



Post-Installation Tasks for IM and Presence Service

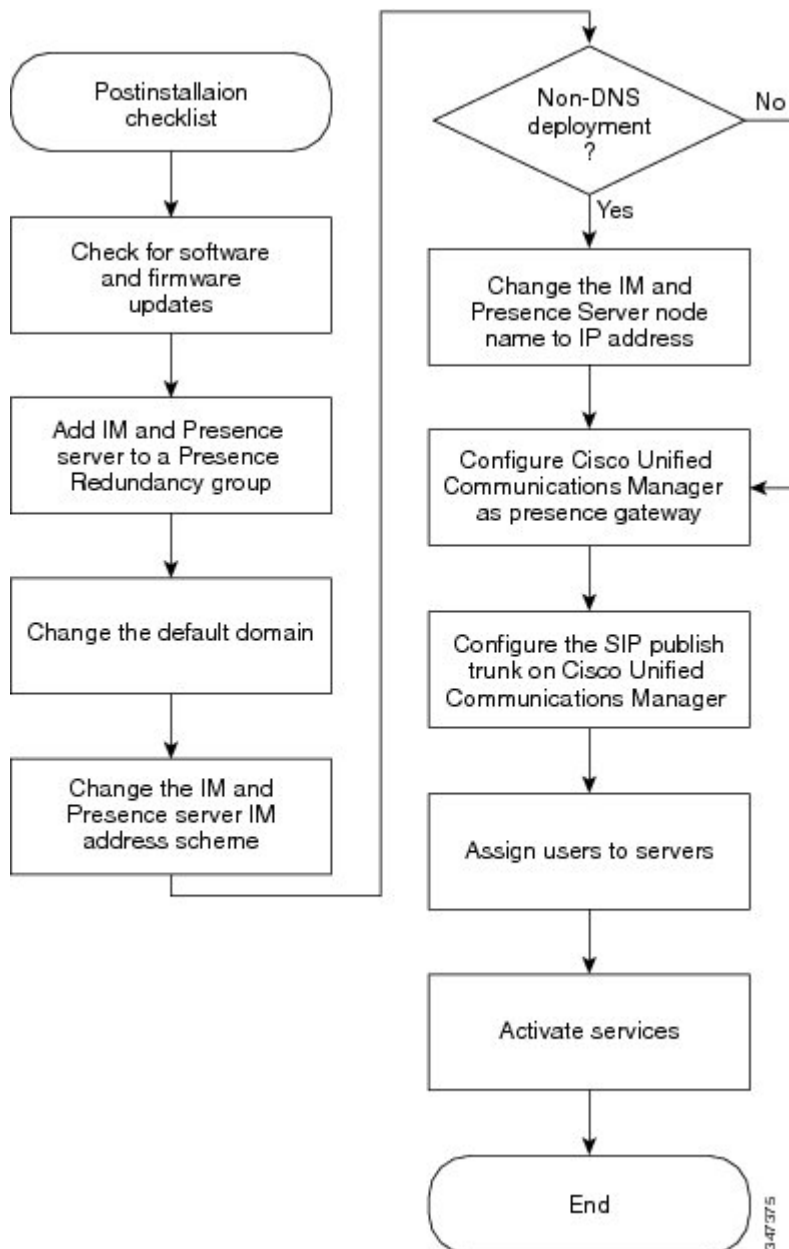
This chapter provides information about the following topics:

- [Post-Installation Tasks for IM and Presence Service, page 2](#)
- [Presence Redundancy Groups and High Availability, page 4](#)
- [Change Default Domain Name, page 5](#)
- [IM Address Scheme, page 5](#)
- [Change of IM and Presence node name to resolvable value, page 7](#)
- [Configure Cisco Unified Communications Manager as Presence Gateway, page 7](#)
- [Configure SIP Trunk on Cisco Unified Communications Manager, page 7](#)
- [User and Server Assignments, page 8](#)
- [Activate services, page 8](#)

Post-Installation Tasks for IM and Presence Service

Complete the following tasks, in sequence, on each server that you install in an IM and Presence Service cluster.

Figure 1: Post-Installation Flowchart



Procedure

- Step 1** Check for software and firmware updates for IM and Presence Service on Cisco.com.
 - Step 2** Add the IM and Presence Service server to a presence redundancy group.
 - Step 3** Change the default domain name.
Note For non-DNS deployments, this step is mandatory. For DNS deployments, this step is optional.
 - Step 4** (Optional) Change the IM and Presence Service IM address scheme.
 - Step 5** (Optional) Change the IM and Presence Service node name.
 - Step 6** Configure Cisco Unified Communications Manager as a Presence Gateway.
 - Step 7** Configure a SIP Publish trunk on Cisco Unified Communications Manager.
 - Step 8** Assign users to servers.
 - Step 9** Activate services.
-

**Caution**

Ensure that you complete this post-installation checklist on the IM and Presence Service database publisher node before you install IM and Presence Service subscriber nodes.

Software Updates

After you install IM and Presence, check to see if Cisco has released software updates, critical patches or Service Updates.

Check for software upgrades

Software upgrades contain fixes that were unavailable at the time of the original release. They often include service updates, security fixes, firmware updates, critical patches or other software fixes that can improve operation.

Complete the following procedure to check for software upgrades.

Procedure

- Step 1** Browse to www.cisco.com.
 - Step 2** Select **Support > Download Software**.
 - Step 3** Navigate to **Products > Voice and Unified Communications > Unified Communications Applications > Cisco Unified Presence > Cisco Unified Presence Version > <the version for your deployment>**.
 - Step 4** If there are any software upgrades, follow the instructions to download the software.
-

What to Do Next

Configure the Cisco Unified Communications Manager as a Presence Gateway.

Presence Redundancy Groups and High Availability

A presence redundancy group is comprised of two IM and Presence Service nodes from the same cluster and provides both redundancy and recovery for IM and Presence Service clients and applications. Use **Cisco Unified CM Administration** to assign nodes to a presence redundancy group and to enable high availability.

- Failover - Occurs in a presence redundancy group when one or more critical services fails on an IM and Presence Service node in the group or a node in the group fails. Clients automatically connect to the other IM and Presence Service node in that group.
- Fallback - Occurs when a fallback command is issued from the Command Line Interface (CLI) or Cisco Unified Communications Manager during either of these conditions:
 - The failed IM and Presence Service node comes back into service and all critical services are running. The failed over clients in that group reconnect with the recovered node when it becomes available.
 - The backup activated IM and Presence Service node fails due to a critical service failure, and the peer node is in the Failed Over state and supports the automatic recovery fallback.

Automatic FallbackIM and Presence Service supports automatic fallback to the primary node after a failover. Automatic fallback is the process of moving users back to the primary node after a failover without manual intervention. You can enable automatic fallback with the Enable Automatic Fallback service parameter on the Cisco Unified CM IM and Presence Administration interface. Automatic fallback occurs in the following scenarios:

- A critical service on Node A fails—A critical service (for example, the Presence Engine) fails on Node A. Automatic failover occurs and all users are moved to Node B. Node A is in a state called “Failed Over with Critical Services Not Running”. When the critical service recovers, the node state changes to “Failed Over.” When this occurs Node B tracks the health of Node A for 30 minutes. If no heartbeat is missed in this timeframe and the state of each node remains unchanged, automatic fallback occurs.
- Node A is rebooted—Automatic failover occurs and all users are moved to Node B. When Node A returns to a healthy state and remains in that state for 30 minutes automatic fallback will occur.
- Node A loses communications with Node B—Automatic failover occurs and all users are moved to Node B. When communications are re-established and remain unchanged for 30 minutes automatic fallback will occur.

If failover occurs for a reason other than one of the three scenarios listed here, you must recover the node manually. If you do not want to wait 30 minutes before the automatic fallback, you can perform a manual fallback to the primary node. For example: Using presence redundancy groups, Cisco Jabber clients will fail over to a backup IM and Presence Service node if the services or hardware fail on the local IM and Presence Service node. When the failed node comes online again, the clients automatically reconnect to the local IM and Presence Service node. When the failed node comes online, a manual fallback operation is required unless the automatic fallback option is set.

You can manually initiate a node failover, fallback, and recovery of IM and Presence Service nodes in the presence redundancy group. A manual fallback operation is required unless the automatic fallback option is set.

For instructions to set up presence redundancy groups and high availability, see *Cisco Unified Communications Manager Administration Guide*.

Change Default Domain Name

You are required to change the default domain name for non-DNS deployments. Changing the domain name is optional for DNS deployments.

If your IM and Presence Service deployment does not use DNS, the domain name for the IM and Presence Service node is set to DOMAIN.NOT.SET during installation. Cisco recommends that you change this value to the enterprise domain value after installation is complete.

You must stop the following services on all nodes in the cluster before you change the domain name, and then restart those services after the changes are made:

- Cisco Client Profile Agent
- Cisco Presence Engine
- Cisco SIP Proxy
- Cisco Sync Agent
- Cisco XCP Router

For information about how to change the default domain name, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

For information about using domain names with Cisco Unified Communications Manager and system managed components, see the *Cisco Unified Communications System Solution Reference Network Design (SRND)* guide for your release.

IM Address Scheme

You can select the scheme that the IM and Presence Service uses for IM addressing in the cluster. Use the Cisco Unified CM IM and Presence Administration GUI to set the IM address scheme. Two IM address schemes are available:

- *UserID@Default_Domain*
- Directory URI

**Note**

The IM address scheme that you choose must be consistent across all IM and Presence Service clusters.

For more information about setting the IM address scheme for the IM and Presence Service cluster and Directory URI requirements, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

IM Address Using UserID@Default_Domain

The *UserID@Default_Domain* IM address scheme is the default option when you perform a fresh install or upgrade IM and Presence Service from an earlier version. To configure the default domain, choose **Cisco Unified CM IM and Presence Administration > Presence > Settings > Advanced Configuration**.

IM Address Using Directory URI

The Directory URI address scheme aligns a user's IM address with their Cisco Unified Communications Manager Directory URI.

The Directory URI IM address scheme provides the following IM addressing features:

- Multiple domain support. IM addresses do not need to use a single IM and Presence Service domain.
- Alignment with the user's email address. The Cisco Unified Communications Manager Directory URI can be configured to align with a user's email address to provide a consistent identity for email, IM, voice and video communications.
- Alignment with Microsoft SIP URI. The Cisco Unified Communications Manager Directory URI can be configured to align with the Microsoft SIP URI to ensure that the user's identity is maintained when migrating from Microsoft OCS/Lync to IM and Presence Service.

You set the Directory URI using Cisco Unified CM IM and Presence Administration GUI in one of two ways:

- Synchronize the Directory URI from the LDAP directory source.

If you add an LDAP directory source in Cisco Unified Communications Manager, you can set a value for the Directory URI. Cisco Unified Communications Manager then populates the Directory URI when you synchronize user data from the directory source.



Note If LDAP Directory Sync is enabled in Cisco Unified Communications Manager, you can map the Directory URI to the email address (mailid) or the Microsoft OCS/Lync SIP URI (msRTCSIP-PrimaryUserAddress).

- Manually specify the Directory URI value in Cisco Unified Communications Manager.

If you do not add an LDAP directory source in Cisco Unified Communications Manager, you can manually enter the Directory URI as a free-form URI.



Caution

If you configure the node to use Directory URI as the IM address scheme, Cisco recommends that you deploy only clients that support Directory URI. Any client that does not support Directory URI will not work if the Directory URI IM address scheme is enabled. Cisco recommends that you use the *UserID@Default_Domain* IM address scheme and not the Directory URI IM address scheme if you have any deployed clients that do not support Directory URI.

See the *Cisco Unified Communications Manager Administration Guide* for more information about setting up the LDAP directory for Directory URI.

Directory URI IM Address Considerations

Observe the following conditions when using the Directory URI IM address scheme:

- All users have a valid Directory URI value configured on Cisco Unified Communications Manager.
- All deployed clients must support Directory URI as the IM address.

- The IM address scheme must be consistent across all IM and Presence Service clusters.

See the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager* for detailed Directory URI IM address requirements and interactions.

Change of IM and Presence node name to resolvable value

During installation, if you select not to use DHCP, you must enter a hostname and IP address for the IM and Presence server. The hostname cannot be null, localhost, or an IP address. The IM and Presence node name gets its value by concatenating the DNS domain to this hostname value to form a fully qualified domain name (FQDN). This FQDN must be resolvable. If you do not use DNS in your deployment, then the IM and Presence node name, which is set to the server's hostname by default, is not resolvable. To overcome this, you must change the IM and Presence node name to be the server's IP address after installation is complete.

For information about how to change the IM and Presence node name, see *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

Configure Cisco Unified Communications Manager as Presence Gateway

**Note**

You must complete this task on each server that you install in an IM and Presence cluster.

- You must configure Cisco Unified Communications Manager as a Presence Gateway on IM and Presence to enable the SIP connection that handles the availability information exchange between Cisco Unified Communications Manager and IM and Presence.
- For more information about how to configure a Presence Gateway on IM and Presence, see the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*.

What to Do Next

Configure a SIP Trunk on a Cisco Unified Communications Manager.

Configure SIP Trunk on Cisco Unified Communications Manager

After you configure Cisco Unified Communications Manager as a Presence Gateway, you must configure a SIP PUBLISH trunk on Cisco Unified Communications Manager. See the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager* for more information.

When you have configured the SIP PUBLISH trunk on Cisco Unified Communications Manager, you must then enable SIP PUBLISH on IM and Presence.

See the *Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager* for more information.

User and Server Assignments

The User Assignment Mode enterprise parameter is set to **Balanced** by default after an initial installation of IM and Presence Service. In balanced mode, users are automatically assigned to IM and Presence Service servers that are configured in a presence redundancy group when users are added to the cluster. No manual user assignment is required when the User Assignment Mode enterprise parameter is set to **Balanced**.

**Note**

For end users to receive the availability and Instant Messaging (IM) services of IM and Presence Service, use Cisco Unified CM Administration to assign end users to IM and Presence Service servers on your nodes and clusters.

For more information about balanced and manual user assignments, and to set up IM and Presence Service servers for users, see the *Cisco Unified Communications Manager Administration Guide* .

Activate services

You must activate the following services:

- Cisco SIP Proxy
- Cisco Presence Engine
- Cisco XCP Connection Manager
- Cisco XCP Authentication Service

To activate the services, select **Tools > Service Activation** in Cisco Unified Serviceability.

**Note**

You must complete this task on each server that you install in an IM and Presence cluster.
