	Description
--nodisplay	Required if the **--silent** option is not used. Optional if the **--silent** option is used. Use this option to configure Instant Messaging Server in command-line mode.
--help	Optional. Displays the help content for this command.
--verbose	Optional. Prints information messages to the standard output.
--savestate *statefilename*	Optional. Should be used with the **--nodisplay** option. If you use this option, the inputs that you provide during configuration are saved in the state file. Specify the name and location of the state file along with this option. Your responses are stored as a list of parameters in the state file. Each parameter represents a single entry or field value.
--silent *statefilename*	Required if the **--nodisplay** option is not used. Use this option to run the **configure** utility in the silent mode. Specify the name and path of the state file with this option. If you are configuring Instant Messaging Server by using a state file, you are not prompted to specify the configuration information. Instead, the values from the state file are used to configure the server.
--state *statefilename*	Optional. During configuration, the **configure** utility provides default values for configuration. You can either use the default values or specify your own value. If you use this option, the **configure** utility uses all the default values for configuration.
--no	Optional. Use this option to perform a dry run of the configuration.
--novalidate	Optional. If you use this option, the **configure** utility does not validate the inputs that you provide during configuration.
--debug	Optional. Use this option to view the debug messages on your terminal.

Note: The **configure** utility ignores any incorrect or invalid command-line options and proceeds with the configuration process by using the valid options.

Configuring Instant Messaging Server After Installation

1. Change to the *InstantMessaging_home***/sbin** directory. By default, the *InstantMessaging_home* directory is **/opt/sun/comms/im**.
2. Use one of the following options to run the **configure** utility.
   - Command-line:

     ```
     configure --nodisplay
     ```

   - From a state file:

     ```
     configure --silent statefile
     ```

where *statefile* is the path to the state file you want to use. If you are configuring by using a state file and using the **--silent** option, you are not be prompted for configuration information. Instead, the values from the state file are used to configure the software. See "Performing a Silent Instant Messaging Server Configuration" for information on generating a state file. If you are not performing a silent installation, a series of prompts appears, requesting information that sets up the initial configuration for Instant Messaging Server. The prompts that appear vary depending on the components you installed. Fill in the requested information using the values from your Instant Messaging Server checklist. See "Configuring Instant Messaging Server".

Note: Do not select the Disable Server option.

3. To use the XMPP/HTTP Gateway, modify the location of the default log file for the XMPP/HTTP Gateway in the **httpbind_log4j.conf** file.

   You need to do this on Linux, however, you only need to do this on Oracle Solaris if you chose to use a location for logs other than the default.

   To do this:

   a. Open the **httpbind_log4j.conf** file. This file is stored at the location you specified in the **httpbind.conf** file as the value for the **httpbind.log4j.config** parameter. By default the file is stored in the following directory under the default Instant Messaging Server instance: *InstantMessaging_cfg_home*/**httpbind_log4j.conf**.

   b. Set the value of the **log4.appender.appender_ID.file** parameter to the location where log files are stored. By default, on Red Hat Linux and Oracle Linux, this value is **/var/opt/sun/im/default/log**. If you chose another location for log files when you ran configure, enter that path as the value for the parameter.

   c. Configure client systems to support Instant Messaging Server.

Note: If **httpbind** and **im** are configured to run on different hosts, you must explicitly add the **c2s** protocol to the **s2s** listener by using the **imconfutil** command to set the **set-listener-prop** property. This is common for all components, and not just **httpbind**. If **httpbind** or any other component is enabled on the same machine during **im** configuration, this step is not required, as it is automatically carried out by the **configure** utility.

Performing a Silent Instant Messaging Server Configuration

To run a silent configuration, you first complete a false configuration to create a state file. During this false configuration session, your responses to the **configure** utility are captured in the state file, but no software is modified. In the state file, your responses are retained as a list of parameters, each representing a single prompt or field.

You can then run the **configure** utility on many hosts by using the state file as input. This process enables you to quickly propagate one configuration across multiple hosts in your enterprise. See "Syntax and Options of the configure Utility" for information on using the state file to configure a new instance of Instant Messaging Server.

To generate a state file:

1. Log in as superuser (**root**).

2. Change to the *InstantMessaging_home*/**sbin** directory. By default, the *InstantMessaging_home* directory is **/opt/sun/comms/im**.
3. Run the **configure** utility by entering the following:

   ```
   configure --no --nodisplay --saveState statefile
   ```

   Where *statefile* is the name you want to use for the state file. To use the state file to configure a different installation of Instant Messaging Server, use the following command:

   ```
   configure --nodisplay --silent statefile
   ```

   As you proceed through the **configure** utility, your answers are captured in the state file. When you complete the configuration, the state file is available in the location that you specified.

Examples of the configure Utility

This section provides **configure** utility examples.

- To configure and save the inputs that you provide in the state file:

  ```
  ./configure --nodisplay --savestate /tmp/imstate
  ```

- To configure and use the values from the state file:

  ```
  ./configure --nodisplay --state /tmp/imsilent
  ```

- To configure through the silent mode and use the values from the state file:

  ```
  ./configure --silent statefile
  ```

- To configure and use the values from the state file:

  ```
  ./configure --nodisplay --state /tmp/imsilent --savestate /tmp/imstate --no
  ```

  The command saves a state file. It does not perform the actual configuration as the **--no** option is used.

Sample configure Utility Configuration Responses

The following shows a sample configuration in response to prompts presented by the **configure** utility. The configuration uses default values for all options.

- Component Selection

  ```
  Select all components you wish to configure.

  1. [X] Server components
  2. [X] Web components
  ```

- Service Runtime Options

  ```
  Runtime User ID : [inetuser]
  Runtime Group ID: [inetgroup]
  Runtime Directory [/var/opt/sun/comms/im]
  ```

- Network Access Points

  ```
  Domain Name example.com
  XMPP Port [5222]
  Multiplexed XMPP Port [45222]
  Gateway Connector Port [55222]
  ```

```
XMPP Server Port [5269]
Disable Server (enable only multiplexor) [no]
Enable SSL [yes]:
Server keystore file:
Server password file:
```

If you decide to enable SSL, the respective server configuration is mandatorily set to TLS for all communication. To disable mandating TLS, set **iim_server.requiressl=false** by using the **imconfutil** command.

- LDAP Configuration

```
LDAP Host Name [imhost.siroe.com]
LDAP Port Number [389]
SSL Enabled [no]
Base DN [dc=siroe,dc=com]
Base DN cn=Directory Manager
Base Password
```

- Mail Server Options

```
Enable Email Integration [yes]
SMTP Server [smtphost]
Enable Email Archiving [yes]
```

- HTTP Gateway Deployment Configuration

```
Deploy IM HTTP Gateway [yes]
Context Root [http://imhost:80/httpbind]
Web Container Path [Web container base directory]
Web Administrator URL [ ]
Web Administrator User ID [admin]
Web Administrator Password
```

- Calendar Agent configuration

```
Enable Calendar Agent [no]
Enable local component [no]
```

- SMS Gateway Configuration

```
Enable SMS Gateway [no]
Enable local component [no]
```

- Facebook Gateway Configuration

```
Enable Facebook Gateway [no]
```

- Instant Messaging Server Services Startup

```
Start Services After Successful Configuration [yes]
Start Services When System starts [yes]
```

Creating Multiple Instances from a Single Instant Messaging Server Installation

You can create multiple instances of Instant Messaging Server on a single host from one installation. You might want to do this to create a secure version of Instant Messaging Server, or to support multiple directory namespaces. A namespace is a node in the directory under which each UID is unique. All instances of Instant Messaging Server on a single host share binaries but have unique versions of runtime and configuration files.

To Create an Additional Instance of Instant Messaging Server

This procedure assumes that you have used default installation and configuration values for the *InstantMessaging_home* and *InstantMessaging_runtime* directories. If you installed using default values, the original runtime directory for Oracle Solaris is:

```
/var/opt/sun/comms/im/default
```

For Red Hat Linux and Oracle Linux, the original runtime directory is:

```
/var/opt/sun/im/default
```

If you used paths other than the defaults, substitute your paths for the paths used in this procedure.

1. Create a runtime directory for the new instance. For example, to create runtime directory **xyz** on Oracle Solaris, type:

   ```
   mkdir /var/opt/sun/comms/im/xyz
   ```

   On Red Hat Linux and Oracle Linux, type:

   ```
   mkdir /var/opt/sun/im/xyz
   ```

2. Create a log directory for the new instance. For example, to create log directory **xyz**, on Oracle Solaris, type:

   ```
   mkdir /var/opt/sun/comms/im/xyz/log
   ```

   On Red Hat Linux and Oracle Linux, type:

   ```
   mkdir /var/opt/sun/im/xyz/log
   ```

3. If you are using a file-based property store for user data, you need to create a database directory (*InstantMessaging_database*) for the new instance. For example, to create database directory **xyz**, on Oracle Solaris, type:

   ```
   mkdir /var/opt/sun/comms/im/xyz/db
   ```

   On Red Hat Linux and Oracle Linux, type:

   ```
   mkdir /var/opt/sun/im/xyz/db
   ```

4. Copy the contents of the *InstantMessaging_home* directory and all of its subdirectories into the newly created directories: For example, on Oracle Solaris, type:

   ```
   cp -r /etc/opt/sun/comms/im/default /etc/opt/sun/comms/im/xyz
   ```

   On Red Hat Linux and Oracle Linux, type:

   ```
   cp -r /etc/opt/sun/im/default /etc/opt/sun/im/xyz
   ```

5. Open the new instance's **imadmin** command in a text editor. By default, this command is stored under the *InstantMessaging_home* directory you just created for the new instance. For Oracle Solaris, the location is:

   ```
   /etc/opt/sun/comms/im/xyz/imadmin
   ```

   For Red Hat Linux and Oracle Linux, the location is:

   ```
   /etc/opt/sun/im/xyz/imadmin
   ```

6. In the **imadmin** command, change the configuration file path to the path for the new configuration file for the new instance. For example, on Oracle Solaris, change

   ```
   /etc/opt/sun/comms/im/default/config/iim.conf
   ```

   to:

   ```
   /etc/opt/sun/comms/im/xyz/config/iim.conf
   ```

   On Red Hat Linux and Oracle Linux, change

   ```
   /etc/opt/sun/im/default/config/iim.conf
   ```

   to:

   ```
   /etc/opt/sun/im/xyz/config/iim.conf
   ```

   Note that the **.xml** suffix is not required for the **iim.conf** file and the **imadmin** command automatically adds the **.xml** suffix.

7. Save and close the **imadmin** command.

8. Use the **imconfutil** command to set configuration properties for the new instance. By default, the **iim.conf.xml** file is stored in the *InstantMessaging_cfg_home* directory you created for the new instance. For Oracle Solaris, the location is:

   ```
   /etc/opt/sun/comms/im/xyz/config/iim.conf.xml
   ```

   For Red Hat Linux and Oracle Linux, the location is:

   ```
   mkdir /var/opt/sun/im/xyz/log
   ```

   The configuration properties you need to set are:

   - **iim_server.port** (default=5269)
   - **iim_mux.listenport** (default=5222)
   - **iim_mux.serverport** (default=45222)
   - **iim.instancedir**

     Set to the runtime directory for the new instance, for example, on Oracle Solaris, change

     ```
     /var/opt/sun/comms/im/default
     ```

     to:

     ```
     /var/opt/sun/comms/im/xyz
     ```

     On Red Hat Linux and Oracle Linux, change

     ```
     /var/opt/sun/im/default
     ```

     to:

     ```
     /var/opt/sun/im/xyz
     ```

9. Ensure that file and directory ownership and permissions are the same for all instances.

10. Start the new instance.

    - On Solaris OS:

      ```
      /etc/opt/sun/comms/im/xyz/imadmin start
      ```

- On Red Hat Linux and Oracle Linux:

```
/etc/opt/sun/im/xyz/imadmin start
```

6

Upgrading Instant Messaging Server

This chapter explains how to upgrade your existing system to the latest release of Oracle Communications Instant Messaging Server.

> **Note:** You can upgrade to Instant Messaging Server only by using the Communication Suite installer.

About Upgrading Instant Messaging Server

The process for upgrading the Instant Messaging server and multiplexor is the same and should take only a few minutes. The upgrade procedure automatically copies the pre-upgrade release product configuration and other data to the post-upgrade version. If Instant Messaging Server is configured to provide email notifications, or calendar alerts, the configuration data of these features is migrated to the post-upgrade version.

Upgrading from 9.0.1.4 to 9.0.2.6

You can upgrade from release 9.0.1.4 to 9.0.2.6.

If you are not yet running a version of Instant Messaging Server 9, see "Upgrading Instant Messaging Server (Prior to Version 9 to 9.0.2.6)".

> **Note:** Java is no longer bundled with the Oracle Communications Unified Communications Suite installer and requires manual installation. It is important that you install the correct version of Java for Instant Messaging 9.0.1.4.0. For information, see "Installing Java".

Upgrading Instant Messaging Server (9.0.1.4 to 9.0.2.6)

To upgrade to 9.0.2.6:

1. Stop Instant Messaging Server.

   ```
   imadmin stop
   ```

2. Use the Communications Suite installer to upgrade Instant Messaging.

   ```
   commpkg upgrade
   ```

   For more information, see the **commpkg upgrade** documentation at:

   https://wikis.oracle.com/display/CommSuite/commpkg+upgrade+7.0.6+Usage

3. Select the Instant Messaging Server 9.0.2.6.0 component from the Product Selection list.
4. Respond to the Communications Suite installer prompts to upgrade.
5. Restart Instant Messaging Server.

   ```
   imadmin start
   ```

6. (Optional) If you have deployed any Web applications, redeploy them.

   ```
   iwadmin redeploy app_name
   ```

   where *app_name* can be **im**, **httpbind**, or **all**.

   This step completes the upgrade process and redeploys the specified component(s).
7. If you had previously configured your deployment to use Service Management Facility (SMF), run the following command to enable SMF, as the upgrade does not preserve SMF status.

   ```
   imadmin smf-register
   ```

8. When upgrading to Instant Messaging Server 9.0.1.4.0, check if you are using any of the following items and do not wish to reconfigure:
   - Components: Calendar Agent, HTTPBind, and so on
   - S2S Federation
   - Server Pool
   - Server health monitoring using Watchdog

If you use any of these items, and if you continue to use the existing configuration file and do not wish to reconfigure, then you must set the **iim_server.useport** property to **true** by using the **imconfutil** command. For example:

```
imconfutil -c xml_config_file set-prop iim_server.useport=true
```

Upgrading Instant Messaging Server (Prior to Version 9 to 9.0.2.6)

Upgrading to Instant Messaging Server 9.0.2.6.0 from an Instant Messaging Server release prior to version 9 is a two step process. You must first upgrade to Instant Messaging Server 9. Then, you upgrade to Instant Messaging Server 9.0.2.6.0.

To upgrade from a version prior to Instant Messaging Server 9:

1. To upgrade to Instant Messaging Server 9, see the upgrade documentation at:

   https://wikis.oracle.com/display/CommSuite7U2/Instant+Messaging+Upgrade
2. Run the following commands for the Instant Messaging Server 8 parameters that did not get migrated:

   ```
   imconfutil set-listener-prop -u -c /opt/sun/comms/im/config/iim.conf.xml c2s
   port=45222 worker-out=muxout
   worker-in=muxin protocols=c2s
   imconfutil set-prop -u -c /opt/sun/comms/im/config/iim.conf.xml iim_
   server.deliverofflinechat=true
   iim_mux.jvm.maxmemorysize=2048 iim_ldap.conferencecontainer="ou=sunConferences"
   iim.policy.cachevalidity=3600
   ```

3. To upgrade from Instant Messaging Server 9 to Instant Messaging Server 9.0.2.6.0, see "Upgrading Instant Messaging Server (9.0.1.4 to 9.0.2.6)".

Post-Upgrade Tasks

See known problems in *Instant Messaging Server Release Notes* for post-upgrade tasks that might be necessary.

Upgrading from 9.0.1.4 to 9.0.2.6 in a Highly Available Environment

Upgrading Instant Messaging Server in an HA environment consists of upgrading the Instant Messaging Server software followed by upgrading the Instant Messaging Server Sun Cluster Agent.

To Upgrade to Instant Messaging Server 9.0.2.6 in an HA Environment

1. Disable the Instant Messaging Server resource.

   ```
   scswitch -n -j im-server-resource
   ```

2. Make sure that the non-active node does not have access to the configuration directory.
3. Run the **commpkg upgrade** command on all cluster nodes.
4. Copy the Instant Messaging 9 configuration file **iim.conf.xml** to the **iim.conf** file with the same permissions.

   Also copy the **iim.conf.xml** file to **iim.conf** after any future configuration changes as cluster uses the **iim.conf** file.
5. To use the new 'GatewayConnector' service in HA, update this service configuration with the virtual host name or IP address and port number as follows:

   ```
   imconfutil --config config_file set-prop iim_gwc.hostport=virtual host-name or ip:port
   ```

   For example:

   ```
   imconfutil --config /DATA1/default/config/iim.conf.xml set-prop iim_
   gwc.hostport=192.10.12.11:22222
   ```

6. Enable the Instant Messaging server resource.

   ```
   scswitch -e -j im-server-resource
   ```

To Upgrade to Instant Messaging Server 9.0.2.6 Sun Cluster Agent (IM_SCHA)

Run the **commpkg upgrade** command on all nodes on the cluster. If cluster node is a non-global zone, run **commpkg upgrade** in global zone as well as in non-global zones.

Rolling Back an Upgrade

If the upgrade fails or if you need to go back to the previously working version of Instant Messaging Server, you can roll back the upgrade process.

To roll back the upgrade process:

1. Stop all services.

```
imadmin stop
```

2. Remove the Instant Messaging Server 9.0.2.6 packages.

   For example, on Solaris, use the **pkgrm** command.

3. Install a prior version of Instant Messaging Server by using the Communications Suite installer for that version.

7

Uninstalling Instant Messaging Server

This chapter describes how to uninstall Oracle Communications Instant Messaging Server.

Uninstalling Instant Messaging Server

The **commpkg uninstall** command enables you to uninstall Communications Suite products, such as Instant Messaging Server, as well as shared components. However, the **commpkg uninstall** command does not remove OS patches or shared components installed by **commpkg install**.

To uninstall Instant Messaging Server:

1. Log in as **root**.
2. Change to the *InstantMessaging_home***/CommsInstaller/bin** directory.
3. Run the **commpkg uninstall** command.
4. Choose Instant Messaging Server from the list of installed Communications Suite components.
5. When prompted, enter **Yes** to continue.

8

Installing Patches

This chapter describes how to install patches on Oracle Communications Instant Messaging Server.

See the patch ReadMe file, included in the patch download, for information about the contents of a patch.

About Patching Instant Messaging Server

Instant Messaging Server patches are posted on the My Oracle Support web site:

https://support.oracle.com

To install patches, use the **patchadd** command on Solaris OS, and use the **rpm** command on Linux.

> **Important:** Always read the patch ReadMe file in its entirety before installing a patch.

Some patches contain fixes and functionality that may not be of any interest to you or may apply to features that you have not installed or purchased. Read the patch ReadMe file to determine if you must install the patch.

Some patches are password protected. To request the password to download a protected patch, open a Service Request on the My Oracle Support web site.

Planning Your Patch Installation

Before installing a patch, verify your version of Instant Messaging Server and ensure the patch is not already installed.

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

Oracle recommends installing a patch on a test system with a copy of your production data before installing the patch on your production system. Test the patch by logging into Instant Messaging Server and verifying the version number of installed components.

Installing a Patch

To install a patch on Instant Messaging Server:

1. Stop Instant Messaging Server services.

```
imadmin stop
```

2. Apply the patch.
   - Solaris OS: Run the **patchadd** command. See the **patchadd** main page for more information.
   - Linux: Run the **rpm -F** *rpmname* command. See the **rpm** main page for more information.